

FATF



# Anti-money laundering and counter-terrorist financing measures

## United States

### Mutual Evaluation Report

December 2016





The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: [www.fatf-gafi.org](http://www.fatf-gafi.org)

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation, whose members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the FATF Recommendations.

For more information about the APG, please visit the website: [www.apgml.org](http://www.apgml.org)

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

**This assessment was adopted by the FATF at its October 2016 Plenary meeting.**

Citing reference:

FATF (2016), *Anti-money laundering and counter-terrorist financing measures - United States*, Fourth Round Mutual Evaluation Report, FATF, Paris  
[www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html](http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html)

© 2016 FATF and APG. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: [contact@fatf-gafi.org](mailto:contact@fatf-gafi.org)).

Photocredits coverphoto: © Joe Mabel

## CONTENTS

EXECUTIVE SUMMARY .....	3
A. Key Findings .....	3
B. Risks and General Situation .....	5
C. Overall Level of Effectiveness and Technical Compliance .....	6
D. Priority Actions .....	11
E. Compliance and Effectiveness Ratings .....	13
MUTUAL EVALUATION REPORT .....	15
Preface .....	15
CHAPTER 1. ML/TF RISKS AND CONTEXT .....	17
ML/TF risks and Scoping of Higher Risk Issues .....	17
Materiality .....	22
Structural Elements .....	22
Background and other Contextual Factors .....	23
CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION .....	37
Key Findings and Recommended Actions .....	37
Immediate Outcome 1 (Risk, Policy and Coordination) .....	39
CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES .....	49
Key Findings and Recommended Actions .....	49
Immediate Outcome 6 (Financial intelligence ML/TF) .....	52
Immediate Outcome 7 (ML investigation and prosecution) .....	63
Immediate Outcome 8 (Confiscation) .....	75
CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION .....	87
Key Findings and Recommended Actions .....	87
Immediate Outcome 9 (TF investigation and prosecution) .....	89
Immediate Outcome 10 (TF preventive measures and financial sanctions) .....	99
Immediate Outcome 11 (PF financial sanctions) .....	107
CHAPTER 5. PREVENTIVE MEASURES .....	117
Key Findings and Recommendations .....	117
Immediate Outcome 4 (Preventive Measures) .....	118
CHAPTER 6. SUPERVISION .....	135
Key Findings and Recommended Actions .....	135
Immediate Outcome 3 (Supervision) .....	136
CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS .....	153
Key Findings and Recommended Actions .....	153
Immediate Outcome 5 (Legal Persons and Arrangements) .....	155
CHAPTER 8. INTERNATIONAL COOPERATION .....	163
Key Findings and Recommended Actions .....	163
Immediate Outcome 2 (International Cooperation) .....	163

TECHNICAL COMPLIANCE ANNEX.....	176
Recommendation 1 - Assessing Risks and applying a Risk-Based Approach.....	176
Recommendation 2 - National Cooperation and Coordination.....	179
Recommendation 3 - Money laundering offense.....	180
Recommendation 4 - Confiscation and provisional measures.....	183
Recommendation 5 - Terrorist financing offense.....	186
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing.....	188
Recommendation 7 – Targeted financial sanctions related to Proliferation.....	192
Recommendation 8 – Non-profit organizations (NPOs).....	194
Recommendation 9 – Financial institution secrecy laws.....	196
Recommendation 10 – Customer due diligence.....	197
Recommendation 11 – Record-keeping.....	205
Recommendation 12 – Politically exposed persons.....	207
Recommendation 13 – Correspondent banking.....	208
Recommendation 14 – Money or value transfer services.....	209
Recommendation 15 – New technologies.....	210
Recommendation 16 – Wire transfers.....	211
Recommendation 17 – Reliance on third parties.....	214
Recommendation 18 – Internal controls and foreign branches and subsidiaries.....	215
Recommendation 19 – Higher-risk countries.....	216
Recommendation 20 – Reporting of suspicious transaction.....	218
Recommendation 21 – Tipping-off and confidentiality.....	219
Recommendation 22 – DNFBPs: Customer due diligence.....	220
Recommendation 23 – DNFBPs: Other measures.....	221
Recommendation 24 – Transparency and beneficial ownership of legal persons.....	222
Recommendation 25 – Transparency and beneficial ownership of legal arrangements.....	226
Recommendation 26 – Regulation and supervision of financial institutions.....	229
Recommendation 27 – Powers of supervisors.....	231
Recommendation 28 – Regulation and supervision of DNFBPs.....	233
Recommendation 29 - Financial intelligence units.....	235
Recommendation 30 – Responsibilities of law enforcement and investigative authorities.....	237
Recommendation 31 - Powers of law enforcement and investigative authorities.....	238
Recommendation 32 – Cash couriers.....	239
Recommendation 33 - Statistics.....	241
Recommendation 34 – Guidance and feedback.....	242
Recommendation 35 – Sanctions.....	243
Recommendation 36 – International instruments.....	245
Recommendation 37 – Mutual legal assistance.....	246
Recommendation 38 – Mutual legal assistance: Freezing and Confiscation.....	248
Recommendation 39 - Extradition.....	249
Recommendation 40 – Other forms of international cooperation.....	250
Summary of Technical Compliance – Key Deficiencies.....	255

## Executive Summary

1. This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in the United States at the date of the on-site visit (18 January 2016 to 5 February 2016). It analyses the level of compliance with the *FATF 40 Recommendations*, the level of effectiveness of its AML/CFT system, and makes recommendations on how the system could be strengthened.

### A. Key Findings

- The AML/CFT framework in the U.S. is well developed and robust. Domestic coordination and cooperation on AML/CFT issues is sophisticated and has matured since the previous evaluation in 2006. The understanding of money laundering (ML) and terrorist financing (TF) risks is well-supported by a variety of ongoing and complementary risk assessment processes, including the 2015 *National Money Laundering Risk Assessment* (NMLRA) and *National Terrorist Financing Risk Assessment* (NTFRA), which were both published. The national AML/CFT strategies, key priorities and efforts of law enforcement and other agencies seem to be driven by these processes and are coordinated at the Federal level across a vast spectrum of agencies in a number of areas.
- The financial sectors bear most of the burden in respect of required measures under the Bank Secrecy Act (BSA). Financial institutions (FIs), in general, have an evolved understanding of ML/TF risks and obligations, and have systems and processes for implementing preventive measures, including for on-boarding customers, transaction monitoring and reporting suspicious transactions.
- However, the regulatory framework has some significant gaps, including minimal coverage of certain institutions and businesses (investment advisers (IAs), lawyers, accountants, real estate agents, trust and company service providers (other than trust companies). Minimal measures are imposed on designated non-financial businesses and professions (DNFBPs), other than casinos and dealers in precious metals and stones, and consist of the general obligation applying to all trades and businesses to report transactions (or a series of transactions) involving more than USD 10 000 in cash, and targeted financial sanctions (TFS) requirements. Other comprehensive AML/CFT obligations do not apply to these

sectors. In the U.S. context the vulnerability of these minimally covered DNFBP sectors is significant, considering the many examples identified by the national risk assessment process.

- Law enforcement efforts rest on a well-established task force environment which enables the pooling of expertise from a wide range of law enforcement agencies (LEAs), including prosecutors, to support quality ML/TF investigation and prosecution outcomes. Overall, LEAs have access to a wide range of financial intelligence, capabilities and expertise allowing them to trace assets, identify targets and undertake expert financial ML/TF investigations. There is a strong focus on following the money in predicate offence investigations at the Federal level. A similar focus on identifying terrorist financiers in terrorism-related investigations applies. The U.S. investigates and prosecutes TF networks aggressively in line with its risk profile. International cooperation in these areas is generally effective though improvements are underway to further improve the timely handling of (a large volume) of mutual legal assistance (MLA) and extradition requests.
- Lack of timely access to adequate, accurate and current beneficial ownership (BO) information remains one of the fundamental gaps in the U.S. context. The NMLRA identifies examples of legal persons being abused for ML, in particular, through the use of complex structures to hide ownership. While authorities did provide case examples of successful investigations in these areas, challenges in ensuring timely access to and availability of BO information more generally raises significant concerns, bearing in mind risk and context.
- At the Federal level, the U.S. achieves over 1 200 ML convictions a year. Many of these cases are large, complex, white collar crime cases, in line with the country's risk profile. Federal authorities have the lead role in all large and/or international investigations. There is however no uniform approach to State-level AML efforts and it is not clear that all States give ML due priority. The AML system would benefit from ensuring that a range of tax crimes are predicate offenses for ML.
- The Federal authorities aggressively pursue high-value confiscation in large and complex cases, in respect of assets located both domestically and abroad. The authorities effectively resort to criminal, civil and administrative tools to forfeit assets. At State and local levels, there is little available information, though it appears that civil forfeiture is vigorously pursued by some States.
- The U.S. authorities effectively implement targeted financial sanctions for both terrorism and proliferation financing purposes, though not all U.N designations have resulted in domestic designations (mainly on the basis of insufficient identifiers). Most designations take place without delay, and are effectively communicated to the private sector. The U.S. Specially Designated Nationals and Blocked Persons List (SDN List) is used by thousands of FIs across the U.S. and beyond which gives the U.S sanctions regime a global effect in line with the size, complexity and international reach of the U.S. financial system. The U.S has had significant success in identifying the funds/other assets of designated persons/entities,



and preventing them from operating or executing financial transactions related to terrorism and proliferation. Only minor improvements are needed in this area.

- AML/CFT supervision of the banking and securities sectors appears to be robust as a whole, and is evolving for money services businesses (MSBs) through greater coordination at the State level. The U.S. has a range of sanctions that it can and does impose on FIs as well as an array of dissuasive remedial measures, including informal supervisory actions. These measures seem to have the desired impact on achieving the supervisory objectives. The most significant supervisory gap is lack of comprehensive AML/CFT supervisory processes for the DNFBPs, other than casinos.

## **B. *Risks and General Situation***

2. The global dominance of the U.S. dollar generates trillions of dollars of daily transaction volume through U.S. banks, which creates significant exposure to potential ML activity (generated out of both domestic and foreign predicate offenses) and risks of cross-border illicit flows. The U.S. also faces significant risks from TF and is vulnerable to such abuse because of the unique scope, openness and reach of its financial system globally, and the direct threat posed by terrorist groups to U.S. interests.

3. The United Nations office on Drugs and Crime (UNODC) estimated proceeds from all forms of financial crime in the U.S., excluding tax evasion, was USD 300 billion in 2010 (about 2% of the U.S. economy). Fraud (including healthcare fraud, identity theft, tax fraud, mortgage fraud, retail and consumer fraud and securities fraud) generates the largest volume of illicit proceeds, particularly healthcare fraud against the Federal government which accounts for approximately USD 80 billion annually. Other major sources of proceeds are drug trafficking (generating about USD 64 billion annually), transnational organized crime, human smuggling and public corruption (both domestic and foreign).

4. The main ML vulnerabilities assessed by the U.S. were in the cash, banking, MSB, casino and securities sectors, and were characterized as: use of cash and monetary instruments in amounts under regulatory record-keeping and reporting thresholds; opening bank and brokerage accounts using nominees to disguise the identity of the individuals who control the accounts; creating legal entities without accurate information about the identity of the beneficial owner; misuse of products and services resulting from deficient compliance with AML obligations; and merchants and FIs wittingly facilitating illegal activity. The main TF threats and vulnerabilities include: raising funds through criminal activity, individuals raising funds under the auspices of charitable giving but outside of any charitable organization, individual contributions and self-funding; moving and placing funds through banks, licensed MSBs, unlicensed money transmitters and cash smuggling; and potential emerging threats from global terrorist activities, cybercrime and identity theft, and new payment systems.

### *C. Overall Level of Effectiveness and Technical Compliance*

5. The AML/CFT regime has undergone significant progress since the previous assessment in 2006. The U.S. has a strong legal and institutional framework for combating ML/TF and proliferation financing (PF). The technical compliance framework is particularly strong regarding law enforcement, confiscation, TFS, and international cooperation, but significantly less so regarding transparency of legal persons and arrangements. There is a lack of comprehensive preventive measures by DNFBPs (other than casinos and dealers in precious metals and stones), including those exposed to higher risks. Additionally, not all IAs are subject to comprehensive AML/CFT requirements.

6. In terms of effectiveness, the U.S. achieves high results in prevention, investigation, prosecution and sanctions for TF and PF, for preventing the abuse of the NPO sector, and confiscation. The U.S. also achieves substantial outcomes in understanding ML/TF threats, domestic coordination and international cooperation, using financial intelligence and other information, and investigating and sanctioning ML offenses, such that only moderate improvements are needed in these areas. The U.S. needs to make fundamental improvements in order to protect legal persons, and to a lesser extent legal arrangements, from ML/TF abuse, and ensure that the competent authorities have timely access to BO information. Major improvements are needed to apply appropriate preventive measures to all FIs and DNFBPs, in particular to high risk situations, and to undertake effective supervision of all sectors.

#### *C.1 Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1-2 & 33)*

7. Overall, the U.S. has attained a significant level of understanding of its ML/TF threats which it develops through comprehensive and ongoing risk assessment processes. National AML/CFT strategies, and law enforcement priorities and efforts, are broadly in line with the country's main risks as identified in the 2015 NMLRA and NTFRA.

8. A wide array of other national risk assessments have also been undertaken and are used to support the U.S. strategies to combat terrorism, major proceeds generating predicate offenses, and related ML/TF. These risk assessments are not public, but they underpin national strategies that are published and contain useful information on related ML/TF risks. This process is led, at the highest level of government, by two agencies within the Executive Office of the President: the National Security Council (NSC) and the Office of National Drug Control Policy (ONDCP), with effective participation and involvement of other agencies.

9. National coordination and cooperation on AML/CFT issues has improved significantly in the U.S. since the last evaluation. Policy and operational coordination are particularly well-developed on counter-terrorism, counter-proliferation and related financing issues which are the government's top national security priorities. The authorities have also leveraged this experience into better inter-agency cooperation and collaboration on combating ML.

10. However, mitigation of the identified vulnerabilities is less well developed. The BSA AML/CFT regulatory framework has a number of exemptions, gaps and thresholds which do not appear to be justified or in line with the vulnerabilities identified through the risk assessment process. Further,



the NMLRA did not address the systemic vulnerabilities in the DNFBP sector. For example, there is no requirement to collect BO information (as defined by the FATF) in all cases and there are suspicious transaction reporting thresholds. In addition, most DNFBP sectors are not subject to comprehensive AML/CFT measures (for example, lawyers, accountants, trust and company service providers (except trust companies), and real estate agents). Investment advisers in the securities sector are only indirectly subject to AML/CFT requirements when they are affiliated to a financial group or are acting for a covered financial institution in the framework of outsourcing arrangements. In addition, the extent to which ML is pursued, and risks are mitigated, at the State level is not clear.

## *C.2 Financial intelligence, and ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.3, 4, 29–32)*

11. Competent authorities at the Federal, State and local levels regularly use a wide range of financial intelligence to support ML/TF investigation, trace assets, develop operational and strategic analysis, and identify risks. This is primarily achieved through direct access to and use of the data held by the financial intelligence unit (FIU), FinCEN. FinCEN's extensive financial intelligence includes Suspicious Activity Reports (SARs) and a range of other mandatory reports. FinCEN has adopted a risk-based approach (RBA) to analysing the large amount of data received annually, and uses sophisticated and evolving automatic business rules to identify priority reports and SARs. A large number of SARs are also analysed independently by LEAs and other agencies with direct access to FinCEN's database, in line with their operational needs. Such analysis is supplemented by FinCEN's increasingly pro-active dissemination of intelligence, although there is scope for further improvement in this area.

12. While the financial intelligence system is broadly robust, its effectiveness is somewhat impaired by technical gaps that limit the information available to competent authorities at any given point in time. These include the application of reporting thresholds for SARs, and the lack of reporting requirements for most of DNFBPs (see section C.4 below). In addition, there is scope for FinCEN to continue and enhance its recent practice to use its information collection powers to support operational intelligence analysis and spontaneous dissemination. These gaps are somewhat mitigated by FinCEN's extensive outreach programs and products, as well as by directing covered institutions to report activities requiring immediate attention without regard for the reporting thresholds, particularly for TF.

13. On ML, Federal LEAs have adopted a "follow the money" approach to predicate offense investigation and have extensive capabilities, resources and tools for undertaking specialist financial investigations. The U.S. conducts a large number of financial investigations, resulting in over 1200 ML convictions, on average at the Federal level, each year. A wide variety of ML activity is pursued and there seems to be a strong focus on serious, complex and high-dollar value criminal offenses. Inter-agency task forces bring together complementary agency-specific expertise and resources which facilitates the pursuit of complex financial investigations. Federal prosecutors have the authority to negotiate and potentially drop ML charges against lower level offenders if the defendant cooperates with law enforcement against co-conspirators and higher level criminals in furtherance of national strategies developed and implemented by Federal authorities. State law enforcement

authorities can complement Federal efforts, but more typically pursue State-level law enforcement priorities. Among the States, there is no uniform approach and little data is available. Where information was provided, it tended to suggest that ML is not prioritised by the State authorities.

14. National (Federal) strategies are in place to target higher-risk areas. These are in line with the NMLRA, and resources are allocated accordingly to relevant task forces/Federal agencies. There is overall scope for all Federal agencies to pursue ML more regularly as a discrete offense type. While U.S. authorities effectively use an all-tools approach to pursue ML predicate offenses, they would benefit from ensuring that serious tax crimes are predicates for ML.

15. The U.S. achieves a considerable value of assets confiscation (e.g. over USD 4.4 billion in 2014) and is able to do so effectively using administrative forfeiture, non-conviction based forfeiture and criminal confiscation tools. The U.S. Federal authorities aggressively pursue high-value confiscation. They are able to do so in the context of large and complex cases, and in respect of assets located both domestically and abroad. Effectiveness in this area would be further enhanced by legislating to introduce a general power to seize/freeze property of corresponding/equivalent value which may become subject to a value-based forfeiture order, and to ensure that all predicate offenses include the power to forfeit instrumentalities.

### *C.3 Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R.5–8)*

16. The U.S. has a robust legal framework to combat TF, and a clear and comprehensive understanding of its terrorism and TF risks. Its CFT efforts are fully integrated into its wider counterterrorism strategy, and any terrorism-related investigation is accompanied by a parallel investigation to identify potential sources of financial support. Specialized financial investigation units are fully integrated into departments responsible for investigating terrorism. The U.S. has also adopted a strong multi-agency approach with 104 Joint Terrorism Task Forces (JTTFs) operating nation-wide and pooling together a wide range of LEA capabilities.

17. The U.S. proactively and aggressively investigates, prosecutes and convicts individuals involved in a wide range of TF schemes using its broad TF statutes which capture any form of material support. Where a TF charge is not possible, the U.S. employs an 'all tools' approach to prosecute and convict terrorists or would-be terrorists. The U.S. continually adjusts its efforts by setting up specialist units and/or operations to respond to emerging threats. CFT is further supported by comprehensive two-way intelligence exchange mechanisms between field offices and policy analysis units. U.S. authorities also engage extensively with the private sector enabling constructive information sharing on TF and terrorism-related threats.

18. Both proliferation financing (PF) and TF are considered a high priority. The U.S. has implemented both TF and PF-related TFS - mostly without delay. Designations are communicated proactively and widely to FIs/DNFBPs via several communication channels. The U.S. SDN List is used by thousands of FIs across the U.S. and around the world to screen real-time transactions and accounts. U.S. regulators are able to enforce requirements imposed on U.S. and correspondent FIs wishing to do business in or through the U.S., or in U.S. dollar-denominated transactions. This global reach of the U.S. sanctions regime reflects the size, complexity and international reach of the U.S.

financial system. The U.S. has established a targeted RBA to NPO outreach, oversight, investigations and enforcement actions which are largely based on regular engagement with NPOs and intelligence.

19. The U.S. has had significant success in identifying the funds/other assets of designated persons/entities, and preventing them from operating or executing financial transactions related to proliferation. However, deficiencies in the country's implementation of BO requirements impacts the ability of FIs and DNFBPs to identify the funds/assets of designated individuals/entities, as does the fact that the U.S. has not domestically designated all of the individuals/entities designated by the UN. These deficiencies are, however, significantly mitigated by the coordinated inter-agency approach taken by the U.S. authorities to the sharing of information and intelligence in relation to both TF and PF.

#### *C.4 Preventive measures (Chapter 5; IO.4; R.9–23)*

20. The U.S. has extremely large and diverse financial and DNFBP sectors. The vulnerabilities to ML/TF of individual FIs and DNFBPs vary greatly. Overall, the financial sector bears most of the burden of preventive measures and reporting, with the domestic banking sector playing a predominant role in the domestic and international financial sectors, along with the securities sector. MSBs are large in number, diverse and also an important part of the financial architecture. Among DNFBPs, the casino sector is large and has been identified in the NMLRA as vulnerable to money laundering. In practice, while not essential to the process of company or legal arrangement formation, lawyers, company formation agents and to a lesser extent, accountants are often involved (with varying degrees) and with related transactions (lawyers and company service providers are involved in the formation of close to 50% of legal persons). Lawyers and real estate agents also have roles in relation to buying and selling of high-end real estate. The remaining DNFBP sectors are of less relative importance in the U.S. given its risks and context, as noted in the Scoping Note (see Chapter 1).

21. FIs, in general, demonstrate a fair understanding of ML/TF risks and obligations, though the quality of understanding varies across and within sectors, and between institutions. The level of understanding is highest in the banking sector. The Residential Mortgage Lenders and Originators (RMLOs - FIs considered by the U.S. as an important intersection with the real estate sector and hence subject to AML/CFT obligations) do not seem to have a good understanding of ML vulnerabilities in their sector or the importance of their role in addressing them. Furthermore, there are TC gaps, specifically certain exemptions and thresholds in the BSA regime, non-coverage of all IAs, which collectively soften the deterrent value of preventive measures being applied by FIs in general, as well as negatively impacting intelligence gathering.

22. As regards DNFBPs, only casinos and dealers in precious metals and stones are subject to comprehensive AML/CFT requirements. Of late, there appears to be greater appreciation of ML/TF vulnerabilities and implementation of preventive measures by casinos; and some professional guidance exists for other sectors (in particular, lawyers) on AML/CFT issues. However, DNFBPs other than casinos and dealers in precious metals and stones have limited preventive measures applied leaving vulnerabilities particularly in respect of the high-end real estate sector and those sectors involved in the formation of legal persons. Furthermore, apart from casinos, there is no

evidence that DNFBPs as a whole have an adequate understanding of ML/TF vulnerabilities and the need to implement appropriate controls to mitigate them. Lawyers, accountants, high-end real estate agents and trust and company service providers (other than trust companies) who establish or otherwise facilitate access to financial services for legal persons and arrangements are not subject to comprehensive AML/CFT requirements, and are not systematically applying basic or enhanced due diligence processes and other preventive measures, as needed; and this is further exacerbated by the deficiencies in the BO requirements.

### *C.5 Supervision (Chapter 6; IO.3; R.26–28, 34, 35)*

23. The U.S. supervisory framework for Covered FIs and DNFBPs is very complex with AML/CFT supervision being undertaken by multiple regulators at the Federal and State levels, using different supervisory approaches. In the banking sector, the Federal Financial Institutions Examination Council's Banking Secrecy Act (FFIEC/BSA) Manual is a good, up-to-date reference document, both for banks and supervisors, and constitutes a robust baseline for the implementation of the AML/CFT requirements and their controls. The insurance sector is supervised for BSA AML/CFT requirements primarily by State authorities although, BSA AML/CFT enforcement authority resides with the Federal government. IAs are not covered by BSA obligations. However some IAs are indirectly covered through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements.

24. The DNFBP sectors are subject to varying AML/CFT requirements. While there has been a strong supervisory focus on the casino sector in recent years due to the identified vulnerabilities, and the fact that the IRS examines dealers in precious metals and stones for BSA compliance, other DNFBPs are subject to less supervision as they are not subject to comprehensive AML/CFT preventive measures. This is mitigated somewhat for lawyers and accountants who have strong professional entry and continuing ethical requirements, though these do not adequately address ML/TF vulnerabilities or require reporting of suspicious activity to authorities.

### *C.6 Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

25. The ML/TF risks of legal persons and arrangements are very well understood by Federal competent authorities and are reflected as case examples in the 2015 NMLRA. However, overall, the measures to prevent the misuse of legal persons are inadequate. The U.S. legal framework has serious gaps that impede effectiveness in this area.

26. The 2015 NMLRA sets out numerous instances of legal persons and, to a lesser extent, arrangements being abused for ML. It also highlights the use of complex structures, shell or shelf corporations, other forms of legal entities, and trusts, to obfuscate the source, ownership, and control of illegal proceeds.

27. The authorities provided case examples to demonstrate that LEAs are able to obtain some information about the BO of legal persons and legal arrangements that are created in the U.S. In certain instances the information eventually obtained has been shown to be adequate and accurate. However, as there are no legal requirements to record BO information (as defined by the FATF)

systematically, LEAs must often resort to resource-intensive and time-consuming investigative and surveillance techniques. As a result, concerns remain about the ability of competent authorities to access accurate BO information in a timely manner.

#### *C.7 International cooperation (Chapter 8; IO.2; R.36–40)*

28. The U.S. has an effective system for international cooperation. As one of the largest economies and financial systems in the world, it is the recipient of a very large number of requests for financial-crime related MLA. Feedback received from other countries did not highlight any systematic concerns and supported the view that the U.S. provides good quality and constructive MLA and extradition across the range of international cooperation requests, including in relation to ML, TF and asset forfeiture. As part of a modernisation plan, the U.S is currently significantly increasing the number of staff to improve the timely processing of MLA requests, and improving its IT system to systematically collect statistics on how long the MLA/extradition process takes.

29. The lack of readily accessible BO information means that U.S. authorities are unlikely to undertake a resource-intensive investigation to uncover BO information on behalf of a foreign counterpart unless the case is of a significantly high priority. Even if relevant resources are devoted to the case, timely access to the information may not be guaranteed.

#### **D. Priority Actions**

30. The prioritised recommended actions for the United States, based on these findings, are:

1. Take steps to ensure that adequate, accurate and current BO information of U.S. legal persons is available to competent authorities in a timely manner, by requiring that such information is obtained at the Federal level.
2. Implement BO requirements under the BSA (scheduled to come into force in 2018) and apply these to the sectors discussed in point 3 below.
3. Apply appropriate AML/CFT obligations as follows:
  - a) To investment advisers. Even if some investment advisers are already indirectly covered through their association with banks, bank holding companies and security broker dealers, the direct application of AML/CFT rules to all investment advisers will address a vulnerability identified by the U.S. authorities themselves;
  - b) On the basis of a specific vulnerability analysis, to lawyers, accountants, trust and company service providers (other than trust companies which are already covered); and
  - c) After the outcomes of the recent GTO have been analysed, take appropriate action to address the ML risks in relation to high-end real estate.
4. Issue guidance to clarify the scope of the immediate SAR reporting requirement, in order to make it clear that the requirement applies below the otherwise applicable thresholds; and conduct a focused risk review of the existing SAR reporting thresholds and the 60/30 day reporting deadlines.

5. Improve the visibility of AML and State level activities and statistics, including via improved data collection and sharing, for a clearer nation-wide picture of the adequacy of AML efforts at all levels.
6. FinCEN should continue to expand its use of tools such as the GTO and 314a requests, and further its pro-active dissemination of strategic and operational intelligence products to law enforcement.



## E. Compliance and Effectiveness Ratings

### Effectiveness Ratings (High, Substantial, Moderate, Low)

<b>IO.1</b> - Risk, policy and coordination	<b>IO.2</b> - International cooperation	<b>IO.3</b> - Supervision	<b>IO.4</b> - Preventive measures	<b>IO.5</b> - Legal persons and arrangements	<b>IO.6</b> - Financial intelligence
<b>Substantial</b>	<b>Substantial</b>	<b>Moderate</b>	<b>Moderate</b>	<b>Low</b>	<b>Substantial</b>
<b>IO.7</b> - ML investigation & prosecution	<b>IO.8</b> - Confiscation	<b>IO.9</b> - TF investigation & prosecution	<b>IO.10</b> - TF preventive measures & financial sanctions	<b>IO.11</b> - PF financial sanctions	
<b>Substantial</b>	<b>High</b>	<b>High</b>	<b>High</b>	<b>High</b>	

### Technical Compliance Ratings

(C - compliant, LC - largely compliant, PC - partially compliant, NC - non compliant)

<b>R.1</b> - assessing risk & applying risk-based approach	<b>R.2</b> - national cooperation and coordination	<b>R.3</b> - money laundering offence	<b>R.4</b> - confiscation & provisional measures	<b>R.5</b> - terrorist financing offence	<b>R.6</b> - targeted financial sanctions - terrorism & terrorist financing
<b>PC</b>	<b>C</b>	<b>LC</b>	<b>LC</b>	<b>C</b>	<b>LC</b>
<b>R.7</b> - targeted financial sanctions - proliferation	<b>R.8</b> - non-profit organisations	<b>R.9</b> - financial institution secrecy laws	<b>R.10</b> - Customer due diligence	<b>R.11</b> - Record keeping	<b>R.12</b> - Politically exposed persons
<b>LC</b>	<b>LC</b>	<b>C</b>	<b>PC</b>	<b>LC</b>	<b>PC</b>
<b>R.13</b> - Correspondent banking	<b>R.14</b> - Money or value transfer services	<b>R.15</b> - New technologies	<b>R.16</b> - Wire transfers	<b>R.17</b> - Reliance on third parties	<b>R.18</b> - Internal controls and foreign branches and subsidiaries
<b>LC</b>	<b>LC</b>	<b>LC</b>	<b>PC</b>	<b>LC</b>	<b>LC</b>
<b>R.19</b> - Higher-risk countries	<b>R.20</b> - Reporting of suspicious transactions	<b>R.21</b> - Tipping-off and confidentiality	<b>R.22</b> - DNFBPs: Customer due diligence	<b>R.23</b> - DNFBPs: Other measures	<b>R.24</b> - Transparency & BO of legal persons
<b>LC</b>	<b>PC</b>	<b>C</b>	<b>NC</b>	<b>NC</b>	<b>NC</b>
<b>R.25</b> - Transparency & BO of legal arrangements	<b>R.26</b> - Regulation and supervision of financial institutions	<b>R.27</b> - Powers of supervision	<b>R.28</b> - Regulation and supervision of DNFBPs	<b>R.29</b> - Financial intelligence units	<b>R.30</b> - Responsibilities of law enforcement and investigative authorities
<b>PC</b>	<b>LC</b>	<b>C</b>	<b>NC</b>	<b>C</b>	<b>C</b>
<b>R.31</b> - Powers of law enforcement and investigative authorities	<b>R.32</b> - Cash couriers	<b>R.33</b> - Statistics	<b>R.34</b> - Guidance and feedback	<b>R.35</b> - Sanctions	<b>R.36</b> - International instruments
<b>LC</b>	<b>C</b>	<b>LC</b>	<b>LC</b>	<b>LC</b>	<b>LC</b>
<b>R.37</b> - Mutual legal assistance	<b>R.38</b> - Mutual legal assistance: freezing and confiscation	<b>R.39</b> - Extradition	<b>R.40</b> - Other forms of international cooperation		
<b>LC</b>	<b>LC</b>	<b>LC</b>	<b>C</b>		



## MUTUAL EVALUATION REPORT

### *Preface*

This report summarises the AML/CFT measures in place in the United States (U.S.) as at the date of the on-site visit. It analyses the level of compliance with the *FATF 40 Recommendations* and the level of effectiveness of the U.S.'s anti-money laundering/counter-terrorist financing (AML/CFT) system, and recommends how the system could be strengthened.

This evaluation was based on the *2012 FATF Recommendations*, and was prepared using the *2013 Methodology*. The evaluation was based on information provided by the U.S., and information obtained by the evaluation team during its on-site visit to the U.S. from 18 January to 5 February 2016.

The evaluation was conducted by an assessment team consisting of:

- Ms Liz Atkins, PSM, Australian Transaction Reports & Analysis Centre (AUSTRAC), Australia (financial expert)
- Mr. Nicolas Burbidge, Office of the Superintendent of Financial Institutions (OSFI), Canada (financial expert)
- Ms Violaine Clerc, Banque de France, France (financial expert)
- Mr. Bill Peoples, Legal Services, New Zealand Police (law enforcement expert)
- Mr. Jeremy Rawlins, Financial Conduct Authority (FCA), U.K. (legal expert)
- Mr. Jesús Santiago Fernández García, Guardia Civil, Servicio Ejecutivo de Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), Spain (law enforcement expert)
- Ms Valerie Schilling, Senior Policy Analyst, and Ms Marion Ando and Mr. Ashish Kumar, Policy Analysts, FATF Secretariat, and
- Mr. Eliot Kennedy, Deputy Executive Secretary, Asia/Pacific Group on Money Laundering (APG) Secretariat

The report was reviewed by: Mr. Jean Denis Pesme, World Bank; Mr. Sanjeev Singh, Department of Income Tax, Government of India; and Mr. Andrew Theo Strijker, European Commission Secretariat General.

The U.S. previously underwent a FATF Mutual Evaluation in 2006, conducted according to *the 2004 FATF Methodology*. The 2006 evaluation and the subsequent follow-up reports have been published and are available at the [FATF website](#).

U.S.'s 2006 Mutual Evaluation concluded that the U.S. was compliant with 15 Recommendations; largely compliant with 28; partially compliant with 2; and non-compliant with 4. The U.S. was rated compliant or largely compliant with 15 of the 16 Core and Key Recommendations (with PC rating for key recommendation 5). The U.S. was placed under the regular follow-up process immediately after

the adoption of its 3<sup>rd</sup> round Mutual Evaluation Report. Due to its failure to address deficiencies related to old Recommendation 5 of the *2003 FATF Recommendations*, the U.S. remains in the mutual evaluation follow-up process.

## CHAPTER 1. ML/TF RISKS AND CONTEXT

1

31. The U.S. is the third largest country in the world both by area (9.8 million square kilometres) and population (321 million people): *CIA World Fact Book*. The U.S. comprises 50 States, the District of Columbia, and 16 territories of which five are inhabited: American Samoa, Guam, Northern Marianas, Puerto Rico, and the U.S. Virgin Islands. The continental U.S. is bordered by Canada to the north and Mexico to the south. The U.S. population is generally well-educated with over 81% living in urban areas. The U.S. has one of the largest immigrant populations in the world (over 14% of the national population): *Education at a Glance 2015* (OECD). Among OECD nations, the U.S. has one of the highest average household and employee income, with an average GDP of USD 54 800 per capita. The U.S.'s GDP was estimated to be USD 17.91 trillion as of June 2015.

32. The U.S. has a Federal system of government comprised of legislative, executive and judicial branches whose respective powers are determined by the U.S. Constitution. Congress is the legislative branch (comprised of the House of Representatives and the Senate), the executive branch is headed by the President, and the Federal courts (including the Supreme Court) comprise the judicial branch. The approval of both chambers of Congress and the President are required to approve any legislation. Both the Federal and State levels of government have criminal law powers. Federal criminal law effectively supersedes State criminal law. The Federal government has full jurisdiction over the District of Columbia and the U.S. territories.

33. The States have historically exercised "police powers" to make laws relating to public safety and welfare, including criminal laws; however, there are certain areas in which the Congress is constitutionally permitted to legislate, such as on matters affecting interstate or foreign commerce. Due to the international nature of both the financial system and serious crime and terrorism, the Federal Government has taken the primary role in law making and enforcement in the areas of money laundering (ML) and terrorist financing (TF). State laws can be pre-empted when Congress explicitly includes a pre-emption clause, when a State law conflicts with a Federal law, and when the States are precluded from regulating conduct in a field that Congress has determined must be regulated exclusively by Federal authorities.

### *ML/TF risks and Scoping of Higher Risk Issues*

#### *(a) Overview of ML/TF Risks*

34. This section of the report presents a summary of the assessors' understanding of the ML and TF risks in the U.S. Overall, the U.S. faces significant risks from TF and is vulnerable to such abuse because of the unique scope, openness and reach of its financial system globally, and the direct threat posed by terrorists to U.S. interests: *2015 National Terrorist Financing Risk Assessment* (NTFRA), p.11-14. The global dominance of the U.S. dollar generates trillions of dollars of daily transaction volume through U.S. banks which also creates significant exposure to potential ML activity: *National Money Laundering Risk Assessment* (NMLRA), p.34. The widespread use of U.S. currency abroad and the important role that the U.S. financial sector plays in the global financial system leave it significantly exposed to risks of cross-border illicit flows, including bulk cash

smuggling, and the placement, layering or integration of illicit proceeds generated out of domestic and foreign predicate offenses: NMLRA, p.32-35.

35. The United Nations Office on Drugs and Crime (UNODC) estimated proceeds from all forms of financial crime in the U.S., excluding tax evasion, was USD 300 billion in 2010 (about 2% of the U.S. economy)<sup>1</sup>. Fraud (including healthcare fraud, identity theft, tax fraud, mortgage fraud, retail and consumer fraud and securities fraud) generates the largest volume of illicit proceeds, particularly healthcare fraud against the Federal government which accounts for approximately USD 80 billion annually. Other major sources of proceeds are drug trafficking (generating about USD 64 billion annually) and transnational organized crime: NMLRA, p.3-4.

36. The U.S. is an attractive destination for domestic and foreign proceeds at the integration stage. U.S. legal persons are vulnerable due to serious gaps in the legal framework (in particular, no requirement to systematically make beneficial ownership information (either through the incorporation or the banking processes<sup>2</sup>) available to law enforcement agencies (LEAs) and for these reasons this vulnerability is very significant. The risks are magnified by the fact that certain businesses and professions—lawyers, accountants, company formation agents, most trustees (aside from trust companies) and real estate agents (most notably, high-end real estate agents and other market actors) are not subject to comprehensive AML/CFT requirements. The vulnerabilities are further amplified by contextual factors (the enormous size of the U.S. economy and the large number of companies formed in the U.S.). Although, as in many countries, most companies are established in the U.S. for legitimate purposes, there are numerous examples of legal persons misused in complex ML and TF schemes. To a much lesser extent, trusts have been identified in complex ML schemes, but there is currently no estimate of the number, size and/or activity of U.S. trusts as these are not created by governments. Another vulnerability is that not all investment advisers are implementing comprehensive AML/CFT requirements.

### (b) Country's risk assessment

37. In 2015, the U.S. published: the *2015 NMLRA* which follows up from the *2005 National Money Laundering Threat Assessment* (the 2005 NMLTA) and a series of national ML strategies produced by the Treasury and DOJ (at the direction of Congress) from 1999 to 2003 and in 2007<sup>3</sup>; and the *2015 NTFRA* which is the country's first publicly available TF risk assessment. Both were prepared by the Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) in consultation with a wide range of other relevant competent authorities (including intelligence, law enforcement and regulatory agencies), using terminology and a methodology based on the 2013 *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment: NMLRA*, p.6-9, *NTFRA*, 6-10. The NMLRA and NTFRA identify (but do not quantify) particular areas of *residual risk*— by which the U.S. authorities mean whatever ML/TF risk remains once mitigation measures have been applied to

<sup>1</sup> *Estimating Illicit Financial Flows Resulting From Drug Trafficking and other Transnational Organized Crimes*, UNODC, October 2011, [www.unodc.org/documents/data-and-.../Illicit\\_financial\\_flows\\_2011\\_web.pdf](http://www.unodc.org/documents/data-and-.../Illicit_financial_flows_2011_web.pdf)

<sup>2</sup> Since the on-site, the Final CDD Rule on BO was issued on 5 May 2016. The implementation period for the Rule is two years, [www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx](http://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx)

<sup>3</sup> See the [FinCEN website](http://fincen.treasury.gov) for the National ML Strategies from 1999, 2000, 2001, 2002, 2003 and 2007.



address inherent risks. Both NMLRA and NTFRA define terms ‘threat’, ‘vulnerability’, ‘consequence’ and ‘risk.’ The NMLRA does not examine, systemically, the vulnerabilities of the DNFBP sectors, apart from casinos.

38. **The NMLRA** identifies serious ML threats in five categories of predicate crime: fraud (particularly healthcare fraud, identity theft, tax fraud, mortgage fraud, retail and consumer fraud, and securities fraud), drug trafficking, human smuggling, organized crime, and public corruption (both domestic and foreign). The report also identifies ML vulnerabilities and cites case examples involving the use of: cash (particularly bulk cash smuggling and trade-based ML); the misuse of correspondent accounts and nominee account holders; money services businesses (MSBs), and unlicensed MSBs; casinos and the securities sector, including investment advisers (IAs) and the misuse of legal entities. The NMLRA concludes that the underlying ML vulnerabilities remain largely the same as those identified in the 2005 NMLTA (p.3). However, as noted above the NMLRA does not specifically assess DNFBP sector vulnerabilities aside from casinos. **The NTFRA** identifies serious TF vulnerabilities and risks from: raising funds through criminal activity, individuals raising funds under the auspices of charitable giving but outside of any charitable organization, individual contributions and self-funding; moving and placing funds through banks, licensed MSBs, unlicensed money transmitters and cash smuggling; and potential emerging threats from global terrorist activities, cybercrime and identity theft, and new payment systems.

39. A wide array of other national risk assessments have also been undertaken and used to support strategies to combat terrorism, major proceeds generating predicate offenses, and related ML/TF. These risk assessments are not public, but underpin published national strategies and contain useful information on related ML/TF risks. This process is led at the highest level of government by two agencies within the Executive Office of the President: the National Security Council (NSC) and the Office of National Drug Control Policy (ONDCP), with participation of other agencies. For example, see *National Security Strategy 2010*, *National Drug Control Strategy 2014*, *National Strategy to Combat Transnational Organized Crime 2011*, and *National Strategy for Counter Terrorism 2011* prepared by NSC. See also *National Southwest Counternarcotics Strategy 2013*, and *National Northern Border Counternarcotics Strategy 2014* prepared by ONDCP. Although the assessors did not have access to these confidential risk assessments, they did have the opportunity to discuss these issues extensively with the authorities.

40. Overall, the conclusions of the NMLRA and NTFRA are generally reasonable, and appear to be consistent with those reflected in the above-noted national strategies, which themselves are reasonable and supported by confidential national risk assessments that specifically address related ML/TF risks.

### (c) *Scoping of higher-risk issues*

41. In deciding what issues to prioritize for increased focus, the assessors reviewed material provided by the U.S. on national ML/TF risks (as outlined above), and information from reliable third

party sources (e.g. reports of other international organizations)<sup>4</sup>. The following list of priority issues is broadly consistent with the issues identified in the national risk assessments:

- a) **Terrorism financing** represents a significant threat to the U.S. given the unique reach of its financial system and the direct threat posed by terrorists who have successfully attacked U.S. interests both at home and abroad: NTFRA p.11-14. The assessors focused on the effectiveness of the U.S. approach to combat TF, including its ability to effectively monitor MSBs, prevent the misuse of NPOs, swiftly apply targeted financial sanctions, and the impact of measures to minimize the use of unlicensed MSBs and cash couriers.
- b) **Beneficial ownership**: The lack of beneficial ownership (BO) requirements was identified in the previous mutual evaluation as a serious deficiency. The NMLRA identifies the misuse of legal entities in complex ML schemes: NMLRA p.41-43. The assessors focused on: the extent to which gaps in the legal framework affect competent authorities' ability to access adequate and accurate BO information in a timely manner, and respond to international requests related to BO; the extent to which the volume and relative ease of company formation in the U.S., and the perceived credibility of companies and legal arrangements incorporated in the U.S. impacts the risk of them being abused for ML/TF; and measures that may compensate for lack of access to BO information by competent authorities, FIs and DNFBPs.
- c) **Fraud**: According to the NMLRA (p.10-13), fraud encompasses a number of distinct crimes, including healthcare fraud against the Federal government, tax fraud and securities fraud, which together generate the largest volume of illicit proceeds in the U.S. of any predicate crime type. The assessors focused on the extent to which the laundering of the proceeds of such fraud is being successfully investigated, prosecuted, and confiscated. The assessors also went beyond simple tax fraud to examine the handling of tax crime predicates overall both at domestic and foreign level.
- d) **Illegal Drug Trade**: The NMLRA (p.13-16) identifies drug trafficking as an important predicate for ML, with the south-west border being a major transit point of drugs into the U.S. market and a route of profits back to drug trafficking organizations with subsequent repatriation of U.S. currency. As a lucrative business, the drug trade has also been exploited by terrorist groups to raise finances. The assessors focused on the extent to which the laundering of the proceeds of drug offenses is being successfully investigated, prosecuted and confiscated and on the measures undertaken to combat ML/TF related to drug trafficking. Particular attention was given to bulk cash smuggling, including the identification and detection of illegal cash couriers, and the monitoring of commercial cash couriers.

<sup>4</sup> Including the *Financial Sector Assessment Program - Financial System Stability Assessment of the United States* (IMF, 2015), [www.imf.org/external/pubs/ft/scr/2015/cr15170.pdf](http://www.imf.org/external/pubs/ft/scr/2015/cr15170.pdf); the *Phase 3 Report on Implementing the OECD Anti-Bribery Convention in the United States* (OECD, 2010); *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (UNODC, 2013); *The Puppet-Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It* (World Bank and UNODC Stolen Asset Recovery Initiative, 2011), <https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf>; and *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes* (UNODC, 2011), [www.unodc.org/documents/data-and-analysis/Studies/Illicit\\_financial\\_flows\\_2011\\_web.pdf](http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf)

- e) **Organized crime:** The NMLRA (p.17-20) acknowledges that transnational organized crime groups from all over the world operate in the U.S. and generate vast amounts of illegal proceeds from a wide range of criminal activities including extortion, illegal gambling, kidnapping, loan sharking, murder, prostitution, fraud, racketeering and the illegal drug trade. The assessors focused on the extent to which the laundering of the proceeds of offenses related to organized crime is being successfully investigated, prosecuted and confiscated and on the effectiveness of measures to combat ML related to the activity of transnational organized crime groups.
  - f) **Role of the U.S. in the global financial system:** As noted in the IMF's *Financial Sector Assessment Program-Financial System Stability Assessment of the U.S. (2015)*, the "interconnectedness of the U.S. system with the rest of the world remains key for global stability (...) The U.S. financial sector is one of four jurisdictions at the core of the world's bank networks, as well as at the core of the equity market, debt market, and price correlation networks". The size, complexity and international reach of the U.S. financial system, and its innovative environment for new products, services and delivery mechanisms to facilitate the free flow of capital create significant ML/TF vulnerabilities. In particular, the U.S. financial system faces significant risks of abuse for the placement, layering or integration of illicit proceeds generated out of domestic and foreign predicate offenses, including tax crime and foreign corruption, as is documented in the NMLRA. The assessors focused on how effectively the U.S. is able to mitigate these risks through the domestic AML/CFT legal and regulatory framework, with particular attention to the coverage of foreign predicates.
  - g) **ML/TF risks of the minimally covered DNFBP sectors:** Many DNFBPs are not covered by (or are exempted from) comprehensive AML/CFT preventive measures. The NMLRA notes that some DNFBPs have been abused for ML. The assessors focused on the ML/TF risks associated with DNFBPs not subject to comprehensive AML/CFT preventive measures, and considered whether and to what extent the U.S. is able to effectively mitigate vulnerabilities through LEA activity. Particular focus was placed on the roles of company formation agents (CFAs) and the facilitating roles of lawyers and accountants, coupled with the vulnerability of the high-end real estate agent sector and the role played by RMLOs in the mass real estate financing market.
  - h) **Effectiveness of operational coordination and cooperation:** Given the challenges posed by the complexity and sheer size of the U.S., the assessors focused on how effectively Federal and State authorities coordinate and cooperate at the operational level. This approach touched upon: the effectiveness of financial intelligence analysis and flows at all levels; financial crime task forces; inter-State supervision of MSBs and the effective coordination and sharing of information amongst banking supervisors; and the extent to which enforcement and supervisory processes work together to achieve supervisory and enforcement outcomes.
42. Through the scoping exercise, the assessors identified the following areas for lesser focus:
- a) **Notaries** have a very limited role in the U.S. They are appointed by State governments to witness the signing of important documents (verifying the identity of the signer, but not the role of the individual) and to administer oaths. They conduct none of the activities

listed in Recommendations 22 and 23, and are not covered under the domestic AML/CFT framework.

- b) **Technical compliance of DNFBPs not subject to comprehensive AML/CFT measures:** A number of DNFBPs that do perform activities listed in Recommendations 22 and 23 (real estate agents, trust and company service providers, lawyers and accountants) are not subject to comprehensive AML/CFT measures. Consequently, the assessors did not focus on technical compliance issues associated with these sectors during the on-site visit, but did meet with representatives of these sectors to examine the extent to which they understand their ML/TF risks and what risk mitigation measures may be in place.

### *Materiality*

43. The U.S. has the world's largest economy with an annual gross domestic product (GDP) of around USD 17.9 trillion<sup>5</sup>. It has a developed, industrialized, free-market economy with the world's largest consumer market (consumer spending comprises over 70% of the U.S. economy). The U.S. is one of the world's largest trading nations, and is the world's second largest manufacturer representing about one fifth of global output. It is also rich in natural resources, and the world's largest producer of oil and natural gas.

44. The U.S. financial system is large and highly diversified. Before the global financial crisis, total U.S. financial assets amounted to almost four and a half times the size of GDP, less than a quarter of which was accounted for by traditional depository institutions. Since the 2008 crisis, the shape of the U.S. financial system has radically changed. The top investment banks were reconfigured as bank holding companies, non-banks were severely weakened, the Government-sponsored housing enterprises are now in government conservatorship, and private securitization remains dormant<sup>6</sup>. Despite these changes, the U.S. financial sector remains the largest in the world and very diverse. The wealth management sectors (investments, securities, insurance) are very large. The U.S. began recovering from the global financial crisis in late 2009, and in 2015 showed a real growth rate of 2.6% of GDP<sup>7</sup>: In 2015, the U.S. exported over USD 1.5 trillion worth of goods including machinery, electronic equipment, aircraft and spacecraft, vehicles and oil. Its largest trading partners (in order of importance) are Canada, China, Mexico, Japan, Germany, South Korea, United Kingdom and France.

### *Structural Elements*

45. The U.S. has all of the key structural elements for an effective AML/CFT system including political and institutional stability, governmental accountability, rule of law, and a professional and independent bar and judiciary at both the Federal and State levels. Corruption is identified as a threat in the NMLRA and combating it is a high priority of U.S. law enforcement authorities.

<sup>5</sup> All references to currency in this report are in U.S. dollars (USD), unless stated otherwise.

<sup>6</sup> *United States Financial Stability Assessment Program Report on Standards and Codes* (IMF 2010), p.5, [www.imf.org/external/np/fsap/fsap.aspx](http://www.imf.org/external/np/fsap/fsap.aspx)

<sup>7</sup> *CIA World Fact Book. 2015*, [www.cia.gov/library/publications/the-world-factbook/](http://www.cia.gov/library/publications/the-world-factbook/)

### *Background and other Contextual Factors*

46. The U.S. was one of the first countries in the world to place a significant focus on ML, and has a mature and highly developed AML/CFT system. Relatively speaking, financial exclusion is not a serious issue. As of 2014, almost 94% of the U.S. population over the age of 15 had accounts at FIs (up from 88% in 2011), and over 75% of the population had debit cards: *Global Findex 2014* (World Bank). The U.S. is a significant source of outgoing remittances, primarily due to its large immigrant population (almost USD 56.3 billion outgoing remittances, and over USD 6.9 billion incoming remittances in 2014): *Migration and remittances data* (World Bank).

#### *(a) AML/CFT strategy*

47. The U.S. considers AML/CFT to be a pillar of its national security strategy and of a strong financial system. The government's top priority is to disrupt terrorism and its financing before it touches the U.S. and its financial system. Combating ML is another top priority, with the authorities aggressively pursuing a "follow the money" approach aimed at disrupting and dismantling organized crime groups and their financing networks. The U.S. AML/CFT strategy focuses on three major goals: (1) to more effectively cut off access to the international financial system by money launderers and terrorist financiers; (2) to enhance the Federal government's ability to target major TF and ML organizations and systems; and (3) to strengthen and refine the AML/CFT regime for financial services providers to improve the effectiveness of compliance and enforcement efforts and to prevent and deter abuses. Combating the proliferation of weapons of mass destruction (WMD) and its financing is also a priority.

#### *(b) Legal & institutional framework*

48. The legal framework of AML/CFT preventive measures is set out in Federal legislation. The Bank Secrecy Act (BSA), as amended by the USA PATRIOT Act sets out the main AML/CFT requirements which apply to covered FIs and DNFBPs, regardless of their Federal or State registration/status. ML and TF are criminalised at the Federal level and some States have separately criminalized ML/TF. Only the State of New York has its own TF legislation. However, ML and TF are primarily pursued at the Federal level.

49. The institutional framework for AML/CFT is complex, multi-faceted and involves a significant number of authorities from a range of ministries. **Department of Treasury (Treasury)** is the lead AML/CFT agency, and is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the U.S. **Department of Justice (DOJ)** is the principal government entity responsible for investigating and prosecuting ML/TF offenses. **Department of Homeland Security (DHS)** is responsible for national security, including investigating ML and the prevention of terrorism. **Department of State** is responsible for U.S. foreign policy. **Department of Health and Human Services (DHHS)** is responsible for enhancing and protecting the health of Americans, and plays a role in combating healthcare fraud and related ML. **Department of Commerce** is involved in export control and plays a role in countering the financing of proliferation of weapons of mass destruction (WMD).



50. In addition to the key ministries noted above, the main policy-making bodies in the area of AML/CFT and counter-proliferation are:

- a) National Security Council (NSC) (within the Executive Office of the President) comprised of the President's senior national security advisors and cabinet officials. Its staff coordinate the national security strategy development process which includes considering relevant illicit finance risks as they pertain to transnational organized crime, terrorism, and WMD proliferation: 50 U.S. Code §402.
- b) Office of National Drug Control Policy (ONDCP) (within the Executive Office of the President) which develops the National Drug Control Strategy and related strategies, and evaluates the effectiveness of the strategies' implementation<sup>8</sup>.
- c) Office of Terrorism and Financial Intelligence (TFI) (within Treasury) responsible for developing/implementing national AML/CFT strategies, and overseeing implementation of the nation's economic sanctions laws/programs developed by Treasury's Office of Foreign Assets Control (OFAC) and the Department of State's Bureau of Counterterrorism.
- d) Office of Terrorist Financing and Financial Crime (TFFC) (within Treasury TFI) which is responsible for AML/CFT policy and strategy functions, and heads the U.S. delegation to the FATF and FATF-style regional bodies (FSRBs).

51. At the operational level, there are numerous agencies handling intelligence analysis, investigations, prosecutions, regulation and supervision. Specialised units/initiatives are described later in the report where relevant to the analysis of effectiveness in particular areas. The following are the **key intelligence agencies**. See also the description of **SAR Review Teams**, **Financial Crime Task Forces**, and **Fusion Centres** described in IO.1 (Core Issue 1.4) and IO.6 (Core Issue 6.1 and 6.4):

- a) **Financial Crimes Enforcement Network (FinCEN)** (within Treasury TFI) is the financial intelligence unit (FIU) and is also the administrator of the BSA.
- b) **Treasury's Office of Intelligence and Analysis (OIA)** (within Treasury TFI) is Treasury's intelligence analysis branch. Its priorities are to identify and attack the financial infrastructure of terrorist groups, and the vulnerabilities that terrorists/criminals may exploit in domestic/international financial systems. OIA is also tasked with identifying and attacking the financial infrastructure of proliferation networks, organized crime groups, and drug trafficking organizations. By creating OIA, Treasury became the world's first finance ministry with in-house intelligence and analytical expertise to develop sanctions designations, and support other preventative and enforcement actions to combat ML/TF and WMD proliferation.
- c) **National Counter Terrorism Center (NCTC)** integrates and analyses all intelligence pertaining to terrorism possessed or acquired by the U.S. government (except purely

<sup>8</sup> See the *Office of National Drug Control Policy Reauthorization Act of 2006*, [www.congress.gov/109/plaws/publ469/PLAW-109publ469.pdf](http://www.congress.gov/109/plaws/publ469/PLAW-109publ469.pdf); the *Government Performance and Results Act Modernization Act of 2010* [www.whitehouse.gov/omb/performance/gprm-act](http://www.whitehouse.gov/omb/performance/gprm-act); and the *ONDCP FY 2015 Budget and Performance Summary*.



domestic terrorism), and provides all-source intelligence support to government-wide counterterrorism activities.

- d) **Department of Homeland Security Office of Intelligence and Analysis (DHS I&A)** is responsible for: developing DHS-wide intelligence through managing the collection, analysis and fusion of intelligence throughout DHS; disseminating intelligence throughout DHS, the U.S. Intelligence Community, and first responders at the State, local, and tribal level; tracking terrorists and their networks; and assessing threats to critical American infrastructures, biological and nuclear terrorism, pandemic diseases, the U.S. borders (air, land, and sea), and radicalization within American society.
- e) **Special Operations Division (SOD)** (within DEA) is a multi-agency coordination center designed to identify significant international and domestic drug trafficking and ML organizations. It supports multi-jurisdiction/-nation and /-agency wire intercept investigations, and works jointly with Federal, State and local agencies to coordinate overlapping investigations, ensuring that tactical and strategic intelligence is de-conflicted and shared between LEAs.
- f) **Department of State, Bureau of Counterterrorism** has the authority to designate Foreign Terrorist Organizations under section 219 of the *Immigration and Nationality Act*, and shares authorities with the Treasury to designate individuals and entities under E.O. 13224.
- g) **National Counter Proliferation Center (NCPC)** (within the Office of the Director of National Intelligence-ODNI) centralizes the work and collaboration of 17 U.S. intelligence agencies regarding proliferation intelligence. It also works closely with the NCTC on combating WMD proliferation and terrorism, including by helping the intelligence community understand counter-proliferation financing.

52. The main Federal LEAs and investigative bodies with AML/CFT responsibilities are:

- a) **Federal Bureau of Investigation (FBI)** (within DOJ) is the primary agency responsible for investigating over 200 Federal crimes including terrorism and ML. **FBI-Terrorist Financing Operations Section (FBI-TFOS)** (within FBI's wider counterterrorism division) investigates attempts by terrorists and terrorist organizations to raise, move, and use funds in the U.S., and provides financial investigative support to FBI counterterrorism investigations.
- b) **Drug Enforcement Administration (DEA)** (within DOJ) investigates illicit drug trafficking and associated ML.
- c) **Organized Crime Drug Enforcement Task Force (OCDETF)** (within DOJ) operates nationwide and coordinates multi-agency<sup>9</sup> and multi-jurisdictional investigations targeting the most serious drug trafficking threats, including the financial infrastructures supporting

<sup>9</sup> The participants involved include: 94 U.S. Attorneys' Offices; Bureau of Alcohol, Tobacco, Firearms and Explosives; DEA; FBI; IRS-CI; U.S. Coast Guard; ICE; U.S. Marshals Service; Criminal and Tax Divisions of DOJ; and numerous State & local agencies.

these organizations. The OCDETF allocates resources partly on the basis of how successfully participants focus their efforts on the Consolidated Priority Organization Targets (CPOTs) and Regional Priority Organization Targets (RPOTs): *FY 2015 Interagency Crime and Drug Enforcement Congressional Budget Submission*.

- d) **Internal Revenue Service Criminal Investigation (IRS-CI)** (within Treasury) is the enforcement arm of the Internal Revenue Service, the U.S. federal tax authority. In addition to investigating criminal violations of the tax code, IRS-CI investigates complex, high-profile financial crimes including corporate fraud, FI fraud, ML, public corruption, and TF.
  - e) **Immigration and Customs Enforcement (ICE)** (within DHS) is responsible for enforcing Federal laws related to governing border control, customs, trade and immigration. Within ICE, the **Homeland Security Investigations division (ICE-HSI)** investigates all types of cross-border criminal activity, including financial crimes, ML and bulk cash smuggling. **Customs and Border Protection (CBP)** (within DHS) is responsible for controlling the U.S. border at/between official ports of entry, has authority to search outbound/inbound shipments, and works with ICE to seize contraband, currency and monetary instruments.
  - f) **El Dorado Task Force (EDTF)** targets financial crime and ML in the New York and New Jersey metropolitan area. It is ICE-HSI-led and brings together 250 staff and 13 investigative teams of analysts, LEAs, and prosecutors from 44 Federal, State, and local LEAs.
  - g) **Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF)** (within DOJ) investigates violations of Federal laws on firearms, explosives, arson, and alcohol and tobacco diversion.
  - h) **U.S. Coast Guard** (within DHS) patrols and controls access to the U.S. coast.
  - i) **U.S. Secret Service (USSS)** (within DHS) is responsible for preventing and investigating counterfeiting of U.S. currency and U.S. Treasury securities, and investigating cybercrimes.
  - j) **U.S. Postal Inspection Service (USPIS)** is the law enforcement arm of the U.S. Postal Service (USPS) with jurisdiction over crimes that may adversely affect or fraudulently use the U.S. mail. Postal Service money orders are a payment method used by money launderers and international criminal organizations.
53. The main Federal authorities responsible for AML/CFT prosecutions and related activity are:
- a) **United States Attorney's Offices (USAO)** (within DOJ) prosecute criminal cases and bring lawsuits on behalf of the U.S. They are complemented by a relatively smaller number of trial attorneys, based at Main DOJ in Washington, DC. There are 94 USAOs, and 93 presidentially appointed U.S. Attorneys, who act as the chief Federal law enforcement officer in their districts, and oversee roughly 6,075 Assistant U.S. Attorneys, about 4,800 of whom do criminal prosecution.
  - b) **Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS)** (within DOJ) prosecutes and coordinates complex, sensitive and multi-district and international

ML and asset forfeiture investigations and cases. It also provides legal and policy assistance and training to Federal, State and local prosecutors and law enforcement personnel, as well as to foreign governments and in multilateral forums, and manages DOJ's Assets Forfeiture Fund.

- c) **Counterterrorism Section, National Security Division (CTS) (within DOJ)** supports investigations and prosecutions of international and domestic terrorism.

54. Main authorities for managing targeted financial sanctions and seized assets are:

- a) **Office of Foreign Assets Control (OFAC)** (within Treasury TFI) administers and enforces targeted financial sanctions against both terrorism and proliferation, and other economic/trade sanctions based on U.S. foreign policy/national security goals.
- b) **Treasury Executive Office for Asset Forfeiture (TEOAF)** (within Treasury TFI) administers the Treasury Forfeiture Fund (TFF).
- c) **U.S. Marshals Services (USMS)** (within DOJ) manages seized assets and the sale of forfeiture of assets for the Asset Forfeiture Fund (DOJ-AFF).

55. The U.S. financial sectors are regulated by several Federal and State regulatory bodies. The main authorities responsible for supervising AML/CFT compliance in the banking sector are:

- a) **FinCEN** is the primary AML/CFT regulator responsible for developing, issuing, administering and civilly enforcing regulations implementing the BSA (in addition to its FIU role).
- b) **Board of Governors of the Federal Reserve System** (BGFRS-the U.S. central bank) and its 12 Federal Reserve Banks (**Federal Reserve**) supervises and examines State-chartered banks that elect to become members of the Federal Reserve System (State member banks), bank holding companies (BHCs), Edge and Agreement corporations, and uninsured U.S. State-chartered branches and agencies of foreign banking organizations.
- c) **Federal Deposit Insurance Corporation (FDIC)** is the deposit insurer for all depository institutions (about 6,200) other than credit unions, and the primary Federal supervisor for State-chartered banks & savings institutions not members of the Federal Reserve System.
- d) **Office of the Comptroller of the Currency (OCC)** is an independent bureau within Treasury that charters, regulates, and supervises national banks, Federal savings associations and the U.S. Federal branches and agencies of foreign banking organizations.
- e) **National Credit Union Administration (NCUA)** charters, supervises, and regulates Federally-chartered credit unions. It operates and manages the National Credit Union Share Insurance Fund, insuring the deposits in all Federal credit unions and the majority of State-chartered credit unions (about 6,021 in total).
- f) **Federal Banking Agencies (FBAs)** are collectively defined for the purposes of this report as including the BGFRS, the OCC, the FDIC, and the NCUA. The BGFRS, OCC, and FDIC have authority under the *Federal Deposit Insurance Act* (FDI Act) to supervise for and enforce

compliance with the BSA within their supervised institutions. The NCUA has the same authority under the Federal Credit Union Act (FCUA).

- g) **State Banking Regulators:** Each State charters banks and shares supervisory responsibility over some banks, where required, through Joint Supervisory Agreements with the Federal Reserve and FDIC. Most States also charter and examine credit unions and share supervision with the NCUA.

56. The main authorities responsible for supervising AML/CFT compliance in the securities and futures and derivatives sectors are:

- a) **Securities and Exchange Commission (SEC)** is the Federal regulator of the securities markets. It regulates and oversees key participants in the securities industry, including securities exchanges, securities broker-dealers, IAs, investment companies and the Self-Regulatory Organizations' (SROs) compliance with their statutory obligations under the U.S. Federal securities laws.
- b) **Commodity Futures Trading Commission (CFTC)** is the Federal regulator for derivatives, commodity futures, options on futures, commodity options and swaps. It also oversees the operations of the National Futures Association.
- c) **National Futures Association (NFA)** is the SRO for the futures market. Membership in the NFA is mandatory for anyone conducting business with the public on the U.S. futures exchanges. Approximately 4,200 firms and 55 000 associates are members of the NFA. The CFTC has delegated some regulatory responsibilities to the NFA.
- d) **Financial Industry Regulatory Authority (FINRA)** is an SRO for broker-dealers and regulates both the firms and professionals that sell securities in the U.S and the U.S. securities markets. FINRA oversees more than 3,964 brokerage firms, 161,510 branch offices and 641,144 registered securities representatives. FINRA registers and examines brokerage firm, and enforces its rules and the Federal securities laws.

57. Other authorities have responsibilities for supervising the financial sectors without a Federal functional regulator (FFR), casinos, and non-profit organizations (NPOs):

- a) **IRS Small Business and Self-Employment Division (IRS-SBSE)** (within Treasury) has been delegated examination authority for civil compliance with the BSA for all FIs without a FFR as defined in the BSA, including MSBs (as broadly defined), credit card companies, non-Federally insured credit unions, casinos (tribal and non-tribal) and dealers in precious metals and stones. It also has responsibility for auditing compliance with Form 8300 cash reporting requirements.
- b) **National Indian Gaming Commission (NIGC)** is an independent Federal regulatory agency created by Congress whose primary mission is to regulate gaming activities on Indian lands for the purposes of ensuring that Indian tribes are the primary beneficiaries of gaming revenues, and gaming is conducted fairly and honestly by operators and players. In general, the primary regulators for these activities are the tribal-level regulators themselves.

- c) **Tribal-level regulators:** There are tribal gaming commissions established by the tribes to oversee tribal gaming. Tribal nations have primary regulatory authority over Class II gaming (bingo and similar games of chance). Class III gaming (casino style gaming) is only lawful on Indian lands if the relevant State permits such gaming, if the tribe's governing body authorises it in an ordinance or resolution approved by the NIGC Chairman, and such gaming is conducted in conformity with a Tribal-State compact (i.e. an agreement between a State and a tribe, approved by the Secretary of the Interior, governing the conduct of Class III gaming). Although the terms of Tribal-State compacts vary by State, in most instances the tribes remain the primary regulator for Class III gaming.
- d) **State-level regulators** regulate insurance companies, MSBs and non-tribal casinos for: consumer protection and (in the case of insurance companies) for safety and soundness; and examine for compliance with BSA AML/CFT obligations in coordination with FinCEN, IRS-SBSE, and the FFRs.
- e) **IRS Tax Exempt and Government Entities Division (IRS-TEGE)** (within Treasury) provides Federal oversight to NPOs in the U.S. through reviewing applications for tax exempt status and subsequent examinations. It ensures that NPOs are filing returns and may use the information from returns to help determine if NPOs are facilitating TF.

58. Competent authorities relevant to combating WMD proliferation and its financing:

- a) **Department of State** coordinates U.S. government interdiction efforts across the policy, enforcement and intelligence communities through four State-chaired inter-agency working groups focused on (i) nuclear; (ii) ballistic missile; (iii) chemical and biological weapons; and (iv) conventional arms interdictions; and a counterproliferation finance team. When engaging countries on shipments of proliferation concern, the groups consider financial aspects (including bank accounts and payments) as appropriate.
- b) **Department of Commerce Bureau of Industry and Security (BIS)** administers and enforces export controls on dual-use and certain munitions items through the Export Administration Regulations (EAR) under authority of the International Emergency Economic Powers Act (IEEPA), works with the exporting community to prevent violations, and conducts investigations to gather evidence supporting criminal and administrative sanctions. It also develops several lists that FIs can use to identify transactions that may involve proliferation financing.
- c) **FBI Counterproliferation Center (CPC)** manages all FBI counterproliferation investigations, identifies critical intelligence gaps and emerging proliferation threats, and develops counterproliferation strategies, in collaboration with Federal partners and the private sector.
- d) **CounterProliferation Investigations Program** (within DHS ICE-HSI) is responsible for overseeing a broad range of investigative activities related to export violations and enforces U.S. export laws involving military items and controlled dual-use goods, as well as products going to sanctioned or embargoed countries.
- e) **Export Enforcement Coordination Center (E2C2)** (within DHS) is the enforcement and intelligence coordination hub for all U.S. agencies with a role in export enforcement, including the LEAs and export control authorities.

- f) **Counterintelligence and Export Control Section (CES)** of NSD supports the investigation and prosecution of individuals and entities for violations of U.S. laws and regulations intended to combat WMD proliferation, including various **CounterProliferation Task Forces** in U.S. Attorneys' Offices across the country.

(c) *Financial sector and DNFBPs.*

59. General information on the size and make-up of the financial and DNFBP sectors:

- a) **Banking sector:** About 13 000 depository institutions of widely varying sizes. About half are banks (the six largest U.S. banks hold over 40% of total domestic deposits). The other half are credit unions (mutually owned and holding slightly less than 10% of total domestic deposits).
- b) **Lending:** Banks offer extensive lending products at the commercial and retail level. Insurance companies offer commercial loans. RMLs of varying size provide mortgage lending in the retail mass market. In addition, a number of other lenders operate in the U.S. such as pawn shops and other unregulated commercial lenders. There is no estimate of the aggregate size of these operations.
- c) **Securities Dealers, Mutual Funds and Investment Advisers:** About 4 100 broker-dealers, 8 100 mutual funds with over USD 15 trillion in assets, nearly 12 100 SEC-registered IAs managing over USD 67 trillion in assets, in addition to 17 000 State-registered IAs and over 325 000 State-registered investment adviser representatives.
- d) **Money services businesses:** 41 788 MSBs registered with FinCEN of which 25 000 reported having agents. Of these, 170 were responsible for more than 230 000 agents, ranging from under 10 agents to tens of thousands of agents per MSB principal. Individuals in the U.S. send about USD 37 billion annually to households abroad. The average remittance value of a transaction from the U.S. to Latin America and Mexico is estimated to be between USD 290 and USD 400 respectively.
- e) **Life Insurance Companies:** 895 life insurance companies employing or otherwise using 1 007 600 agents, brokers and service employees. Life insurance companies provide life insurance services and frequently provide related investment savings services, including annuities.
- f) **Casinos:** Over 1,300 casinos and card rooms across the 42 States that allow some form of casino gambling: American Gaming Association. The 246 tribes with gaming operations had revenues of approximately USD 27 billion in 2012, accounting for more than 70% of the gross gambling revenue at all licensed gaming facilities in the U.S. While tribal gaming operations dominate overall U.S. gaming revenue, Las Vegas and Atlantic City top the list of casino markets with annual revenues of USD 6.2 billion and USD 3 billion respectively.
- g) **Lawyers:** Approximately 1 million lawyers of whom about 400 000 are members of the American Bar Association (ABA), the country's largest bar association. Lawyers are licensed by the State bar associations and are bound by professional codes of ethics. Some maintain bank accounts in their own name for client use (mostly escrow accounts in which clients' funds are held for future transactions).



- h) **Accountants:** Approximately 1.17 million accountants and auditors (including approximately 660 000 Certified Public Accountants (CPAs)), with the sectors of accounting, tax preparation and payroll services generating about USD 137 billion annually. Like lawyers, accountants are licensed professionals but typically do not maintain bank accounts for client funds.
- i) **Real estate agents:** About 394 400 real estate agents. There are also significant numbers of condominium associations and cooperative real estate associations which can impose conditions (including financial conditions) on the purchase and sale of attractive higher value real estate and which act as gatekeepers.
- j) **Dealers in precious metals & stones:** Approximately 200 000 (FinCEN, 2006).
- k) **Trustees:** The exact number of trustees in the U.S. cannot be known as trustee legal arrangements are not registered or subject to supervisory oversight. Any natural person may act as a trustee. In the U.S. the only identifiable group of professional trustees is trust companies, which are FIs with fiduciary (trust) powers to act as trustee. However, the BSA does not impose explicit obligations on trustees. Trust companies are subject to the Covered FI obligations when dealing with clients and this extends to their role as trustees. A minimum of one trustee is required to act in a legal arrangement.
- l) **Company formation agents (CFA):** Although it is not mandatory in the U.S. to use a CFA to incorporate a legal entity, a substantial CFA business sector provides a full range of competitive services to individuals and corporations. CFAs handle approximately half of all incorporations of legal persons in the 56 U.S. incorporating jurisdictions.

(d) *Preventive measures*

60. The cornerstone of the U.S. AML/CFT regime is the *Currency and Foreign Transactions Reporting Act (1970)*, commonly known as the *Bank Secrecy Act (BSA)*, as amended by the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001)* (the USA PATRIOT Act), and detailed implementing sector-specific regulations. The BSA and its implementing regulations set out sector-specific CDD, record-keeping, suspicious activity reporting and internal control requirements. The USA PATRIOT Act augmented the BSA framework by strengthening customer identification procedures, prohibiting FIs from engaging in business with foreign shell banks, requiring FIs to have due diligence procedures and, in some cases, enhanced due diligence (EDD) procedures for foreign correspondent and private banking accounts, and improving information sharing between FIs and the government.

61. The Federal Financial Institutions Examination Council (FFIEC) (comprised now of the BGFRS, the Consumer Financial Protection Bureau (CFPB), the FDIC, the NCUA, the OCC and the State Liaison Committee) was originally established in March 1979 to prescribe uniform principles, standards, and report forms and to promote uniformity in the supervision of FIs. The FFIEC maintains a *Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual* (the FFIEC Manual), which is a 442-page up-to-date guide to examination procedures for FBA examiners. While its application is mandatory for examiners, it also serves as guidance for banks. The FFIEC Manual contains an overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices, and examination procedures. The prescriptive elements of the

Manual (as opposed to those that are clearly "for consideration") are deemed mandatory and considered "enforceable means" for the purposes of this report. Sector regulators such as the SEC and the CFTC use similar manuals. The life insurance sector has included an AML/CFT examination component in the NAIC examination manual used by State insurance supervisors. FinCEN and IRS SBSE have published a similar BSA/AML Examination Manual for MSBs.

*(e) Legal persons and arrangements*

62. The formation of U.S. legal entities<sup>10</sup> is governed by laws in each of the 50 States, the 5 inhabited territories and the District of Columbia. Federal law also applies in certain areas (e.g. criminal law, securities regulation, taxation). There are no precise statistics on the exact number of legal entities in the U.S. Estimates range around 30 million, with about 2 million new formations every year. Delaware is one of the most popular States for company formation and was home to roughly 1.11 million legal persons in 2014, with about 169 000 new formations in that year.

63. Trusts in the U.S. are also governed primarily by State law, whether under legislation or the common law. A total of 31 of the 50 states have enacted legislation, codifying their common law provisions to the *Uniform Trust Code of 2000* (the UTC). The trust laws of the remaining 19 States are based on common law or their own individual codification of the UTC. There are no estimates on the number of trusts governed by State law.

*(f) Supervisory arrangements*

64. FinCEN administers the BSA which is the Federal AML law. It has the authority to issue regulations implementing the BSA, examine FIs for compliance, and take enforcement actions for violations of the BSA and its implementing regulations. FinCEN has delegated BSA examination authority to the FBAs, the SEC and the CFTC (which also have independent supervisory and enforcement authority), for the institutions they supervise and to the IRS for all other FIs that are subject to the BSA, but which do not have a FFR. In all sectors, FinCEN has retained civil enforcement authority. The following table aligns financial activity as defined by the FATF to the primary U.S. entities that generally carry on the activity, the primary sector regulatory arrangements, and the applicable core AML/CFT regulations:

---

<sup>10</sup> The terms *legal entity* and *legal person* are used synonymously to refer to any form of entity that is created by a filing with a State office.

Table 1. Financial activity as defined by FATF

Primary U.S. Entities Generally Authorized to carry on the activity	Primary Sector Regulatory authorities (outside of FinCEN enforcement oversight)	Core AML regulations
<b>Acceptance of deposits and other repayable funds from the public:</b>		
Domestic Banks, comprising national and State chartered banks, former savings associations (“thrifts”), credit unions, Branches of foreign banks, Certain other banks and trust companies <sup>11</sup> , private bankers	FBAs [BGFRS (member banks of the Fed including State-chartered banks), FDIC, NCUA, OCC], State banking supervisors	AML Program Rule, Customer Identification Program (CIP) Rule, Currency Transaction Reporting (CTR) Rule, Suspicious Activity Reporting (SAR) Rule, Record-keeping requirements
<b>Lending (This category includes some commercial and consumer loan companies that are not currently Federally regulated for AML)</b>		
Banks, non-bank retail Mortgage Lenders (RMLO), Life Insurance Companies <sup>12</sup> , Pawnbrokers, Businesses engaged in vehicle sales (automobiles, airplanes, boats)	FBAs (banks), State banking and insurance supervisors (banks and life insurance companies), IRS- SBSE (there is no “sector” regulator <i>per se</i> for RMLOs either at the Federal or State level), Pawnbrokers are not subject to AML/CFT obligations but are subject to the Form 8300 reporting obligation	For banks: AML Program, CIP, CTR and SAR Rule, Record-keeping requirements. For Life Insurance Companies and RMLOs: AML Program, CTR, SAR Rule, Record-keeping requirements
<b>Financial leasing<sup>13</sup></b>		
Banks, Equipment Leasing companies	FBAs, State banking supervisors	AML Program, CIP, CTR, SAR Rule, Record-keeping requirements
<b>Money or value transfer services</b>		
Legal/or natural persons-MSBs	State MSB supervisors, IRS-SBSE	AML Program, CTR, SAR Rule, Record-Keeping requirements, Travel rule

<sup>11</sup> More than 98% of all depository institutions, holding well over 99% of all deposits, are subject to Federal supervision and examination. A small number of State-licensed and supervised banks (approximately 350 non-depository trust companies, 265 non-Federally insured credit unions, and one private bank) are subject to the Federal SAR, CIP, and CTR requirements, but for historic reasons are not subject to an AML program obligation.

<sup>12</sup> U.S. authorities report that U.S. insurance companies do not offer retail loans. They can offer commercial loans. Most often, insurance companies invest in loan portfolios that are sold by banks.

<sup>13</sup> This includes some equipment leasing companies that are not currently Federally regulated for AML.

Primary U.S. Entities Generally Authorized to carry on the activity	Primary Sector Regulatory authorities (outside of FinCEN enforcement oversight)	Core AML regulations
<b>Issuing and managing means of payment (e.g. credit and debit cards, checks, traveller's checks, money orders and bankers' drafts, electronic money)</b>		
Banks (Credit/ debit cards, checks, travellers cheques, money orders, and bankers drafts), MSBs (Travellers checks, money orders), Virtual currency or prepaid products (Electronic money that is represented as prepaid access, such as a prepaid card, is issued by banks, but program managers can be MSBs), Travel Agencies	FBA (banks), State banking supervisors (banks), IRS-SBSE and State authorities (MSBs) Travel Agencies are not subject to AML/CFT obligations but are subject to the Form 8300 reporting obligation	For banks: AML Program, CIP, CTR and SAR Rule, Record-keeping requirements For MSBs: AML Program, CTR, SAR, Record-keeping requirements
<b>Financial guarantees and commitments<sup>14</sup></b>		
Banks, Surety bonding Companies	FBA (banks), State banking supervisors (banks), Surety bonding companies are not subject to AML/CFT requirements	AML Program, CIP, CTR and SAR Rule, Record-keeping requirements
<b>Trading in: money market instruments (checks, bills, certificates of deposit, derivatives etc.) ; foreign exchange; exchange, interest rate and index instruments; transferable securities; commodity futures trading</b>		
Securities dealers, broker dealers, Investment dealers, Banks, Commodity futures dealers, Commodity Pool Operators and commodity trading Advisors, Investment Companies (other than mutual funds)	FBA (banks), SEC/FINRA – broker/dealers, CFTC (derivatives) commodity, FinCEN Investment Companies (other than mutual funds), Commodity Pool Operators and Commodity trading advisors are respectively exempted from and not subject to AML/CFT obligations	AML Program, CIP, CTR and SAR Rule, Record-keeping requirements
<b>Participation in securities issues and the provision of financial services related to such issues</b>		
Broker-dealers, Banks	SEC, FINRA, FBA and State banking regulators	AML Program, CIP, CTR and SAR Rule, Record-keeping requirements
<b>Individual and collective portfolio management<sup>15</sup></b>		
Broker-dealers, , FCMs, IBs	SEC, FINRA, CFTC, NFA	For Broker/dealers and FCMs/IBs: AML Program, CIP, CTR and SAR Rule, Record-keeping requirements

<sup>14</sup> This is generally issued by banks, but also by insurance and surety bonding companies that are not currently Federally regulated for AML.

<sup>15</sup> This includes investment advisers.

Primary U.S. Entities Generally Authorized to carry on the activity	Primary Sector Regulatory authorities (outside of FinCEN enforcement oversight)	Core AML regulations
<b>Safekeeping and administration of cash or liquid securities on behalf of other persons</b>		
Banks, Couriers such as Brinks, Broker-dealers	FBAs, SEC, FINRA	AML Program, CIP, CTR and SAR Rule, Record-keeping requirements
<b>Otherwise investing, administering or managing funds or money on behalf of other persons</b>		
Investment Advisers, Broker-dealers, Mutual funds, FCMs, IBs	SEC, FINRA, FBAs, State banking supervisors. Investment Advisors are not subject to BSA AML/CFT obligations <sup>16</sup>	AML Program, CIP, CTR and SAR Rule, Record-keeping requirements
<b>Underwriting and placement of life insurance and other investment-related insurance<sup>17</sup></b>		
Life insurance companies, Broker-dealers	SEC, FINRA, State/territory insurance supervisors. Non-captive agents and brokers are not covered separately but are required to be included in the obligations imposed on their life insurance company principals.	AML Program, CTR, SAR Rule, Record-keeping requirements
<b>Money and currency</b>		
Foreign exchange dealers	IRS-SBSE, State MSB regulators. <sup>18</sup>	AML Program, CTR and SAR Rule, Record-keeping requirements

65. As noted above, IRS-SBSE is required to conduct BSA compliance examinations for MSBs, casinos and card clubs with annual gaming revenue over USD 1 million, life insurance companies that deal in covered products, dealers in precious metals and stones, non-Federally insured credit unions, operators of credit card systems, and non-bank residential mortgage lenders and originators (RMLOs). Unlike the FBAs, IRS-SBSE has no enforcement authority of its own for AML/CFT supervisory purposes, but can refer cases to FinCEN to decide whether civil enforcement measures are warranted. FinCEN has directed IRS-SBSE to suspend routine AML/CFT examinations of life insurance companies, relying instead on supervision of life insurance companies conducted by State authorities, pursuant to the NAIC exam manual. However, IRS-SBSE retains authority to conduct life insurance company AML/CFT exams, if requested by the States or directed by FinCEN.

<sup>16</sup> Investment advisers will be directly subject to BSA AML/CFT obligations when legislation, in the process of being enacted at the time of the on-site, comes into force. Certain investment advisers (around 54% of the total) are estimated to be already covered indirectly through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements.

<sup>17</sup> Investment-related insurance that includes the buying or selling of securities or other SEC-registered investments that involve a broker-dealer includes the full scope of AML safeguards. Life insurance underwriting and placement that does not involve an investment component is supervised by FinCEN for AML compliance with the support of State insurance supervisors. Insurance companies have AML Program and SAR filing obligations.

<sup>18</sup> FinCEN regulates foreign exchange dealers, and although foreign exchange dealers are not subject to the CIP rule, their record-keeping obligation includes similar specific customer identification and verification requirements.

1

*(g) International Cooperation*

66. The U.S. cooperates with many countries, and in recent years, the most frequently requested and requesting countries have been the United Kingdom, Canada, Mexico, Switzerland, and Hong Kong, China. The ***Office of International Affairs, Criminal Division (OIA)*** (within DOJ) is the U.S. central authority for all incoming and outgoing mutual legal assistance (MLA) and extradition requests. FinCEN also has a formal role in relation to cooperation with foreign FIUs and other competent authorities have their own arrangements with counterparts.



## CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

### *Key Findings and Recommended Actions*

#### *Key Findings*

1. National coordination and cooperation on AML/CFT issues has improved significantly since the last evaluation in 2006. Policy and operational coordination are particularly well-developed on counter-terrorism, counter-proliferation and related financing issues which are the government's top national security priorities. The authorities have leveraged this experience into better inter-agency cooperation and collaboration on ML risks and issues.
2. Overall, the U.S. has attained a significant level of understanding of its ML/TF risks through a comprehensive risk assessment process which has been ongoing for many years. The U.S. has demonstrated a high level of understanding of its key ML/TF threats, but a less evolved level of understanding of vulnerabilities. National policies and activities tend to address ML/TF threats well and there is a strong focus and reliance on LEAs. The NMLRA does not address DNFBP sector vulnerabilities systemically, but cites many situations where various DNFBPs were abused (wittingly or otherwise).
3. There is a number of gaps and exemptions (some more material than others) in the regulatory framework, most of which the assessors believe are not justified by a proven low risk assessment. The most significant of these is the lack of systemic and timely access to beneficial ownership (BO) information by LEAs, and inadequate framework for FIs and DNFBPs to identify and verify BO information when providing services to clients.
4. National AML/CFT strategies, and law enforcement priorities and efforts, are broadly in line with the 2015 national risk assessments which represent a point-in-time summation of the main ML/TF risks: TF and the laundering of proceeds from fraud (particularly healthcare fraud), drug offenses, and transnational organised crime groups.
5. The U.S. AML/CFT system has a strong law enforcement focus. All LEAs (Federal, State, local) have direct access to SARs filed with FinCEN. A particularly strong feature is the inter-agency task force approach, which integrates authorities from all levels (Federal, State, local). This approach is widely used to conduct ML/TF and predicate investigations, and has proven very successful in significant, large and complex cases. There is a high level of effective cooperation and coordination amongst competent authorities to address ML/TF and the financing of WMD. The FI sector is reasonably aware of NMLRA and the NTFRA, though there is scope for improved guidance, particularly on SAR reporting, and a more focused approach to more frequent updates of national risk assessments.
6. BSA AML/CFT preventive measures are mostly imposed on the financial sector, with the casino sector being the only significant DNFBP sector comprehensively covered. Accordingly, the financial sector is the focus of most guidance relating to suspicion, and the authorities' view of risk is heavily influenced by financial activity. The financial sector is therefore generally aware of and responsive to ML/TF risks. All non-financial businesses and

professions, including DNFBPs other than casinos, are subject to a cash transaction reporting requirement (Form 8300)<sup>19</sup>. All U.S. businesses and professions, including all financial institutions and all DNFBPs, are required to implement targeted financial sanctions.

7. However, comprehensive AML/CFT preventive and deterrent measures are not applied to DNFBPs, other than casinos and dealers in precious metals and stones, many of whom act as gatekeepers in practice, and are therefore potentially a substantial source of information on high risk sectors and transactions for FinCEN and LEAs. The assessors attribute compliance costs and burden on the private sector as the more heavily weighted factors influencing these exemptions and thresholds rather than a proven low risk of ML/TF, as required by the FATF Recommendations.
8. Generally the objectives and activities of competent authorities align well to national policies and identified threats. The supervisory authorities have adequate mechanisms in place to address FI supervision, but apart from casinos, very limited DNFBP supervisory activities are in place, as these are not subject to comprehensive AML/CFT preventive measures.

### *Recommended Actions*

1. Take steps to ensure that BO information of U.S. legal persons is available to competent authorities in a timely manner, by requiring that such information is obtained at the Federal level (see IO.5).
2. To address the identified vulnerability in the securities sector, the U.S. should continue working on extending comprehensive AML/CFT requirements directly to investment advisers (IAs).
3. The U.S. should consider building upon the Geographic Targeting Order (GTO) assessment already started in the high-end real estate sector by addressing the roles of key players involved in the purchase/sale of real estate, to help mitigate ML risks in the high-end real estate sector: IO.1 and R.1 (see also IO.3, IO.4).
4. The U.S. should issue guidance to clarify the scope of the immediate SAR reporting obligation to make it absolutely clear that it applies below the reporting thresholds (USD 5 000 for banks, USD 2 000 for MSBs) and in which cases it applies. The U.S. should also conduct a focused risk review of the existing thresholds, which are not in line with the FATF Standards or the identified risks relating to terrorism or ML: IO.1 and R.1 (see also IO.4, IO.6, R.20, R.23).
5. The U.S. should conduct a vulnerability analysis of the minimally covered DNFBP sectors to address the higher risks to which these sectors are exposed, and consider what measures could be introduced to address them.
6. In order to publicly communicate its confirmed or updated understanding of ML/TF threats, the U.S. should consider updating NRAs on a more regular basis.

<sup>19</sup> Financial institutions and casinos have a separate cash transaction reporting obligation (Currency Transaction Reports).

67. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The recommendations relevant for the assessment of effectiveness under this section are R1-2.

### ***Immediate Outcome 1 (Risk, Policy and Coordination)***

#### *Country's understanding of its ML/TF risks*

68. Overall, the U.S. has attained a significant level of understanding of its ML/TF risks through a comprehensive risk assessment process that has been ongoing for many years. The understanding of TF risk is highly developed at all levels among all relevant agencies. There is a very good understanding of ML risk within the relevant Treasury, DOJ and Federal LEAs, but an uneven understanding of risks across the supervisory sectors, with the FBAs and FinCEN displaying a high level of understanding, and the civil components of the IRS and some State authorities a lower level.

69. The U.S. understands terrorism, proliferation and their financing to be the most serious risks to national security. Knowledge of the risks of TF is particularly high and supported by well-coordinated inter-agency activity and input, geographic focus and good input from the intelligence services and reporting sectors in the form of SARs. Cutting edge work is being done on tracking TF threats presented by U.S. based flights traveling to or near conflict zones. However, some financial supervisors tend to take a more limited view of TF risk than others, sometimes equating TF risk with designated persons and entities and sanctions.

70. The U.S. also has a good understanding of the significant threats it faces from various sources (see paragraph 38). The U.S. recognizes: the risks posed by the misuse of legal persons and legal arrangements; the vulnerabilities of the financial sector, high-end real estate sector and casinos. However, overall the U.S.' understanding of the vulnerabilities in the DNFBP sector as a whole is less evolved than that in the financial sector.

71. The U.S. bases its understanding of ML/TF risks on the entire body of national and other risk assessments (not all of which are public), including the publicly available NMLRA, NTFRA, and 2005 NMLTA (still valid); ***confidential national risk assessments*** underpinning national security strategies to combat terrorism, proliferation and their financing, and major proceeds generating crimes and related ML; and ***agency-level risk assessments*** by key Federal LEAs within their area of expertise (see Chapter 1, *Country's Risk Assessment & Scoping of Higher-Risk Issues*) for information on how these risk assessments are prepared, and the reasonableness of their conclusions.

72. The Federal LEAs with principal investigative authority over financial crimes (DEA, FBI, HSI-ICE, IRS-CI, and U.S. Secret Service) individually identify and analyse, on an ongoing basis, the ML/TF risks associated with the predicate crimes within their areas of responsibility. These threat assessments are based on each agency's operational experience and intelligence, supplemented by SAR information. FinCEN does the same in its role as both FIU and AML/CFT regulator, developing its understanding of risks on the basis of: analysis of its SAR database; discussions with the private sector through the Bank Secrecy Act Advisory Group (BSAAG); direct involvement in inter-agency threat-based forums (such as NSC working groups) and AML/CFT compliance working groups (for example, the FFIEC BSA/AML working group); ongoing collaboration with policy makers, LEAs, and supervisory agencies; and information sharing with foreign partners.

*National policies to address identified ML/TF risks*

2

73. Overall, national criminal justice policies, activities, and resource allocations are well-focused on addressing the ML/TF risks through the various public and confidential national and agency-level risk assessments (e.g. agency-specific strategic plans and annual performance goals identified in [annual performance plans](#), and updated with the President's budget each February). The national security strategies address major predicate crimes and terrorism, including a substantive focus on tackling related ML/TF, and are all broadly in line with the country's main threats as identified in the 2015 NMLRA and NTFRA. Below are key examples of how the major ML/TF risks are addressed through national AML/CFT policies and activities.

74. **Terrorism:** The *National Strategy for Counterterrorism 2011* specifically addresses this risk and sets out a strategy for combating terrorism and specifically its financing. The Director of National Intelligence is advised by the **National Counter Terrorism Center (NCTC)** on how well U.S. intelligence activities, programs, and budget proposals for counterterrorism and TF conform to the President's priorities. The U.S. is undertaking ground-breaking work to identify and address the risks posed by foreign terrorist fighters.

75. **Health-care fraud: The Health Care Fraud and Abuse Control Program (HCFAC)** (directed by the Attorney General (AG) and Secretary of DHHS) identifies States, healthcare providers, suppliers and beneficiaries at high risk of being abused for healthcare fraud and related ML, uses these results to coordinate national efforts to combat such activities, and demonstrates impressive successes in dismantling high-value fraud schemes: *HCFAC Annual Report for FY 2013*.

76. **Drug trafficking:** The *National Drug Control Strategy*, *National Northern Border Counter Narcotics Strategy*, and *National Southwest Border Counter Narcotics Strategy* specifically address both the predicate crime and related ML. A major focus is dismantling the largest drug trafficking organizations (DTOs) and related ML networks operating internationally and domestically. The **Southwest Border Executive Steering Group** (chaired by ONDCP) includes senior leaders from more than 20 Federal agencies, meets several times a year to assess the threats along the southwest border and develops responses to emerging challenges.

77. **Transnational crime organizations (TCOs)** are specifically addressed in the *National Strategy to Combat Transnational Organized Crime*. A key component of this strategy is using powers under the USA PATRIOT Act to designate foreign jurisdictions, institutions, or classes of transactions as *primary money-laundering concerns* which restricts financial dealings by U.S. persons with those entities, as well as a sanctions program to block the property of significant TCOs. Operationally, the LEAs focus on disrupting and dismantling TCOs and their financing networks.

78. The authorities understand that the U.S. is often a desirable destination for the proceeds of foreign predicate offenses, including corruption. In response to that risk, DOJ's Asset Forfeiture and Money Laundering Section (AFMLS) has a dedicated **Kleptocracy Asset Recovery Initiative** which specifically focuses on recovering the proceeds of foreign official corruption. The NMLRA notes that the use of domestic shell companies is a known typology to introduce foreign proceeds into the U.S. for layering and integration.

*Exemptions, enhanced and simplified measures*

79. ***In certain high risk circumstances, law or regulation requires enhanced due diligence (EDD).*** FIs are required to apply EDD when establishing/maintaining correspondent accounts for foreign banks, and to conduct enhanced scrutiny of private banking accounts maintained for foreign PEPs, and the authorities can designate other high risk situations requiring EDD: USA PATRIOT Act, s.311 & 312. This is in line with the NMLRA which specifically identifies correspondent banking relationships with foreign banks as being an elevated risk, and the 2005 NMLTA which specifically identified foreign PEPs as being elevated risk. Although legislated PEPs requirements do not specifically apply to the vast majority of depository accounts or investment accounts (only private banking accounts, where the threshold deposit at account opening is USD 1 million or more are covered), in practice, the FFIEC Manual broadens the application on an enforceable basis, and most FIs do apply PEPs determinations to a broader array of accounts and relationships, including BO, where known (see Chapter 5). The regulatory framework also has gaps and thresholds which in the view of the assessors are not justified or in line with the vulnerabilities identified through the risk assessment process, and which negatively impact effectiveness to varying degrees.

80. ***There is no requirement to collect BO information in all cases,*** and in any event the U.S. definition of BO is of very limited application and does not conform to the FATF standards (see TC Annex). Lawyers, accountants, trust and company service providers (other than trust companies) who can establish, facilitate or provide corporate and financial services to complex corporate structures or complex transactions are not subject to comprehensive AML/CFT requirements. Even though the involvement of these professionals in such activities is not required under U.S. law, in practice, they often are involved in the creation and management of complex legal persons and arrangements. Consequently, these gaps are significant as they pertain to high risk situations and are inconsistent with the NMLRA (and 2005 NMLTA before that), which contains examples of the vulnerabilities of these sectors to ML/TF. Over the years, the authorities have made several attempts to make the necessary legislative amendments largely without success, although limited progress has been made: see IRS procedures for obtaining an EIN, and measures extending AML/CFT requirements to BO and the IA sector. Efforts are once again underway, with draft rule-making pending on BO.<sup>20</sup>

81. ***Investment advisers*** (a part of the securities industry which manages over USD 67 trillion in assets) are not directly covered by BSA obligations. Some IAs, however, are indirectly covered through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements. Nonetheless, there is a gap, given the size and importance of this sector, which is not in line with the NMLRA which recognizes the risks of ML through the securities sector: p.78-80. FinCEN has proposed regulations which would extend AML/CFT requirements explicitly to all IAs.

82. ***Real estate agents (REAs)*** have been exempted from AML/CFT requirements. This is not in line with the NMLRA which documents significant cases of ML through this sector: pp. 26, 42, 67-68, 70. The U.S. has been assessing the ML/TF risks in the real estate sector since 2003. In the U.S.

<sup>20</sup> Since the on-site, the Final CDD Rule, that includes a BO requirement, was published on 11 May 2016. The implementation period for the Rule is two years (see [www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx](http://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx))



context, REAs do not themselves process financial transactions, but they are deeply involved in negotiating transactions and are therefore subject to the *FATF Recommendations*. Following the exemption, the U.S. attempted to mitigate risk in this sector by extending AML/CFT obligations to RMLOs in the financial sector on the basis that these institutions handle mortgage loans in the majority of transactions not otherwise financed by banks. Historically, 75% of U.S. real estate transactions involve borrowed money, and lenders, both banks and non-banks, are covered by AML rules.<sup>21</sup> However, addressing the vulnerabilities of lenders is only a partial solution, because: (a) RMLOs can only conduct CDD on the purchaser, not the vendor; (b) on an average, about 25% of the market in real estate does not involve financing (particularly the high-end market) (see [link](#). Figures for some States: Florida: 46.7%; New York: 46.3%); (c) although banks have reasonably good AML/CFT programs overall, the same cannot be said of RMLOs whose programs are still in the early implementation stage (their programs do not appear to be very robust and at most would address financed transactions in the mass market only); and (d) lawyers (who frequently play a key role in handling/negotiating financial transactions) and other gatekeepers in the sector (such as cooperative associations and *condominia* associations and others who play an active role applying sales conditions to real estate sales, which may include prohibiting financing, thereby making real estate an attractive market for large cash investments) are subject to limited AML requirements. In early 2016, FinCEN initiated a temporary measure - a Geographic Targeting Order (GTO) - to gather data on certain high-end real estate sales in two major urban markets. In summary, the assessors believe that the strategy of addressing ML/TF risk in the real estate sector through the financial sector has been of only limited value as it focussed attention mostly on lower risk (the mass market) rather than the high-end market. This is now being addressed by the recent U.S. initiatives using the GTO tool to gather information on high risk transactions.

83. ***There is generally a USD 5 000 threshold on SAR reporting (USD 2 000 for MSBs)*** which is not in line with the standard even though structuring is an identified risk in NMLRA, as are individual contributions and self-funding of terrorist activity involving small amounts of money (NTFRA). This issue is somewhat mitigated by two factors: (1) the financial sector is particularly aware of and responsive to TF risks, and FIs with a SAR obligation are required to notify law enforcement immediately and file a timely SAR to report violations that require immediate attention, such as suspected TF or an ongoing ML scheme, regardless of threshold. The U.S. was able to demonstrate that some SAR reporting below the threshold is taking place. (2) Rather than reporting each suspicious low value transaction as it occurs, if there is a pattern of activity, the U.S. requires FIs and DNFBPs to aggregate the transactions for SAR reporting. The U.S. believes that the thresholds help the authorities focus on larger transactions with a higher probability of a nexus to illicit activity. The thresholds and their impact were discussed extensively with the U.S. and the assessors acknowledge that some smaller transactions are reported if they qualify for the aggregation or under the immediate reporting obligation. Nevertheless, it is likely that some transactions are not being reported, though FATF standards require reporting of all suspicious transactions regardless of thresholds.

<sup>21</sup> [www.realtormag.realtor.org/daily-news/2016/02/05/fewer-buyers-are-bringing-all-cash-close](http://www.realtormag.realtor.org/daily-news/2016/02/05/fewer-buyers-are-bringing-all-cash-close)



*Operational objectives and activities of competent authorities*

84. The priorities and activities of the Federal LEAs are well aligned to and consistent with the ML/TF risks identified through the risk assessments, particularly on TF and ML related to healthcare fraud, drug trafficking and transnational organized crime. This was demonstrated by: annual, budget and thematic reports published by key agencies demonstrating that their activities and resource allocations are focused on ML/TF both in conjunction with predicate activities and as stand-alone offenses; special initiatives aimed at targeting priority ML/TF activities; and numerous cases showing that investigations of serious proceeds-generating predicate offenses always include a financial component.

85. **On terrorist financing: FBI-TFOS** is charged with managing FBI's investigative efforts into TF facilitators and ensuring financial investigative techniques are used, where appropriate, in all FBI counterterrorism investigations. **FBI-TFOS** supports the 104 local FBI-led *Joint Terrorism Task Forces* which coordinate counterterrorism investigations in their respective locations, and specialized units such as the **Foreign Terrorist Tracking Task Force (FTTTF)** which conducts in-depth analyses using government and public source datasets and classified information, to identify and track terrorist and national security threats and provide intelligence on these threats to FBI field offices, headquarters sections, and intelligence community partners.

86. **On ML related to fraud:** The creation of the **Health Care Fraud Prevention and Enforcement Action Team (HEAT)** in 2009 by the DHHS and DOJ raised the fight against Medicare fraud to a Cabinet-level priority. It investigates high dollar value/high impact fraud cases and related ML in nine high risk locations (Miami, Los Angeles, Detroit, Houston, Brooklyn, South Louisiana, Tampa, Chicago, and Dallas) through **Medicare Fraud Strike Forces (MSFS)**.

87. **On ML related to tax fraud, IRS** identifies trends, detects high-risk areas of non-compliance, and prioritizes enforcement actions against taxpayers who file fraudulently, including related financial crimes such as ML/TF, currency violations, and tax-related identity theft fraud adversely affecting tax administration: *IRS FY 2015 President's Budget*. The IRS-CI strategic plan sets out three high level investigative priorities: pursuing tax crimes (including legal and illegal source tax crimes) which is its core mission; other financial crimes such as public corruption, currency violations, and cybercrimes and narcotics-related and counterterrorism financial crimes.

88. **On ML related to fraud, the Bank Fraud Working Group** (chaired by DOJ Fraud Section) facilitates coordination between LEAs and the FBAs in investigating and prosecuting FI fraud and related ML where proceeds are laundered through the banking sector.

89. **On ML related to drug trafficking and transnational organized crime:** The High Intensity Drug Trafficking Areas (HIDTA) program provides assistance to Federal, State, local, and tribal law enforcement agencies operating in 28 critical drug-trafficking regions of the U.S. supported by 59 Intelligence and Investigative Support Centers which help identify new targets and trends, develop threat assessments, de-conflict targets and events, and manage cases. The National Guard Counter Threat Finance Program supported over 566 ML investigations of outlaw motorcycle gangs on the Northern border, transnational criminal organizations on the Southwest border, and FIs and front companies with links to TF, drug trafficking, and ML. ICE-HSI uses the Financial Crimes Illicit

Pathways Attack Strategy (IPAS) Methodology Assessment (a performance metric) to allocate resources toward high impact/high risk cases focused on disrupting/dismantling DTOs, identified through pre-defined criteria which are reviewed monthly (see also Chapter 1 for a description of the OCDETF). The U.S. has implemented a specific initiative to address trade-based money laundering (TBML), one of the methods used by transnational organised crime (TOC) and identified in the NMLRA. Within ICE, Trade Transparency Units (TTU) identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries' trade units.

90. **On ML generally, the High Intensity Financial Crime Area (HIFCA) program** is aimed at targeting financial crime (including ML) in high risk areas, by combining the resources of Federal, State and local authorities in an inter-agency task force model. **FinCEN's Strategic Plan 2014-2018** identifies particular risks and vulnerabilities in the financial system, and outlines its strategy for addressing them. The **National Bulk Cash Smuggling Center (BCSC)** (within ICE-HSI) is an operations support facility providing real-time investigative assistance to the Federal, State, and local officers enforcing and interdicting bulk cash smuggling, the transportation of illicit proceeds, and domestic/international currency seizures. It coordinates with the U.S. Transportation Security Administration (TSA) which screens travellers for contraband at U.S. airports. If TSA encounters suspicious bulk cash, it notifies the BCSC which exploits information related to domestic and international currency seizures. LEAs meet quarterly in the **Virtual Currency and Emerging Threats Group** to discuss trends in the virtual currency industry.

91. **On the regulatory side**, most activities of Federal regulators and SROs are broadly consistent with the evolving national AML/CFT policies and identified ML/TF vulnerabilities of supervised sectors (see Chapter 6). For example, to address the emerging threat of **virtual currencies and prepaid cards**, FinCEN applied AML/CFT requirements to administrators and exchangers of virtual currency, and issued guidance in this area which has given prosecutors the tools to combat ML through this sector<sup>22</sup>. The **FFIEC updates the BSA/AML Examination Manual** periodically to reflect new ML/TF risks and supervisory expectations. Supervisors are quick to apply **enforcement measures** if an FI's risk assessments do not align to those of the authorities (see Chapter 6).

### *National coordination and cooperation*

92. National coordination and cooperation on AML/CFT issues has improved significantly since the last evaluation in 2006. Policy and operational coordination are particularly well-developed on counter-terrorism, counter-proliferation and related financing issues. Learning from their experience in those areas is also leading towards better inter-agency cooperation and collaboration on AML issues. Numerous mechanisms are used which is reflective of the complex nature (Federal, 50 States and numerous local governments) and vast size of the U.S. and its financial system.

93. **Policy level coordination and cooperation:** The NSC staff chair a number of **Inter-agency Policy Committees (IPC)**, comprised of representatives from relevant government agencies, which

<sup>22</sup> See Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the ABA's National Institute on Bitcoin and Other Digital Currencies, June 26, 2015, [www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-aba-s-national-institute](http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-aba-s-national-institute)

address a range of national security concerns, including AML/CFT policy and strategy coordination to protect the financial system and strategic markets from abuse by terrorists and other criminals. For example, the IPC on TOC and the **Threat Mitigation Working Group** manage operational implementation of the *TOC Strategy*, and the **IPC on Corruption** oversees inter-governmental coordination of strategies to counter foreign corruption. One of the IPCs meets at least weekly to assess implementation of the *National Strategy for Counterterrorism*, to identify emerging terrorist threats and TF risks, and consider targeted sanctions targets. The **AML Task Force** is led by the Treasury's TFFC and is an ongoing interagency group (established in 2012) to review the AML framework, consider where improvements are needed, and implement the necessary legal and operational changes. It includes senior representatives from the CFTC, DOJ, FBAs, IRS, SEC, and FinCEN. It has a **law enforcement sub-group** to advise on ML/TF risks and challenges to law enforcement investigations.

94. **Operational level coordination and cooperation:** A particularly strong feature is the inter-agency task force model, which integrates authorities from all levels (Federal, State and local), is widely used to conduct ML/TF and predicate investigations, and has proven very successful in sophisticated, large and complex cases. The benefits and 'force multiplier effect' within the task force environment was regularly noted during the on-site. For example, the Federal LEAs highlighted the benefits of being able to leverage off the deep knowledge of the State and local LEAs. The State and local LEAs highlighted the benefits of utilizing Federal authorities' expertise in conducting financial investigations, their resources, and the additional legal powers that exist at the Federal level. The task force model also facilitates inter-agency information sharing (see the description of the **Joint Terrorism Task Forces (JTTFs)** in Chapter 4 (IO.9)). The widespread use of **fusion centers** to address de-confliction and provide enhanced leads to LEAs is another innovative feature (see Chapters 1 and 3, especially IO.6). The **Attorney General's Organized Crime Council** coordinates all Federal law enforcement activity against organized crime, including ML. Chaired by the Deputy AG, it consists of the Assistant AG for the Criminal Division, the chair of the AG's Advisory Committee and the leaders of nine participating Federal LEAs: FBI; ICE; DEA; IRS; ATF; USSS; USPIS; Department of State, Bureau of Diplomatic Security; and the Department of Labor, Office of the Inspector General.

95. **Supervisory level coordination and cooperation:** There is also good coordination at the supervisory level, particularly among FinCEN, the FBAs, and the State-level supervisors for MSBs. The **FFIEC** and the **FFIEC Manual** enhance coordination and provide banking examiners and FIs with consistent guidance. The **FFIEC BSA/AML Working Group (FBAs, Conference of State Bank Supervisors, and FinCEN)**, meets monthly to discuss examination issues and procedures, regulations and guidance; and meets quarterly with **OFAC, CFPB, SEC, CFTC, and other stakeholders**. The **SEC communicates regularly with FINRA** to discuss strategic initiatives, examination coordination, risk assessment efforts, and industry risks. The **Securities and Commodities Fraud Working Group** (chaired by DOJ Fraud Section) facilitates coordination between LEAs and regulatory agencies in the investigation and prosecution of fraud in the securities and futures industries and related ML. The **Indian Gaming Working Group** (comprising the National Indian Gaming Commission, DOJ, FBI, FinCEN, and the Bureau of Indian Affairs Law Enforcement Services) coordinates the work of the Federal agencies with authority over various aspects of Indian gaming.

96. **Policy coordination and cooperation on combating WMD proliferation and its financing:** The NSC (Senior Director for WMD, Terrorism and Threat Reduction) coordinates government

departments and agencies involved in combating WMD proliferation and its financing. The Department of State chairs four inter-agency working groups that review and share information on activities of potential proliferation concern and recommend appropriate courses of action to disrupt transfers.

97. **Operational coordination and cooperation on combating WMD proliferation and its financing** (see Chapter 1: *Legal & Institutional Framework*): The **Office of Export Enforcement (OEE)** (within BIS) has direct access to FinCEN's BSA data, works cooperatively with the export community and conducts investigations to support criminal and administrative sanctions. BIS is also responsible for developing lists that FIs can use to identify transactions which may involve WMD proliferation financing, including the [\*Denied Persons List, the Entity List, and the Unverified List\*](#). The **Export Enforcement Coordination Center (E2C2)** is staffed with fulltime personnel from ICE-HSI, and individuals detailed from other relevant departments and agencies. The **National Export Control Coordinator (NECC)** (within CES) coordinates counterproliferation investigations and prosecutions, manages nationwide training of prosecutors, and monitors progress on export control prosecutions around the country. **Counter-Proliferation Task Forces (CPTF)** exist in certain U.S. Attorney's offices to prosecute individuals and entities for violations of U.S. counter-proliferation laws and regulations, and to enhance cooperation among all agencies involved in export control, forge relationships with affected industries, and facilitate information sharing to prevent illegal foreign acquisition of U.S. technology. The **National Counterproliferation Center (NCPC)** is the relevant intelligence entity in this area.

#### *Private sector's awareness of risks*

98. The authorities have mechanisms in place to ensure that FIs, DNFBPs and other sectors affected by the application of the FATF standards are aware of the relevant results of the national ML/TF risk assessments. The **NMLRA and NTFRA are both public documents** available on the Treasury website, and the FIs/DNFBPs met with by the assessors during on-site were aware of them.

99. The **Bank Secrecy Act Advisory Group (BSAAG)** (chaired by FinCEN) is a major vehicle for the authorities and the private sector to have shared input, and has cross sector representation, though it is heavily oriented to the depository sector reflecting the significant role of banks as the primary gatekeepers of the financial system. The BSAAG holds two plenary meetings each year, and has three standing committees that meet on an ad hoc basis to consider ML risk compared to regulatory obligations, feedback to industry on the use of SARs, and areas requiring private sector guidance or an advisory. In May 2015, **FinCEN created a working group under the BSAAG** composed of law enforcement, private sector, regulators and FinCEN working together to identify joint industry-wide ML threats and emerging risks to the U.S. financial system on the basis of available data and the NMLRA. Ultimately, FinCEN will communicate the risks identified through the BSAAG discussions broadly to industry.

100. The **Securities and Derivatives Markets Working Group (SDWG)** (co-chaired by the SEC and the CFTC) focuses on identifying and addressing ML risks associated specifically with the securities and derivatives markets. The group fosters communications among industry, other regulators and

law enforcement. Participants include staff from Treasury, FinCEN, FINRA, NFA, DOJ and the IRS, and the group also seeks input from industry representatives.

101. Through an industry and academic outreach program called ***Project Shield America***, HSI Special Agents conduct presentations for U.S. manufacturers and exporters of arms and sensitive technology. The program provides an overview of export laws and solicits the private industry's assistance in preventing illegal foreign acquisition of their products. Since the program's inception in late 2001, ICE-HSI Special Agents have conducted more than 21 000 industry outreach presentations.

102. The LEAs and supervisors are all proactive in providing ***guidance to reporting sectors***, although the quality and frequency vary. There is a steady stream of formal guidance to FIs with a wide variety in scope and topics. The U.S. expects the FI and DNFBP sectors to take the national risk assessments into account in their own risk assessment processes; although most formal guidance comes from FinCEN and the LEAs, some minimally covered sectors seemed aware of the risks and the national risk assessments, even though the latter were issued quite recently. Ongoing outreach and publication of advisories by the FIU and LEAs on specific risks is the primary method of communicating with the private sector. Some vulnerabilities identified in the NMLRA could be better addressed (e.g. the vulnerabilities associated with shell companies and the real estate sector). The NMLRA identifies the risks of the misuse of legal persons through case examples demonstrating how legal persons have been abused for ML/TF purposes (although the U.S. argues that lawyers and TCSPs are not comprehensively covered, primarily because they are not necessary to register a legal entity). The U.S. does not apply comprehensive AML/CFT measures to all DNFBPs and there has been little or no systemic guidance to the minimally covered sectors, although there is some informal dialogue and other touch points. Some sectors (notably the American Bar Association) have developed internal AML policies to address the risks as they see them, even though their understanding of the risks is not always well aligned to the U.S. risk assessment findings as a whole.

**103. The U.S. is rated as having a substantial level of effectiveness for IO.1.**





## CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

### *Key Findings and Recommended Actions*

#### **Key Findings**

##### *Use of financial intelligence (Immediate Outcome 6)*

1. Financial intelligence is regularly and extensively used by a wide range of competent authorities to support investigations of ML/TF and related predicate offenses, trace assets, develop operational and strategic analysis, and identify risks. Direct access to the FinCEN database significantly enhances LEAs' ability to use financial intelligence in a timely manner, in line with their own operational needs and without waiting for disseminations from the FinCEN. A strong feature of the system is how financial intelligence is used within the task force environment through Suspicious Activity Report (SAR) Review Teams (149 nationally), Financial Crimes Task Forces, and Fusion Centers comprised of Federal, State and local authorities.
2. FinCEN also actively and increasingly supports operational needs by responding to specific LEA requests for information and analysis; providing information to identify unknown targets and new activities related to specific investigations; detecting new trends and producing strategic and tactical intelligence products; and initiating new cases through spontaneous disseminations. FinCEN's approach to dissemination relating to TF is very proactive. In recent years, it has increasingly applied a similar approach to ML.
3. Gaps in the legal framework somewhat limit the extent and timeliness of information available impacting U.S. authorities' ability to collect and share accurate and timely intelligence. These gaps are partly mitigated, particularly in the TF context, by the obligation to report immediately suspicious activities that require immediate attention regardless of threshold and through FinCEN's extensive outreach programs, guidance, advisories, other information and engagement with the private sector.

##### *ML investigation and prosecution (Immediate Outcome 7)*

1. The U.S. authorities actively pursue a "follow-the-money" approach at the Federal level, and have demonstrated their ability to successfully pursue sophisticated, large, complex, global and high-value ML cases. A wide variety of ML activity is pursued, and examples were provided of successful prosecutions of standalone ML, third party ML, and of the laundering of proceeds of foreign predicates. Criminals committing predicate crimes outside the U.S. have been detected and prosecuted when laundering proceeds in the U.S.
2. The U.S. achieves over 1200 ML convictions per year on average at the Federal level, which encompasses prosecutions in all 50 States and U.S. territories. Federal authorities prioritize large value, high impact cases, which often occur in the largest States such as California, Florida, New York, and Texas. Money laundering is investigated and prosecuted by Federal authorities. In addition, thirty-six States criminalize ML. Some State-level statistics are available but are not federally reported. Where provided, the information indicates that

States do not generally prioritise ML. At the Federal level, the sanctions which are being applied for ML are effective, proportionate and dissuasive.

3. The U.S. has national strategies aimed at pursuing ML related to fraud, drug offenses and transnational organized crime which is in line with the main risks identified through the risk assessment process. In 2015, the FBI made pursuing ML one of its top priorities. Several other agencies have a strong focus on the financial component of key criminal activity though there is scope for them to pursue ML more regularly as a discrete offense type.

#### *Confiscation (Immediate Outcome 8)*

1. The U.S. is successful in confiscating a considerable value of assets (e.g. over USD 4.4 billion was recovered by Federal authorities in 2014).
2. The U.S. is able to pursue administrative forfeiture, non-conviction based forfeiture and criminal confiscation and uses these tools appropriately. Most asset recovery cases proceed as civil forfeiture and most civil forfeitures take place administratively.
3. Confiscation achievements by agencies, specific task forces or initiatives suggest that authorities achieve confiscation in high risk areas, in line with national and agencies' AML/CFT priorities. Additionally, the authorities' focus on targeting high value cases also ensures that high risk areas are addressed.
4. The U.S. Federal authorities aggressively pursue high-value confiscation and provided numerous cases which demonstrate their ability to obtain high value confiscation in large and complex cases, in respect of assets located both domestically and abroad.
5. There is little official information in respect of criminal confiscation, or civil forfeiture, at a State and local levels, but it is apparent that State and local asset forfeiture activity is undertaken by joint task forces targeting priority offending and the remainder is likely to arise from State drug trafficking legislation.
6. Asset sharing arrangements are regularly agreed with both domestic and foreign counterparts, which encourage inter-agency and inter-jurisdictional cooperation.
7. Some gaps in the legal framework impact on effectiveness including the lack of general power to obtain an order to seize/freeze property of corresponding/equivalent value which may become subject to a value-based forfeiture order (such authorities exist in only one judicial circuit covering several States). The result is that such assets are unlikely to still be available by the time a final forfeiture order is made. Likewise, not all predicate offenses include the power to forfeit instrumentalities. Nevertheless, the U.S. is successful in confiscating a significant value of assets.

#### ***Recommended Actions***

##### *Immediate Outcome 6*

1. FinCEN should continue and enhance its current initiative to increase the level of spontaneous disseminations of information and intelligence relating to TF, and especially ML and predicate crimes.

2. FinCEN should continue and enhance its recent approach to go to reporting entities, including those not reporting the initial SAR, to obtain additional information for the purposes of FinCEN's operational analysis and dissemination, in addition to supporting ongoing cases/investigations.
3. The U.S. should address the gaps in the legal framework which currently limit the extent and timeliness of financial intelligence available to FinCEN and competent authorities. In particular, it should:
  - a) Extend reporting requirements to investment advisers, and DNFBPs (other than casinos);
  - b) Issue formal guidance clarifying reporting entities' immediate reporting obligations.
  - c) Conduct a focused risk review of the existing reporting SAR thresholds (in place since 1992) and timeframes.

#### *Immediate Outcome 7*

The authorities should:

1. Continue to prioritise investigation of the financial component of predicate offenses.
2. Continue to enhance inter-agency coordination and cooperation including by further improving inter-agency access to information, in particular IRS information.
3. Continue to prioritise the investigation and prosecution of ML activities per se, at both Federal and State level agencies, rather than as an associate type offense to other offenses.
4. Improve the visibility of AML State level activities and statistics, including via improved data collection and sharing, for a clearer nation-wide picture of the adequacy of AML efforts at all levels.
5. Legislate to ensure that a range of tax crimes are explicitly considered predicates for ML.

#### *Immediate Outcome 8*

The U.S. should ensure that:

1. All predicate offenses include the power to forfeit instrumentalities;
2. Authorities are able to seize and freeze pre-conviction non-tainted assets that are likely to be required to satisfy a value based forfeiture order in criminal proceedings;
3. Policy guidance is issued to investigators and/or prosecutors on when to pursue and prioritise confiscation in types of cases highlighted as being of particular concern in the risk assessments.
4. AML State level proceeds recovery activities and statistics are more widely and uniformly available, including via improved data collection and sharing, for a clearer nation-wide picture of the adequacy of asset recovery efforts at all levels.

104. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.3, R4 & R29-32.

3

### ***Immediate Outcome 6 (Financial intelligence ML/TF)***

#### ***Use of financial intelligence and other information***

105. The U.S. authorities make extensive and regular use of financial intelligence and other relevant information to identify investigative leads, develop evidence in support of investigations, and trace criminal proceeds related to ML, associated predicate offenses and TF. This is primarily achieved through direct access to and use of FinCEN data by LEAs, supplemented by active (and growing) dissemination of intelligence by FinCEN. The assessment team bases its conclusions on a variety of information including: statistics on the volume/types of BSA data collected by FinCEN and accessed by LEAs; discussions with a wide range of LEAs, task forces and prosecutors at the Federal/State/local levels; and the team's review of numerous cases demonstrating such information and intelligence is used in practice to support investigations and trace assets.

106. Many mechanisms facilitate the use of financial intelligence in conjunction with other relevant information. For example, ***FBI-TFOS's Strategic Intelligence Unit*** analyses methodologies to identify possible TF transactions at their earliest point. This includes ongoing analysis of BSA data to identify high-risk jurisdictions and TF typologies that, combined with analysis of other data including classified information, can provide investigators with new leads for possible TF investigations.

107. Particularly strong features in this area are the fusion centers and joint task forces which bring together Federal/State/local partners in an inter-agency environment. Fusion centers serve as focal points for receiving, analyzing, gathering, sharing threat-related information, and disseminating actionable intelligence (based on financial information, national intelligence, and local, State, and regional information). A prominent example is the ***OCDETF Fusion Center (OFC)*** which is a comprehensive data center that combines information from FinCEN with information from its member agencies (DEA, FBI, ATF, USMS, IRS, ICE and USCG, in cooperation with DOJ's Criminal and Tax Divisions, the Department of State's Bureau of Consular Affairs, the 94 U.S. Attorneys' Offices (USAOs), and State and local law enforcement), and others. Using this information, it analyses drug and drug related financial data to create comprehensive intelligence pictures of targeted organizations, including those identified as Consolidated Priority Organization Targets (CPOTs) and Regional Priority Organization Targets (RPOTs). It then passes actionable leads to OCDETF field agents. The ***International Organized Crime Intelligence and Operations Center (IOC-2)*** was created to enhance OCDETF's capacity to engage in intelligence-driven investigations. It leverages the resources of the OFC to target international organized crime, and has representatives from the same nine Federal LEAs that participate in the OFC.

108. There are 55 ***Financial Crime Task Forces*** led by IRS-CI which review Suspicious Activity Reports (SARs) based on a geographic or threat specific basis and bring together Federal, State and local authorities. Key task forces such as the DOJ's ***OCDETF*** (described in Chapter 1 *Legal & institutional framework*), and the New York-based ***El Dorado Task Force*** (see Chapter 1, *Legal &*

*institutional framework* section, IO.7 and IO.8) make extensive use of BSA data and their own in-house capacity to query and analyse such data. This task force environment fosters a high degree of cooperation and exchange of information and intelligence between FinCEN and other competent authorities, facilitating collaborative work and operational coordination among Federal, State and local agencies. LEAs highlighted the added-value of IRS-CI agents in these task forces, given their ability to “follow the money” and their forensic accountancy expertise, although some concerns remain over the limited access that other LEAs have to IRS tax information in the early stage of investigations (from an intelligence-sharing perspective).

109. U.S. authorities use financial intelligence and other information from diverse sources:

- a) *FinCEN's database of Bank Secrecy Act* reports and its analytical reports is the primary repository of financial intelligence in the U.S. coming from reporting entities in many forms including SARs, Currency Transaction Reports (CTRs), Reports of International Transportation of Currency or Monetary Instruments (CMIRs), Foreign Bank Account Reports (FBARs), and Reports of Cash Payments over USD 10 000 Received in a Trade or Business (Form 8300);
- b) *FEDWIRE*: The New York Federal Reserve Bank can search names, addresses, and account numbers for any fund transfers done through its system;
- c) *Clearing House Interbank Payment Systems (CHIPS)*: A subpoena can be served to search the CHIPS network, used by FIs to process wire transfers;
- d) *Tax returns*: These can be obtained by the USAO through an ex-parte court order;
- e) *Correspondent bank accounts*: Many foreign banks maintain correspondent accounts in the U.S. to conduct U.S. dollar transactions on behalf of their customers. Even without jurisdiction over a foreign bank, investigators can serve a grand jury subpoena and receive records of any cheques or wire transfers that cleared through the U.S. correspondent account on behalf of the foreign bank;
- f) Databases of investigative information held by the LEAs and prosecutorial authorities themselves, including investigative intelligence, criminal records, and mutual legal assistance requests; and
- g) Information from corporate, motor vehicle and property registries, and open source data.

110. FinCEN's database of BSA data contains 11 years of financial intelligence (over 190 million records) which can be analysed, disseminated to or shared with domestic and foreign partners, making FinCEN one of the largest repositories of information available to law enforcement in the country. FinCEN receives an average of 55 000 new reports per day (including 4 800 SARs) from approximately 150 000 FIs, DNFBPs, and other legal/natural persons. The 2006 mutual evaluation of the U.S. noted delays and backlogs in entering SAR information into FinCEN's database. These have been eliminated by the IT modernization process. Now, the vast majority of SARs are filed electronically and are available within one business day of being received by FinCEN.

Table 2. Reports received by FinCEN annually

Average number of reports received per year (2012-2014)					
SARs (Suspicious Activity Reports)					1 725 322
CTRs (Currency Transaction Reports)					15 283 950
CMIRs (Reports of International Transportation of Currency or Monetary Instruments)					209 918
FBARs (Foreign Bank and Financial Account Reports)					927.151
8 300 Reports (Reporting Cash Payments of Over USD 10 000)					259 521
Average number of Bank Secrecy Act reports received annually					18 405 862
Total number of Suspicious Activity Reports (SARs) reported (2010-2014)					
2010	1 326 372	2011	1 517 520	2014	1 973 813
2013	1 640 391	2012	1 587 763		

111. The information collected by FinCEN under the BSA can be linked with a variety of law enforcement and commercial databases during analysis. FinCEN's information sources fall into three categories: (i) direct access to its financial database (SARs, CTRs, CMIRs, FBARs, 8300 Reports); (ii) direct access to open source data and commercial databases (State corporation records, property records, people locator records, professional licenses, databases for court records, and vehicle registrations); and (iii) indirect access to law enforcement data from partner agencies (FBI, DEA, USSS, USPIIS, DHS, etc. – see Chapter 1, Legal and Institutional Framework).

112. All LEAs, task forces and prosecutors met with by the assessment team confirmed that the use of financial intelligence is a regular component of Federal, State and local investigations. Given the model for intelligence sharing and direct access by LEAs to BSA data, the authorities consider this intelligence as a regular part of their investigative process (rather than as something done only in response to dissemination by the FIU). Authorities therefore do not collect specific comprehensive statistics on the results obtained using this intelligence including investigations or convictions arising as a result of spontaneous disseminations by FinCEN. However, numerous cases were provided which demonstrate that financial intelligence and other relevant information are being successfully used to identify new targets, dismantle the financing networks of criminal enterprises, and trace assets.

#### Box 1. Financial intelligence and other information supporting investigations and asset tracing

**Belair Financial Services (2015):** ICE-HSI agents noticed a series of suspicious transactions involving multiple businesses listed at the same address writing checks to each other. Through FinCEN queries, ICE-HSI and IRS identified beneficial owner information for approximately 30 sham companies, connected the address to the main target, and ultimately dismantled a sophisticated transnational criminal organization laundering money from fraudulent health-related claims using sham companies, U.S. bank accounts and attorneys. Agencies involved: ICE-HSI, IRS-CI, New York EDTF, DOJ/AFMLS and USAO/EDNY.

**Disshod "Dema" Sidikov (2015):** MSB SARs identified 34 subjects wiring funds from numerous locations in



the U.S. to receivers in Russia, Ukraine, and Uzbekistan, and led to the identification of wires from these countries back to the U.S. Another MSB SAR identified the individual who wrote the virus and conducted the cyberattacks on the trucking companies to steal their account numbers and check codes. Related CTRs were discovered showing cash deposits/withdrawals from suspected bank accounts used by the defendants which enabled LEAs to monitor these accounts and track the proceeds. This investigation led to the dismantling of a criminal ring that skimmed more than USD 1.7 million from trucking companies engaged in legitimate commerce. Agencies involved: ICE-HSI; Youngstown, OH City Police and USAO/NDOH.

### *STRs received and requested by competent authorities*

113. Competent authorities make frequent use of SARs, CTRs and other mandatory reports filed with FinCEN. Although many reports contain relevant, accurate and useful information, the quality of reports varies and continues to improve. The extent to which reports are available from some sectors is reduced by technical deficiencies in the legal framework. The assessment team based these conclusions on various information sources including: statistics on the reports received/requested by FinCEN, and how often BSA data is accessed by LEAs; the NMLRA concerning ML/TF risks in sectors not subject to SAR reporting requirements; discussions with supervisors and reporting entities (on the quality of SARs, and feedback and guidance received), and with a wide range of LEAs, task forces and prosecutors at the Federal/State/local levels (on the quality and usefulness of SARs and other reports); and the team's review of cases demonstrating how SARs and other reports are used in practice.

114. FinCEN provides direct, self-service access to its data to about 10 000 authorized users from over 100 Federal/State/local LEAs and Federal supervisory agencies. Authorized users are easily able to access, query and analyse BSA data through the FinCEN Portal and FinCEN Query on-line inquiry systems introduced in 2012. On average, 30 000 searches of BSA data are undertaken daily, indicating extensive use of this data to support investigations. Nine key agencies have bulk access allowing them to match BSA data with information in their own databases to identify suspects, associates, possible leads, etc. The largest Federal LEAs also maintain liaison staff at FinCEN, on a full/part-time basis, enabling them to work directly with FinCEN analysts. These relationships are very important when partner agencies need FinCEN's support or coordination on investigations or other activities.

**Table 3. Top Five (5) FinCEN Query Users in FY 2015**

*(not including additional access to financial intelligence and other information that FinCEN provides by other means)*

Agency Name	Number of FinCEN Query Searches
<b>Federal Law Enforcement and Other Competent Authorities</b>	
Drug Enforcement Administration	256 011
Internal Revenue Service Criminal Investigation	223 111
Immigration and Customs Enforcement	191 324
Office of Personnel Management	189 301
Federal Bureau of Investigation	63 267

Agency Name		Number of FinCEN Query Searches
State Law Enforcement		
New York County District Attorney's Office		34 255
Florida Department of Law Enforcement		8 945
Illinois State Police		6 909
California Department of Justice		5 865
Texas Department of Public Safety		5 578

115. During the on-site visit, all LEAs, task forces and prosecutors stressed the usefulness of financial intelligence generally (and BSA data in particular). FinCEN indicated that the quality and depth of SARs varies considerably, depending on the reporting entity and the nature of the suspicion. Some reporting entities provide very sophisticated SARs, while others may not always provide comprehensive information. The authorities have taken steps to improve SAR quality and FinCEN confirms that quality is improving thanks to enhancements made to the SAR form, the introduction of electronic SAR filing, extensive outreach and guidance to reporting entities (including through the BSAAG mechanism described in IO.1), and feedback and compliance/supervisory actions by regulators. This includes: formal guidance provided to reporting entities by FinCEN, the FFRs, State agencies, and law enforcement partners; 66 advisories published by FinCEN on a diverse range of threats from mortgage fraud to financing terrorist organizations (some public and others non-public distributed by FinCEN through its secured network); enforcement actions published by regulators; and direct clarification and assistance provided by FinCEN and partners to reporting entities.

116. A particularly strong feature of the system is that section 314(b) of the PATRIOT Act encourages FIs (and any association of FIs) to share information amongst themselves for the purpose of identifying and, where appropriate, reporting possible ML or terrorist activity—a mechanism which enhances the quality of SARs. FinCEN is also able to seek further information from the entity which reported a SAR without need for a court order/subpoena (707 such requests were made to reporting entities in FY 2015). Furthermore, FinCEN has several authorities to collect additional information from reporting entities and this additional information becomes part of FinCEN's financial database (available directly to LEAs). Statistics about the use of these authorities were shown to assessors but some of the figures provided are not included to ensure confidentiality of ongoing investigations.

**Box 2. FinCEN's authorities to collect additional information from reporting entities**

3

**Geographic Targeting Orders (GTOs)** require any domestic financial institution or group of domestic financial institutions in a geographic area and any other person participating in a given type of transaction to file a report in the manner and to the extent specified in such order. Four GTOs have been publicly issued in the last two years (previously, they were not public). Examples include: a 2015 GTO requiring trades or businesses that export electronics located near Miami to record and report to FinCEN information on certain transactions in excess of USD 3 000; and a 2016 GTO on title insurance (see Box 3).

**Foreign Financial Agency (FFA)** rules impose additional reporting requirements on domestic financial institutions regarding transactional information involving identified FFAs. Since 2014, FinCEN has issued multiple FFA regulations to gather transaction data and U.S. FIs have reported over 5 million transactions to FinCEN. Information collected has enabled FinCEN to identify new trends in illicit activity (terrorist methodology for money movement, use of shell companies for ML, etc.). With this lead information, LEAs have opened numerous investigations into U.S.-based connections to foreign threats.

**Demand Letter** is a request for records relating to international funds transfers of USD 3 000 or more. The scope of the requested information can vary depending on the specific circumstances of the request. Since December 2014, FinCEN has issued nearly 100 Demand Letters to U.S. FIs requesting records. Information provided in response has assisted ongoing investigations, generated leads opening new investigations and assisted in TF investigations.

**Section 314(a) (USA PATRIOT Act)** enables Federal, State, local and foreign LEAs, through FinCEN, to reach out to over 43,000 points of contact at over 22,000 FIs to locate accounts/transactions of persons that may be “engaged in or reasonably suspected, based on credible evidence, to engage in terrorist acts or money laundering activities, with respect to a particular criminal investigation”. In practice, authorities wait until late in an investigation to use such requests in order to locate additional assets that may be involved in terrorism or serious ML. Waiting until an investigation is mature is due to the reach of the request and the potential for the account holder to be made aware of the investigation. Since 2006 FinCEN has submitted 2,055 section (a) requests to FIs for ML purposes and 480 for TF purposes.

**Special Information Sharing Authority (Section 314(a) (USA PATRIOT Act)** program involves a small number of U.S. financial institutions that are chosen based upon the particular 314(a) request characteristics (specific ongoing case) in order to report information linked to specific targets and/or typologies under investigation. Statistics show a very low use of this specific authority to date since it is a resource-intensive and time consuming procedure that entails several information sharing and coordination meetings, and maintaining ongoing communications with FIs and partners, etc.

117. FinCEN can use the above authorities in combination to obtain additional information regarding a particular SAR from any reporting entity (i.e. not just the entity that reported a particular SAR). This is however very rarely done for operational intelligence analysis by FinCEN of a particular SAR or related group of SARs early in the intelligence process. FinCEN indicated that use of information gathering powers in this way is a recent development and has been done few times in

the previous 18 months. FinCEN's powers to obtain additional information tend to be used much more either to support strategic analysis of particular priority issues (for example, human trafficking and smuggling, TBML, corruption and sophisticated ML networks) or in response to requests from LEAs to support existing investigations. While the use of these powerful tools in these broad ways is a real strength of the system, FinCEN is also strongly encouraged to make more expansive use of these tools for operational purposes, particularly noting its current efforts to enhance spontaneous disseminations of intelligence to law enforcement (as discussed below).

118. To some extent, technical deficiencies in the legal framework have an impact on effectiveness as they limit the reports and information available to the competent authorities. It is difficult to gauge the precise extent to which these deficiencies (described below) reduce effectiveness, especially as some of the deficiencies are partly mitigated in practice.

119. Investment advisers and a majority of DNFBPs are only partially subject to AML Programs or mandatory SAR reporting requirements. Investment advisers are not directly covered by the BSA and the SAR requirement. They can be indirectly covered through their affiliation to a FI, or when they act for a FI in the framework of an outsourcing relationship. Nonetheless, FinCEN is in the process of extending SAR reporting requirements to all investment advisers.<sup>23</sup> Real estate agents are not subject to AML Program or mandatory SAR reporting requirements. However around 75% of real estate transactions are partly covered because they involve loans issued by covered bank and non-bank lenders. Furthermore, FinCEN is addressing concerns about the high-end real estate sector by issuing GTOs (specially aimed to high-end market) in order to collect relevant information and assess how best to address the vulnerabilities. Casinos are covered under both AML Programs and mandatory SAR reporting.

120. Thresholds on SAR reporting (USD 5 000 for banks, USD 2 000 for MSBs) is a concern, but FIs and DNFBPs with SAR reporting obligations are directed to report immediately suspected violations that require immediate attention without regard for transaction value or whether a transaction has taken place. In practice, this issue seems to be somewhat mitigated and 8.37% of total SARs submitted are below the thresholds (20% of TF SARs and 8.27% of ML SARs). FinCEN indicated that removing the thresholds is not a top priority in terms of improving effectiveness, but that its data mining and IT tools would be able to cope with increased reporting if the thresholds were dropped (See IO.4 for more details about SAR reporting below the thresholds).

121. Deficiencies in CDD requirements (in particular the lack of BO requirements) can undermine the usefulness of SARs (e.g. SARs involving legal persons such as shell companies), and/or complicate the analytical process. However, investigators stated that these SARs can still provide actionable leads enabling LEAs to “follow the money”.

122. The time allowed to file SARs (30/60 days) was criticised in the 2006 U.S. evaluation and may reflect that, until recently, a majority of SARs were filed manually. SARs are now filed electronically. While the FATF standards set no specific deadline for filing SARs, and time limits vary from country to country, STRs must be submitted “*promptly*”. The relatively long time to file may reduce effectiveness, although this is mitigated to some extent by the fact that SARs can be and are

<sup>23</sup> On 25 August 2015, FinCEN issued a notice of proposed rulemaking (NPRM) that would impose certain AML requirements, including suspicious activity report (SAR) filing obligations, on investment advisers.

submitted urgently (e.g. in TF cases they can be, and often are, submitted within hours). Of the SARs filed within 30 days, the median timeframe for submission is 17 days and 24% are filed the same day illicit activity is identified (11% of all SARs are filed the same day the suspicious activity is identified).

### *Operational needs supported by FIU analysis and dissemination*

123. FinCEN's analysis and dissemination support the operational needs of competent authorities to some extent, though FinCEN is encouraged to continue and expand its current efforts to focus more resources on proactive, spontaneous disseminations. The assessment team based these conclusions on various sources including: a review of FinCEN's processes for analyzing SARs and other reports, and its intelligence and analytical products; the priority risks identified in the NMLRA and NTFRA; discussions with a wide range of LEAs, task forces and prosecutors at the Federal, State and local levels about the usefulness of FinCEN's products in investigations/prosecutions of ML, predicate offenses and TF.

124. All information collected from reporting entities is stored in FinCEN's BSA database. FinCEN uses a sophisticated analysis methodology based on IT and technological tools to mine bulk data and detect relevant information for further analysis and dissemination. IT modernization efforts since 2012 have significantly improved FinCEN's data management capabilities, and provided new tools for domestic partners to access the information.

125. Given the very large number of reports being received by FinCEN annually (over 19 million in 2014, including over 1.9 million SARs), FinCEN is not able to comprehensively analyse each SAR. Instead, it identifies priority SARs for further analysis by running sophisticated and evolving automatic business rules on incoming SARs each day - a process enhanced by recent IT modernization. Priority SARs are flagged and analytical resources devoted to those SARs considered most valuable to law enforcement, in accordance with evolving parameters reflecting national strategic priorities and LEA feedback. A large number of SARs are also analysed independently by law enforcement and other agencies with direct access to the BSA database (see Table 3 above).

126. FinCEN's highest priorities at present are: transnational security threats (including terrorism and TF), significant frauds (including health and tax frauds), transnational organized crime (including drug and human trafficking), kleptocracy, and cyber threats. These priorities are well-aligned with the recent national risk assessments. By identifying and flagging priority SARs for further analysis, and providing LEAs direct access to its database (subject to appropriate controls and confidentiality safeguards), FinCEN is able to manage the large number of reports it receives and provide continuous, targeted added value to the analytical and operational needs of LEAs.

127. At the strategic level, FinCEN assigns analysts to study information for trends and patterns based on the needs of FinCEN's law enforcement, regulatory, and policy customers. Such analysis includes identifying geographic and systemic "hot spots," identifying new and emerging phenomena, and providing detailed lead information to law enforcement and the intelligence community. This information may then be used as a basis for operational action. The following table outlines *Priority Threat Products* produced by FinCEN's Intelligence Division in FY2015.

Table 4. **Products developed and disseminated by FinCEN in FY2015**

Investigative Memoranda: <b>Operational analysis products produced by FinCEN to provide case support upon request from LEAs to support ongoing investigations. Used for responses to requests from domestic LEAs/authorities and Egmont.</b>	
<b>Priority areas:</b> TF, significant frauds, 3 <sup>rd</sup> party ML, ML related to drug offenses, transnational organized crime	1 271 produced (916 FIU & 355 domestic)
<b>Intelligence Flashes:</b> Summarize SARs identified by automated rules and alerts. Used to spontaneously disseminate high value SAR information related to terrorism and TF to domestic and foreign LEAs, FIUs, and the intelligence community within 1 to 2 days of receipt from reporting institutions	
<b>Priority areas:</b> Terrorist financing, foreign terrorist fighters	566 disseminated
<b>Dispatches or Proactive Referrals:</b> Operational analysis products which FinCEN produces and disseminates to LEAs spontaneously. They summarize SARs identified by analyst, with some context.	
<b>Priority areas:</b> Terrorist financing, significant frauds	102 disseminated
<b>Executive Alerts:</b> Short papers for governments executives on hot topics	
<b>Priority areas:</b> Cybercrime against FIs	6 published
<b>Intelligence Assessments:</b> Longer tactical or strategic analytical papers. Provide in-depth analyses of financial crime methodologies, associated trends, patterns, and vulnerabilities, and counter-measure recommendations	
<b>Priority areas:</b> Compromised FIs, TF, significant frauds, 3 <sup>rd</sup> party ML, ML related to drug offenses, transnational organized crime	22 disseminated
<b>Technical Bulletin:</b> Strategic with technical or statistical focus	
<b>Priority areas:</b> Compromised FIs, 3 <sup>rd</sup> party ML, significant frauds	8 published
<b>Research Summaries/Situation Reports</b>	48 published

128. Although the LEAs more often use their access to FinCEN's database to conduct their own searches and analysis, they can (and do) also request further information and analysis from FinCEN (*Investigative Memoranda*) to support ongoing investigations. FinCEN asserts that, as the FIU, it has the most sophisticated software tools and expert analysts to interrogate its own database, and this assertion was supported by the LEAs the assessors met during the on-site.

129. FinCEN indicated that a recent decline in the number of Investigative Memoranda being produced reflects the fact that it is seeking to move away from "reactive" disseminations to the extent possible, and to redeploy its analytical resources to focus more on proactive spontaneous disseminations such as Dispatches or Proactive Referrals. This proactive and more operational approach has been welcomed by the Federal LEAs and prosecutorial authorities. Discussions with LEAs confirmed that FinCEN's spontaneous dissemination are useful for identifying unknown targets, generating investigative leads and new cases, identifying new activities related to existing investigations, and detecting new ML/TF trends.

130. This change of approach and priorities by FinCEN is also supported by the assessment team for the following reasons: FinCEN's analytical resources are relatively limited given the size of its database and the number of incoming reports; LEAs have direct access to FinCEN's database, and a growing ability (enhanced by the recent IT modernization) to access and analyse data relevant to



particular investigations. Consequently, it makes sense for FinCEN to devote more of its analytical resources to the identification of SARs and targets that might not otherwise be detected by LEAs, and to the production of other ‘value-added’ analytical products. FinCEN is encouraged to continue strengthening its efforts to produce more reports of its own initiative (noting that only 102 Dispatches or Proactive Referrals were disseminated in FY2015. The previous year (2014) FinCEN disseminated 45 operational proactive products.

131. The U.S. provided numerous case studies demonstrating how BSA data is used to initiate investigations and/or facilitate evidence gathering. During the on-site, LEAs consistently emphasized the centrality and usefulness of financial intelligence in their investigations.

**Box 3. Illustrative examples of FinCEN’s strategic analysis being used to initiate operational action**

In January 2016, FinCEN issued a GTO that temporarily requires certain U.S. title insurance companies to identify the natural persons behind companies used to pay “all cash” for high-end residential real estate in New York City and Miami. This operational action was initiated after FinCEN’s strategic analysis of BSA data raised concerns that all-cash purchases (i.e., those without bank financing) may be conducted by individuals attempting to hide their assets and identity by purchasing residential properties through limited liability companies or other opaque structures.

132. In 2014, FinCEN initiated the Intelligence Flash product—a near real-time, proactively derived report, often generated from automated business-rule alerts and highlighting new or newly discovered SAR information. Flashes are disseminated within 1-2 days of receipt from reporting entities and are intended to provide immediate actionable intelligence to FinCEN’s law enforcement and intelligence community partners on a given subject(s) and/or apparent cluster. Currently, Flashes are focused primarily on TF. Since its inception, over 600 Flash reports have been disseminated to domestic and international stakeholders. The authorities confirmed that Flash reports and information collected from FIs through FinCEN’s “Hotline” have been operationally useful, and the team was provided with concrete examples showing its effectiveness in specific investigations of terrorism. Flash reports are also routinely disseminated to foreign partners, one of whom expressed concern that the reports do not always indicate a connection to the recipient country. FinCEN justifies its approach on the basis that Flash reports are very short (usually 1-2 pages) and aimed at giving the entire global network an opportunity to see another “piece of the puzzle”, and make connections that may not otherwise be obvious.

133. FinCEN works closely with LEAs and receives feedback on the usefulness of SARs reported by FIs; the criteria and rules established for analytical IT tools; and reports disseminated. This collaboration leads to an improvement of the whole system. FinCEN also surveys its partners annually on their levels of satisfaction. In FY 2014, 89% of all U.S. competent authorities and foreign FIU partners expressed satisfaction with the contributions that sharing information with FinCEN has provided to their organizations. This is a very strong result which further substantiates the

conclusion that FinCEN's operational and strategic analysis supports the operational needs of its users.

134. To its credit, FinCEN has addressed and is addressing many of the concerns expressed in the 2006 MER including the need to improve the process for filing SARs and other reports, maintain its key role within the AML/CFT chain, move away from being a sole database to be explored by others, and ensure that its products are meeting LEAs' needs. As was recommended in the 2006 MER, FinCEN has in fact worked closely with law enforcement to identify the kind of transaction information, crime areas and types of analysis that are of interest to LEAs. These initiatives have resulted in significant improvements in satisfaction levels by LEAs and supervisory authorities. FinCEN is encouraged to continue its current efforts in this regard.

### *Cooperation and exchange of information/financial intelligence*

135. The FIU and other competent authorities have a high degree of cooperation, coordination and exchange of financial intelligence. There are adequate safeguards in place to protect the confidentiality of information exchanged or used. LEA cooperation and coordination is an important aspect of the U.S.'s use of financial intelligence and is an extremely important issue in the context of a country such as the U.S. with many authorities and multiple levels of government. The assessment team based these conclusions on various sources including: discussions with members from a range of SAR Review Teams, Financial Crime Task Forces, and fusion centers (described above under Core Issue 6.1); memoranda of understanding (MOUs) governing the exchange of financial intelligence and/or other relevant information; and a visit to the FIU's premises which included a walk-through of some of the security measures in place.

136. **SAR Review Teams** exist in all 94 Federal judicial districts and meet monthly to review all SARs received in that judicial district. Some are assigned to a particular LEA to investigate, based on its expertise, or are investigated jointly. Most are led by IRS-CI with participation of the Federal LEAs with authority to investigate financial crimes. Others are controlled by the U.S. Attorney's Office. SAR Review Teams are also embedded in LEAs and within financial crime task forces (including JTTFs).

137. **An extensive framework of MOUs:** FinCEN seeks to coordinate and support information sharing across its network of more than 100 State and Federal law enforcement and U.S supervisory agencies. FinCEN has executed 373 separate MOUs for intra-agency sharing of information and access to FinCEN's data.

138. **LEAs direct access to FinCEN's database** facilitates information exchange, helping to coordinate law enforcement efforts, support investigations, and provide feedback to the FIU. In turn, this helps FinCEN prioritise its work and focus its analysis on the areas of most value to law enforcement. There are adequate measures in place to protect the confidentiality of FinCEN's information and to mitigate the risk that providing direct access to such a wide variety of agencies could result in leakage of valuable and sensitive information (see c.29.6). FinCEN's IT modernization has also helped enhance security and confidentiality by enabling secure communication for collecting, accessing, analysing and disseminating financial intelligence and other information. FinCEN also vigorously polices misuse of SAR data and the unlawful disclosure of SARs.

**139. The U.S. is rated as having a substantial level of effectiveness for IO.6.*****Immediate Outcome 7 (ML investigation and prosecution)******ML identification and investigation***

140. The U.S. authorities are very focused on “following the money” both to develop leads which may initiate investigations, support ongoing investigations and prosecutions, and trace assets for confiscation. This is particularly evident at the Federal level. Federal law enforcement agents, prosecutors, and courts are resident in 94 Federal judicial districts spread across the U.S. These Federal authorities pursue ML investigations in every State, the District of Columbia, Guam, the Marianas Islands, Puerto Rico, and the U. S. Virgin Islands. Asset generating activities are particularly targeted at the Federal level as part of a wider effort to dismantle and disrupt criminal organizations, and identify forfeitable assets. State and local LEAs can often join up with the Federal authorities in task forces which have greater powers and resources than those at the State level. Thirty-six States have their own separate ML offense which may complement the Federal ML offenses. The State-level information provided generally indicates that States do not prioritise ML. The assessment team based its conclusions on: discussions with Federal, State and local LEAs and prosecutors about how and when they identify and investigate ML; statistics of the numbers of Federal ML investigations and prosecutions undertaken annually; and numerous representative cases.

141. Federal LEAs have highly developed capabilities to identify and investigate ML, as well as serious and organised crime, and effectively conduct parallel financial investigations for asset-generating crimes and Federal prosecutors generally give appropriate consideration to charging ML. ML investigations are traditionally triggered: (i) in the course of an investigation into predicate activity when investigators may identify evidence and patterns of offending known to be associated to ML activity; or (ii) by prosecutors involved in the early stage of investigations who identify the potential for a ML charge which, in turn, focuses investigative efforts further down the ML route; and (iii) by the opening of ML investigations following tips, SARs reviews, or information from foreign authorities. The decision to charge ML involves several factors including:

- a) the requirement for a clear separation between the predicate offense and the conduct that forms the ML activity
- b) the ability to charge individuals who assisted with the ML activity, but are not otherwise implicated in the predicate offense (i.e. ML is favoured for third party ML activity)
- c) an inability to charge an individual with the predicate offense, but where ML is an option. Foreign predicate offenses in particular were cited as an example.

142. The authorities met during the on-site visit were well trained and able to successfully investigate high-value, complex ML, including those involving multiple jurisdictions. New law enforcement officers are trained on how to conduct financial investigations, employ forensic accounting, and conduct net worth analysis. Guidance on ML investigations is also provided to the field. Some examples from the FBI and /HSI Special Agents and DOJ were shared with assessors.

143. The Federal LEAs have extensive capabilities, resources and tools for undertaking specialist financial investigations and making good use of financial intelligence (R.31, IO.6, IO.8). Investigative methodologies emphasise the need to “follow the money” as part of the predicate offense investigation. The well-established inter-agency task force environment pools complementary agency-specific expertise and resources which further enhances their ability to conduct complex financial investigations (see also IO.1). The Federal LEAs and prosecutors met with by the assessment team demonstrated in-depth knowledge of these tools, and how to use them effectively in a wide range of circumstances (the assessment team met with Federal prosecutors from three offices). For example, IRS-CI agents are specifically called in for their forensics accounting and criminal tax investigative expertise.

144. Overall, the U.S. charges approximately 2,500 persons, natural and legal, and achieves over 1 200 Federal ML convictions per year on average, with the focus being on the ML transactional and basic offenses (18 USC 1957 and 18 USC 1956 respectively): see figures in table 5. Based on these numbers alone, the initial impression was that the U.S. pursues ML in only a relatively limited number of cases considering the overall estimate of proceeds and number of predicate offenses at the Federal level alone. However, more contextual information emerged during extensive discussions with the authorities during the on-site. Statistics on the volume of ML investigations are reportedly difficult to obtain and do not capture the full range of Federal ML investigations and prosecutions. Investigating agencies categorize many investigations involving ML under the primary offense (rather than ML). Prosecutors also noted that the final ML convictions represent less than half of the ML charges laid as many are dropped during the plea bargaining process (see Box 9). The ML charge may be dropped if the defendant pleads guilty to an equally serious crime and commits to cooperating with law enforcement in providing evidence against co-conspirators and higher ranking persons in the criminal enterprise.

145. At the Federal level, there is a strong focus on serious complex and high-dollar value criminal offenses, as was demonstrated through the over 100 case examples provided to the assessment team, and discussions with specialized task forces such as OCDETF and El Dorado Task Force (EDTF). The picture that emerged is that the approximately 1,200 Federal level ML convictions each year include a significant number of very large and complex ML investigations. LEAs and prosecutors also demonstrate flexibility and effectiveness in using the range of ML and predicate offenses to great effect including prosecuting tax crimes by relying on linked predicate activity (see Table 6 and Table 10). Beyond the main ML offenses, the U.S. also provided statistics on offenses that it considers key to complete the Federal ML picture as these relate to specific methods of facilitating laundering including: traveling in commerce to distribute proceeds (18 USC § 1952), using or investing income derived from racketeering (18 USC § 1962); and bulk cash smuggling (31 USC § 5332). (See Box 5).

Table 5. Number of ML charges, convictions and conviction rate<sup>1</sup> (2010-2014)

Action	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014
<b>18 USC 1956: Money laundering (proceeds laundering)</b>					
Charged	1879	2147	2163	2172	1895
Convicted	934	983	958	1072	1129
Conviction rate	51%	55%	53%	59%	57%
<b>18 USC 1957: Money laundering (transactional)</b>					
Charged	526	580	540	425	517
Convicted	262	229	272	241	249
Conviction rate	51%	53%	55%	56%	48%
<b>18 USC 1952: Interstate &amp; foreign travel/transportation, including of proceeds, in aid of racketeering enterprises</b>					
Charged	229	198	200	210	266
Convicted	122	136	130	94	111
Conviction rate	51%	52%	58%	49%	52%
<b>18 USC 1962: Receiving or deriving income from racketeering activities (RICO)</b>					
Charged	543	625	714	496	574
Convicted	252	302	400	412	369
Conviction rate	77%	81%	79%	78%	83%
<b>31 USC 5332: Bulk cash smuggling</b>					
Charged	207	207	137	163	117
Convicted	133	152	124	116	109
Conviction rate	73%	78%	78%	73%	69%
<b>TOTALS FOR 2010-2014</b>					
Charged	3081	3757	3754	3466	3369
Convicted	1703	1802	1884	1935	1967

**Table Note:**

1. Note that conviction rates in Table 5 were calculated using the number of defendants in each FY for which a verdict was obtained (not shown), which is not the same as the number of defendants charged in that FY. The cases initiated in any given FY do not necessarily conclude in that same FY.

146. ML investigations can be started within an individual agency (see **Table 6** data on ML and financial investigations initiated by IRS-CI, ICE-HSI and the FBI).

Table 6. Money laundering investigations initiated by IRS-CI, ICE-HSI and the FBI (2011-2014)

Agency	FY2011	FY2012	FY2013	FY2014
<b>Internal Revenue Service-Criminal Investigations (IRS-CI)</b>				
ML investigations initiated	1 726	1 663	1 596	1 312
ML prosecution recommendations	1 383	1 411	1 377	1071
ML indictments/informations laid	1 228	1 325	1 191	934
ML sentences	678	803	829	785
<b>Immigration and Customs Enforcement Homeland Security Investigations (ICE-HSI)</b>				
Financial Investigations Initiated (including for ML/TF)	6620	6526	6606	6594
<b>Federal Bureau of Investigation <sup>1</sup> (FBI)</b>				
ML investigations	309	282	269	220

**Table note:**

1. These figures do not include all investigations in which ML was a component of the criminal activity under investigation, only those cases classified as ML investigations in the FBI case management system. Other cases, which may include a ML investigation, may be classified under another specified unlawful activity (predicate offence).

147. Federal law, including the ML offenses, applies in all 50 States and the District of Columbia. Additionally, 36 States have criminalized ML at the State level and may undertake their own State-level ML investigations and prosecutions. Overall ML statistics are not readily available at State level and authorities confirmed that it is the Federal (not State) agencies which are mostly at the forefront of the U.S. AML efforts. Box 4 indicates that some States are pursuing ML at the State level.

**Box 4. Action by states to pursue ML and/or underlying activity – Illustrative examples of results achieved**

**Texas:** From FY 2013 to FY 2015, Texas has incarcerated 133 offenders for ML with an average of 44 incarcerations a year (figures as of 31 August 2015).

**New York:** Between 2011 and 2015, the New York State had carried out 283 ML prosecutions, and obtained 226 ML convictions according to preliminary figures. ML prosecutions per year have ranged from 46 (FY2011) to 68 (FY2015).

**Florida:** Florida has secured 118 ML guilty counts between 2011 and 2015 with a peak in 2012 with 59 ML guilty counts.

**New Jersey:** New Jersey has achieved 80 indictments or accusations containing ML charges between 2011 and 2015<sup>1</sup>.

**Note:**

1. Compiled by New Jersey Division of Criminal Justice by calendar year. Note that multiple defendants may be charged with ML in a single indictment or accusation and multiple counts of ML may be alleged. Accusations and indictments are both charging documents, but indictments derive from the grand jury and accusations are used when the defendant waives his/her right to grand jury indictment.



148. National strategies are intended primarily for and binding on Federal authorities. Most ML/TF activity in the U.S. is prosecuted under Federal law. Federal, State, and local authorities may work together in joint task forces on ML/TF. Where a case does not already fall under Federal jurisdiction but is too complex, or resource intensive, State and local police authorities may refer it to Federal authorities to investigate. The set-up does vary slightly from State to State. For example, Texan authorities commented that the amount of money involved in a case often dictates whether State or Federal charges are pursued, with relatively smaller cases going to the State. The U.S. provided the assessment team with examples of how State and local forces integrate into and support Federal investigations.

149. Where ML is criminalised at State level, State and local authorities work closely with local prosecutors (e.g. New York, Texas, Florida), and cases have been provided to exemplify some of the work carried out by them (see Box 5). Several factors affect the prioritisation of ML within a given State including the State's risk profile and the priorities set by the State Attorney General. States may focus on crimes mattering more to the local community e.g. crimes of violence and property crimes, rather than the crimes highlighted in the national strategies.

#### Box 5. Illustrative State ML Cases in NY and NJ.

**NY State: William E. Rapfogel & David Cohen (2014):** This case illustrates how NY State prosecuted a ML case based on fraud, kickback and theft activities. Both defendants plead guilty to stealing, together with co-conspirators, USD 9 million from the NPO they were executives of, in a 20-years grand larceny kickback scheme. Cohen admitted to illegally receiving USD 650 000 in cash kickback and payments for personal expenses and will pay USD 650 000 in restitution in addition to a prison sentence. Rapfogel admitted to stealing USD 1 million and pleaded guilty to NY grand larceny, ML, criminal tax fraud. He was sentenced to 3.5 to 10 years imprisonment and USD 3 million in restitution.

**New Jersey: Operation Jacked (2014):** HSI Border Enforcement Security Task Force in partnership with the New Jersey State Police and local law enforcement identified, investigated and dismantled a violent transnational criminal organization. A total of 23 individuals with different roles in the ring, including carjacker, car thief, wheel man, fence, shipper and buyer, were arrested and charged with a range of offenses including first degree money laundering. Stolen cars would be loaded into shipping containers, which were taken to ports for transport by ship to West Africa.

150. Where States have not criminalized ML, the picture is less clear. Discussions with a Federal Judge from one of these States suggested that the lack of State-level criminalisation was not problematic as Federal ML offenses would be available, ensuring that significant cases are pursued in line with the country's ML priorities. Overall, U.S. authorities are encouraged to collect information on a more regular and comprehensive basis concerning State-level ML investigations and prosecutions. Such information would enable Federal authorities to determine the extent to which law enforcement activities at the State and local level only are consistent with national AML/CFT priorities and risks.

### *Consistency of ML investigations & prosecutions with threats, risk profile, & national AML policies*

3

151. The U.S. authorities prioritise and allocate their resources towards pursuing the types of ML activity highlighted in the 2015 NMLRA and national strategies as being of particularly high risk. The assessment team based these conclusions on: a review of the budget and strategy documents of relevant agencies; discussions with specialised units and task forces; and cases demonstrating how effective these specialised units and task forces are.

152. The assessment team placed an increased focus on how the U.S. was pursuing ML related to fraud (particularly health care fraud), drug trafficking, and transnational organized crime (TOC) as the priorities outlined in the national security strategies, and the main risks identified in the NMLRA. To facilitate their ability to pursue these types of ML cases, the U.S. has: established specialised units and task forces focused on all these predicates and related ML; implemented mechanisms to target major criminal organizations and their financial networks, with a view to disrupting or dismantling their operations; and leveraged financial sanctions powers against priority targets of interest. These are primarily described at IO.1, Core Issue 1.4. These efforts have generated good results that have resulted in the disruption and dismantling of serious criminal organizations and their financial networks, including ML organizations.

153. **ML related to fraud:** In 2010-2013, as Healthcare fraud evolved, the **Medicare Fraud Strike Forces** (MSFS – see Chapter 1 Core Issue 2) adopted an approach more focused on ML and structuring which has successfully dismantled some massive high-value healthcare fraud schemes, and shut down related ML networks.

154. **ML related to tax crimes:** Although tax crimes are not predicate offenses for ML, the U.S. has successfully prosecuted ML related to such crimes by using other offenses, particularly fraud, mail fraud, wire fraud and filing of a false tax return. IRS-CI takes a leading role in such investigations, which is critical as it is the only agency with direct access to tax information.

#### **Box 6. ML related to fraud and tax crimes – Illustrative examples of results achieved**

##### **Statistics:**

- In FY 2013, the MFSFs achieved: 137 indictments, informations and complaints involving charges filed against 345 defendants who allegedly collectively billed the Medicare program more than USD 1.1 billion; 234 guilty pleas negotiated and 34 jury trials litigated, with guilty verdicts against 48 defendants; and 229 defendants imprisoned and sentenced to more than 52 months of incarceration on average<sup>1</sup>.
- On average, 1 500 suspects are arrested each year by Postal Inspectors of the USPIS for ML through the mail (including cases involving tax fraud) and drug trafficking.

##### **Representative cases:**

**Belair Financial Services (2015):** This case dismantled a highly sophisticated transnational criminal organization that used a complicit MSB, multiple shell corporations, U.S. bank accounts and

attorneys to facilitate the movement of funds obtained from fraudulent health-related claims made to insurance companies. The fraudulent financial activity involved the movement of approximately USD 28 million. The co-conspirators were convicted of ML and violations of the BSA. The complicit MSB was closed, USD 3.4 million was forfeited, related property was seized, and USD 900 000 in restitution was paid to the IRS. Agencies involved: HSI, IRS-CI, DOJ/AFMLS, EDTF and USAO/EDNY.

**Ihosvany Marquez (2011):** This case dismantled a multi-million dollar healthcare fraud ring, involving several defendants using shell companies to hide USD 61 million in illicit proceeds generated from a Medicare fraud scheme. Marquez pleaded guilty to ML conspiracy, Medicare fraud, and aggravated identity theft. He was sentenced to 16 years in prison and a forfeiture judgement of USD 21 million was issued. Agencies involved: FBI, IRS-CI, Florida Department of Law Enforcement and USAO/SDFL.

**Wegelin & Co (2012):** This case shut down a Swiss bank that had facilitated tax evasion by U.S. tax payers. The bank pleaded guilty to ML and tax fraud charges. It paid USD 57.8 million in restitution and fines, including USD 20 million restitution. A civil forfeiture action of over USD 16 million was also filed in relation to Wegelin's correspondent bank account in the U.S. Agencies involved: IRS-CI, USAO/SDNY and Main DOJ Tax Division.

**Note:**

1. DHHS and DOJ Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2013, pp.10-11, <https://oig.hhs.gov/publications/docs/hcfac/FY2013-hcfac.pdf>

155. **ML related to drug trafficking:** DEA has specialised ML groups in each of its 21 domestic field divisions. OCDETF only pursues top-end cases with a parallel financial investigation or central ML component. Both prioritise the most serious cases by developing lists of priority targets. OCDETF coordinates the annual formulation of the Consolidated Priority Organization Target (CPOT) list which is a multi-agency target list of the "command and control" elements of the most serious international drug trafficking and ML organizations. The DEA develops a list of Priority Target Organizations (PTO) which are the most significant international and domestic drug trafficking and ML organizations.

**Box 7. ML related to drug trafficking – Illustrative examples of results achieved**

**Statistics:**

- 75% of OCDETF investigations target ML in addition to drug trafficking, with approximately 10% targeting ML as the primary activity
- 130 domestic and foreign money laundering PTOs were disrupted or dismantled by the DEA through the 3<sup>rd</sup> quarter of fiscal year (FY) 2015; of these, 29 had a CPOT link.
- 50 CPOTs were identified on the FY 2015 CPOT list. Of these, 18 were indicted (36%), 12 arrested (24%), and 16 received an OFAC designation (32%).
- 696 CPOTs were dismantled between 2001 and 2011. 750 were dismantled in FY2011. 1,082 CPOTs were dismantled in FY2013. DEA has specialised ML groups located in each of the 21

domestic field divisions. In 2012 and 2013, USD 750 million and USD 637 million in cash seizures were achieved respectively.

#### Representative cases:

**Enrique Mendez (Op El Patron) (2013, Texas):** This case seriously disrupted a major DTO. Mendez was sentenced to 35 years and five months in prison for drug conspiracy and ML. A forfeiture order of over USD 41.9 million was issued. Over USD 7.5 million in drug proceeds and 450 kg of cocaine were seized, as was a drug ledger attributing the movement/distribution of around 12 500 kg of cocaine and USD 41.9 million in drug proceeds using commercial trailers. Agencies involved: OCADETF, DEA, HIS, IRS-CI, USMS, CBP, USAO/SDTX, Texas Department of Public Safety, Webb County Dan and Laredo Police Department.

**Joel Sesma-Garcia (Op Ice Vapor) (2015):** This case dismantled a major DTO and ML network which had laundered over USD 12 million in drug proceeds via interstate transportation of bulk cash, sending cash proceeds to Mexico via wire transfers, and acquiring these funds in cash to conceal their true source and nature. The main leader pled guilty to ML conspiracy and was sentenced to 25 years. Over USD 12 million cash, one residence and dozens of vehicles were forfeited. Agencies involved: OCADETF, DEA, HSI, FBI, IRS, CBP, ATF and USAO/AZ.

156. **ML related to transnational organized crime:** ICE-HSI adopts a whole-of-government approach to disrupting and dismantling TOC. It concentrates enforcement activity in high-risk illicit pathways used by TOCs to smuggle people and illicit goods into the U.S. ML is a prime focus within this strategy: see IO.1. One of the methods used by TOC (and identified in the NMLRA) is trade-based money laundering (TBML) which the U.S. is addressing in part through its network of Trade Transparency Units (TTU). TTUs brings together both domestic and foreign trade data, allowing users to see both sides of a trade transaction which effectively enables the identification of international trade anomalies and financial irregularities indicative of TBML, customs fraud, contraband smuggling, and tax evasion: see Box 8. FIs also identify potential TBML in SARs, which SAR Review Teams (See IO.6) flag for investigation. With ML recently being designated a top enforcement priority by the FBI, its 56 field offices will increasingly target ML in the context of sophisticated organized crime investigations and work closely with domestic and international law enforcement partners to identify the criminal organizations involved in ML activities, disrupt those organizations and seize and forfeit their assets.

#### Box 8. ML related to transnational organized crime – Illustrative examples of results achieved

##### Statistics:

- ICE-HSI prioritised and ranked 56 financial crime and ML investigations involving priority TOCs in FY 2014. These cases targeted TOCs generating USD 13 million a month to USD 100 million per year being laundered through bulk cash smuggling, structured bank deposits, trade-based money laundering (TBML), shell corporations, wire transfers, third

party ML, and MSBs.

- In FY 2013, ICE-HSI met its initial target with 42.6% of transnational drug investigations resulting in the disruption or dismantlement of high threat transnational DTOs or individuals. The FY 2014 target was 44%: [ONDCP FY 2015 Budget and Performance Summary](#)
- The EDTF achieved 240 indictments, 223 convictions, and the seizure of more than USD 72 million primarily from evidence developed in drug ML investigations in FY 2014.
- As of 2014, ICE-HSI had 610 open investigations involving TBML of which 442 involved countries which had been identified by the U.S. as being in the top 30 of countries vulnerable to TBML.

#### Representative cases:

**Vadim Trinchier et al. (2013):** This case dismantled a major illegal gaming operation and uncovered a Russian-American organized crime enterprise. The leader was charged with ML, racketeering and illegal gaming offenses, sentenced to 5 years imprisonment and ordered to forfeit USD 20 million in cash, investment and real estate. Another defendant was subject to a lower prison sentence and a forfeiture order of USD 6.4 million. 31 other alleged members and associates were also indicted and plead guilty. Agencies involved: FBI, IRS-CI, USAO/SDNY and NYPD.

**Operation Los Angeles Fashion District (2014):** This is an ongoing investigation aimed at disrupting and dismantling various major Black Market Peso Exchange and Mexican drug trafficking organizations laundering proceeds through TBML. The TTU initiative assisted in analysing the extent of the TBML activity. The operation resulted in confiscations of USD 90 million in bulk cash, USD 22.5 million in domestic bank accounts, USD 15 million in a foreign bank account, about USD 1.7 million in general property (vehicles, jewellery, and merchandise), and three properties worth about USD 10 million. Agencies involved: ICE-HSI, CBP, IRS-CI, FBI, DEA, FinCEN, multiple local police departments and USAO.

**Baja Money Laundering Organization (2014):** This case disrupted a ML organization that moved over USD 50 million annually in drug proceeds on behalf on Mexican-based DTO. The methods used to launder money included TBML, bulk cash smuggling, shell companies and wire transfers. Three key figures of the organization were arrested, plead guilty to unlawful money transmitting, and were sentenced to 1 year in prison. Approximately USD 208 000 was forfeited. Agencies involved: ICE-HSI, San Diego District Attorney's Office and California Attorney General's Office

#### *Emerging threats - Money laundering related to virtual currencies*

157. The 2015 NMLRA identifies virtual currencies as representing a potential emerging ML risk. In response to this risk, the U.S. has successfully investigated and prosecuted such activity.

**Box 9. Emerging threats of virtual currencies – Illustrative examples of results achieved**

**E-Gold (2008):** This case shut down ML and criminal activities through an alternative internet-based payment system which was found to be widely used by criminals to launder proceeds and carry out a whole range of criminal activities. Its executives plead guilty and, as of 2014, over USD 56.6 million has been forfeited from E-Gold accounts involved in criminal offenses. Agencies involved: USSS, FBI, DEA, HIS, IRSS-CI, USAO/DC and USAO/MD.

**Liberty Reserve (2013):** This case shut down a digital currency services provider platform that conducted about 55 million transactions (virtually all illegal) and laundered over USD 6 billion in suspected proceeds of crime. Several co-defendants pleaded guilty of ML. A wide range of pecuniary and prison sentences were applied to several defendants. USD 19.5 million were seized in bank accounts located world-wide including in Cyprus, Morocco, Australia, Spain and Hong Kong, China holding over USD 24 million. Agencies involved: USAO/SDNY, DOJ-Crim, USSS, IRS-CI, HIS and FinCEN.

*Types of ML cases pursued*

158. The authorities demonstrated that they prosecute and are able to obtain convictions for a range of different types of ML including the laundering of foreign predicate offenses, third-party laundering, stand-alone offenses and self-laundering. Specific initiatives focused on pursuing different kinds of ML activity help to generate positive results in this area. The assessment team based this conclusion on discussions with Federal prosecutors from New York and Washington, and numerous case examples.

159. In 2015/2016, FBI Headquarters identified ML facilitation as a stand-alone high priority threat. All FBI offices across the country are now required to incorporate this priority within the threat assessment of their own geographic areas. This focus on ML facilitation is intended to address third party money launderers, key facilitators, and ML networks laundering money for organized crime groups, drug cartels, and terrorist groups. The Asset Forfeiture and Money Laundering Section (AFMLS, see Chapter 1) has also implemented a *gatekeeper initiative* focused on prosecuting professional money launderers, complicit attorneys, accountants, FIs and their officers, managers, and employees, violators of the BSA, and those who launder the proceeds of serious criminal organizations such as drug cartels. The authorities prioritise pursuing ML activity in high-value and complex cases. Where it would be difficult to prove the substantive of ML, the authorities will often pursue the inchoate offense of ML conspiracy instead. This is especially evident for international or foreign predicate offending and inter-State offending.

**Box 10. Prosecuting different types of ML – Illustrative examples of results achieved**

**Laundering proceeds of foreign predicates: Haiti Telecommunication case (2011 -2012):** This case dismantled an international bribery scheme laundering the proceeds of foreign predicate offenses in the U.S. Two executives of a U.S. company were sentenced to 15 years and 84 months in prison for their role in a scheme to pay USD 890 000 in bribes to government officials at Haiti's State-



owned telecommunications company. They were convicted of charges including ML, conspiracy to commit ML, and violations of the FCPA. A USD 3.9 million forfeiture order was also issued. The Haitian officials were convicted of multiple counts of ML and ML conspiracy. Agencies involved: IRS-CI, FBI and USAO/SDFL.

**Third party ML: *Jiles Johnson (Operation Shattered Dreams) (2013)*:** This case dismantled a large-scale ML and DTO involving the laundering of proceeds by third parties (an accountant, auto dealer, real estate agent and financial planner). The defendant laundered drug proceeds through his restaurant with the help of other professionals, and was sentenced to 15 years for conspiracy to distribute cocaine and ML. The accountant and auto dealer were convicted of conspiracy to commit ML (sentenced to 6 and 10 years respectively), the real estate agent was convicted of structuring (3 year's probation), and the financial planner was convicted of interstate transportation in aid of racketeering (3 years). Agencies involved: DEA, USPIS, IRS-CI, Sandy Springs Police, OCDETF and USAO/NDGA.

**ML as a stand-alone offense: *Alvaro Lopez Tardón (Operation Las Tapas) (2010)*:** This case dismantled an operation laundering the proceeds of foreign predicate offenses (drug offenses) in the U.S. While no drugs ever entered the U.S. foreign drug trafficking is a predicate offense for domestic ML (18 USC §1956(c)(7)(B)(1)). The financial investigation revealed that this ML syndicate laundered over USD 14 million in narcotics proceeds in Miami by buying high-end real estate and exotic automobiles using the banking system to conduct international wire transfers directly to Tardón, funds wired to third parties, MSBs, cash couriers, and companies controlled by Tardón in Spain. More than ten cash couriers were involved in the ML enterprise. Tardón was convicted and sentenced to 150 years in prison to be served concurrently for one count of conspiracy to commit ML and 13 substantive counts of ML, along with a USD 14 million asset forfeiture and a USD 2 million fine. Agencies involved: FBI, IRS-CI, DEA, CBP, Miami Police, Monroe County Sheriff, USAO/SDFL, OCDETF.

**Self-laundering: *Mauricio Warner (2014)*:** This case shut down a wire fraud scheme where the defendant filed over 5 000 false tax returns using names and social security numbers of various individuals to claim millions of dollars in fraudulent tax refunds from the IRS. He was sentenced to 20 years in prison and ordered to repay over USD 5 million in restitution on mail fraud, tax fraud and ML counts. Seven bank accounts with over USD 4 million in funds derived from the scheme were forfeited. Agencies involved: IRS-CI and USAO/NDGA.

### *Effectiveness, proportionality and dissuasiveness of sanctions*

160. The range of case studies provided to the assessment team demonstrates that the courts will generally impose significant and dissuasive sentences in relation to serious instances of ML. In relation to top end cases, the courts appear to be imposing dissuasive sentences which in turn ought to encourage LEAs to pursue ML. The assessment team based these conclusions on: statistics of the number of ML charges, convictions and sentences; and numerous cases demonstrating convictions and sentences against natural persons and, to a much lesser extent, legal persons.

161. Over 10 000 unique defendants (natural/legal persons) were charged with violating one of the main ML statutes in 3,470 cases over FY2010-FY2014, including more than 2 000 cases with a charge of conspiracy to commit ML (18 USC §1956(h)). The average conviction rate is just under 60%, although rates vary across agencies. For example, around 80% of prosecutions derived from IRS-CI investigations result in conviction and sentences of imprisonment. In many instances, during the plea negotiation process, the ML charge is dropped which in part explains why the number of persons charged is so much greater than the number of persons convicted. When defendants have been convicted under 18 USC §§1956 or 1957, 40% of them received a sentence of 61+ months (over 5 years), 15% received non-custodial sentences. Life sentences have been applied (see Table 7).

Table 7. **Sentencing for Money Laundering Convictions (FY2010-FY2014)**

Offense	# of Defendants	Not imprisoned	1-12 Months	13-14 Months	25-36 Months	37-60 Months	61+ Months	Life
18 USC 1956	5 076	784	341	520	456	823	2 106	46
18 USC 1957	1 253	174	81	145	112	249	486	6

### *Alternative Measures*

162. Where a conviction for the substantive ML offense cannot be obtained (e.g. because the defendant is a foreign national residing outside the U.S. who cannot be located or extradited), the authorities can resort to the powerful tools under the USA PATRIOT Act and OFAC sanctions programs to apply economic sanctions against drug traffickers under the *Foreign Narcotics Kingpin Designation Act* (the *Kingpin Act*), and against significant transnational criminal organizations (TCOs) under Executive Order 13581 (E.O. 13581), thereby freezing their U.S. financial accounts, blocking their U.S. properties, and denying their access to the U.S. financial system. The *Kingpin Act* is used to target significant foreign narcotics traffickers and ML organizations considered the highest level risk offenders who have evaded arrest or may otherwise be outside the jurisdiction and reach of U.S. authorities, yet maintain assets in the U.S. The designations under the *Kingpin Act* and E.O. 13581 work in the same way as targeted financial sanctions under R.6. The designations have ramifications worldwide with foreign branches of U.S. banks abiding by the list and many foreign banks complying as well. In practice, this measure has effectively shut down some professional ML networks in the U.S and beyond. Violations of the Kingpin Act carry proportionate and dissuasive sanctions<sup>24</sup>. The U.S. provided multiple case examples of the application of the Kingpin Act and E.O.s.

<sup>24</sup> Up to 10 years in prison and civil penalties of up to USD 1 075 million per violation. For wilful violations: criminal penalties of up to 10 years in prison for individuals, and fines of up to USD 5 million. Upon conviction of a violation of E.O. 13581 or the Regulations: criminal fines of up to USD 1 000 000, imprisonment for up to 20 years, or both.

**Box 11. Achievements and Illustrative example of results achieved**

- Since the 1999 *Kingpin Act*, OFAC has designated 1 856 foreign persons (1 027 Individuals and 829 entities) around the world associated with 107 foreign drug kingpins under 150 separate sanctions investigations. Since 2011, six TCOs have been designated which has resulted in the derivative designations of 70 individuals and 13 entities under E.O. 13581.
- Under EO 12978, a precursor of the Kingpin Act which targeted Colombia-based drug traffickers, OFAC named over 1 700 persons (both individuals and companies) from October 1995 to July 2010 under 45 separate sanctions investigations.

**Rosenthal (2015):** In July 2015, OFAC designated three Honduran businessmen from the Rosenthal family and related businesses as Specially Designated Narcotics Traffickers pursuant to the *Kingpin Act* for providing ML and other services to support the international narcotics trafficking activities of multiple Central American drug traffickers. The OFAC action also targeted seven key Rosenthal businesses, including the first ever *Kingpin Act* designation of a bank. All assets that were under the jurisdiction of the U.S. or in the control of U.S. persons were frozen.

**163. The U.S. is rated as having a substantial level of effectiveness for IO.7.*****Immediate Outcome 8 (Confiscation)****Confiscation of proceeds, instrumentalities & property of equivalent value as a policy objective*

164. The Federal LEAs and prosecutors place a high priority on both criminal and civil forfeiture and seek orders forfeiting property of equivalent value as a policy objective. The assessment team based these conclusions on: the high value of orders obtained at a Federal level; reviews of the *National Asset Forfeiture Strategic Plan 2008-12* (the NAFSP); asset forfeiture summaries by key LEAs; discussions with a range of LEAs and prosecutors at the Federal, State and local levels; training guides provided by DOJ's Asset Forfeiture and Money Laundering Section (AFMLS) to Federal prosecutors; and case examples. The U.S. authorities have no data on the number of instrumentalities forfeited, or as to the number of value based confiscation orders made. They did, however, provide examples of cases involving the making of value based confiscation orders and the forfeiture of instrumentalities.

165. In terms of overall policy priority, the NAFSP referred to a long-term vision "to make the tracing and recovery of assets an integral part of every prosecution for the benefit of the American people realised". The NAFSP spoke of pursuing confiscation in appropriate cases and gave priority to the compensation of victims and to the AG's priorities which were: the effective use of forfeiture in terrorism cases; child exploitation cases; and corporate fraud. However no guidance was given as to when confiscation would be appropriate. The plan is no longer current although the assessment team was able to verify, talking to prosecutors from New York, Florida and Washington, that high-value asset recovery remains a priority in investigation and goes hand in hand with the "follow the money" approach adopted in all main asset generating investigations (see IO.7).

166. In extensive discussions with Federal LEAs, confiscation also came across as a Federal law enforcement priority that seeks to remove the tools of crime from criminal organizations, deprive wrongdoers of the proceeds of their crimes, recover property that may be used to compensate victims, and deter crime. All Federal LEAs confirmed that the dismantling of the financial infrastructure of criminal enterprises and other national security threats is essential to achieving their missions. This is reflected in their public priorities and the value of seizures they undertake each year<sup>25</sup>.

167. **AFMLS** seeks to ensure that forfeiture is pursued as a policy objective and is a goal of domestic and international law enforcement including via the assistance and training it provides. It has three litigating units which bring their own cases and assist U.S. Attorneys' Offices (USAOs) in their forfeiture cases. Consistent with this stated priority, Federal prosecutors and law enforcement agents are trained to conduct a financial investigation in every appropriate case and confirmed this to be a priority. AFMLS has a dedicated *Policy and Training Team* that publishes model curriculum for USAOs, and offers seminars, conferences, and other training in ML, forfeiture, financial investigations, complex case litigation, and other relevant topic areas. They administer AFMLS' intranet website, a resource containing legal resources and pleading samples used by practitioners nationwide. They also develop AFMLS' publications on asset forfeiture which are available online to prosecutors and agents across the country.<sup>26</sup> However it was not clear from the on-site visit that prosecutors were necessarily aware of the kind of guidance and information available or if indeed updates on policy practices and objectives would trickle down to them. In addition, it was unclear whether there was clear guidance as to when it was appropriate for confiscation at either Federal, State or local level.

168. The U.S. policy to pursue asset forfeiture has been supported by programs at both Federal and State/local levels. Individual States' confiscation regimes would benefit from ensuring i) that guidance on confiscation objectives and rationale is publically available in all States and ii) detailed confiscation data is collected and available.

### *Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad*

169. The authorities provided case examples demonstrating that the U.S. pursues confiscation using all of the asset recovery tools at its disposal and in all contexts, including in cases involving domestic and foreign predicate offenses, and in respect of proceeds which have been moved to other countries. The U.S. authorities were unable, however, to provide any data providing a breakdown of the number of asset recovery cases based on domestic or foreign predicate offenses, their value, or the type of offenses which led to the asset forfeiture orders being made. However, the authorities did

<sup>25</sup> [DEA, Asset Forfeiture Summary](#); [DHS/ICE, Asset Forfeiture](#); [FBI, Asset Forfeiture Summary](#); IRS, [Asset Seizure and Forfeiture](#); USSS, [Asset Forfeiture](#).

<sup>26</sup> See, e.g. [Asset Forfeiture and Money Laundering Statutes](#) (2015); Civil and Criminal Forfeiture Case Outline (2013); Federal ML Cases (2013); and Guide to Parallel Bankruptcy and Forfeiture Cases (2009). These resources are updated periodically and AFMLS intends that these books be used by Federal prosecutors and law enforcement agents for training and law enforcement purposes. Prosecutors are expected to conduct their own independent legal research, but these books, particularly the case outlines, address almost any conceivable forfeiture issue faced by prosecutors.

provide data on the seizures and forfeiture of foreign assets by Federal agencies going into DOJ's Asset Forfeiture Funds (DOJ-AFF).

170. The U.S. regularly enters into repatriation and asset sharing agreements with its domestic and foreign counterparts, and also regularly seeks restitution orders for victims. The assessment team based these conclusions on: discussions with LEAs and prosecutors at the Federal, State and local levels about what types of confiscation they pursue, in what circumstances, and with what results; numerous case examples which demonstrated that the U.S. is successfully able to confiscate high-value assets in a variety of circumstances; and statistics on asset sharing with other countries and victim compensation.

171. Asset recovery is facilitated by specialised units with training and expertise in confiscation, such as *AFMLS*, the *Kleptocracy Asset Recovery Initiative* (described in IO.1, Core Issue 1.2) and the *OCDETF Proactive Asset Targeting Team (PATT)* which works with OFC (see IO.6) to produce asset leads. The authorities also demonstrated during the on-site visit that they have a high degree of effectiveness in using the range of confiscation tools at their disposal: administrative forfeiture, non-conviction based forfeiture, and criminal confiscation (described in R.4). The Federal prosecutors typically resort to non-conviction based forfeiture (NCBF) in the first instance as it is easier to show probable cause as a basis to freeze or seize assets. Administrative forfeiture is also used, especially by Customs agents, and can easily proceed when it is not contested. NCBF is also used to provide MLA freezing and seizing assistance.

Table 8. Asset forfeitures by seizing agency and by type of forfeiture for FY2014<sup>27</sup>

Seizing Agency	Forfeiture Type	Seized Assets Count	Seized Value (USD)	Forfeited Assets Count	Forfeited Amount (USD)
ATF	Administrative	17 327	11 868 466.43	16 048	8 613 005.63
	Civil/Judicial	2 226	14 947 278.70	3 471	25 841 222.36
	Criminal	2 890	11 655 123.91	4 985	16 192 378.56
<b>ATF TOTALS</b>		22,443	38 470 869.04	24 504	50 646 606.55
DCIS	Civil/Judicial	7	1 723 367.07	6	1 988 909.36
	Criminal	24	1 131 854.74	31	1 401 107.12
<b>DCIS TOTALS</b>		31	2 855 221.81	37	3 390 016.48
DEA	Administrative	10 968	404 959 914.62	10 379	370 613 154.32

<sup>27</sup> Property is *seized* as a consequence of a violation of Federal law. Seized property can include monetary instruments, real property, and tangible personal property of others in the actual or constructive possession of the custodial agency. The value of seized property is its estimated fair market value at the time it was seized. *Forfeited* property is property for which title has passed to the U.S. Government. This property is recorded at the estimated fair market value at the time of forfeiture and is not adjusted for any subsequent increases and decreases in estimated fair market value. The value of the property is reduced by estimated liens of record. The amount ultimately realized from the forfeiture and disposition of these assets could differ from the amounts initially calculated.

Seizing Agency	Forfeiture Type	Seized Assets Count	Seized Value (USD)	Forfeited Assets Count	Forfeited Amount (USD)
3	Civil/Judicial	1 976	162 459 965.99	1 314	216 197 283.41
	Criminal	1 124	88 385 050.21	1 325	107 806 644.67
<b>DEA TOTALS</b>		14 068	655 804 930.82	13 018	694 617 082.40
DSS	Civil/Judicial	9	7 105 901.28	9	5 343 000.97
	Criminal	7	304 661.34	3	64 557.89
<b>DSS TOTALS</b>		16	7 410 562.62	12	5 407 558.86
FBI	Administrative	1 923	68 975 840.86	1 733	50 293 048.89
	Civil/Judicial	941	3 141 396 033.19	578	3 259 295 588.29
	Criminal	2 890	205 200 189.67	3 562	221 040 095.39
<b>FBI TOTALS</b>		5 754	3 415 572 063.72	5 873	3 530 628 732.57
FDA	Civil/Judicial	39	3 653 627.82	10	1 329 567.25
FDA	Criminal	49	69 414 707.12	67	69 153 425.38
<b>FDA TOTALS</b>		88	73 068 334.94	77	70 482 992.63
USMS	Civil/Judicial	30	630 327.51	19	616 874.62
	Criminal	196	7 152 910.84	216	6 671 618.62
<b>USMS TOTALS</b>		226	7 783 238.35	235	7 288 493.24
USPS	Civil/Judicial	128	5 915 189.05	82	6 952 539.96
	Criminal	187	13 160 253.22	300	46 813 002.84
<b>USPS TOTALS</b>		315	19 075 442.27	382	53 765 542.80
<b>TOTALS</b>		<b>42 941</b>	<b>4 220 040 663.57</b>	<b>44 138</b>	<b>4 416 227 025.53</b>

172. While the U.S. has demonstrated effectiveness in using these mechanisms in high-value cases, its ability can be impaired by the fact that not all predicate offenses include the power to forfeit instrumentalities. U.S. prosecutors have suggested that this barrier can be circumvented in some cases by starting a NCBF action based on ML, or by entering into a plea agreement whereby the defendant gives up his/her rights to the instrumentality notwithstanding the lack of a legal basis to do this. Performance would be further enhanced by filling in the legislative gap in this area. Additionally, there is no general power to obtain an order to seize/freeze property of corresponding/equivalent value which may become subject to a value-based forfeiture order prior to conviction (such power exists in only one federal judicial circuit—the Fourth—which covers nine federal district courts in Maryland, Virginia, West Virginia, North Carolina, and South Carolina). The result is that such assets are unlikely to still be available by the time a final forfeiture order is made. Addressing this shortcoming would further bolster asset forfeiture outcomes.



173. In FY 2014, the combined value of assets in the **DOJ Asset Forfeiture Funds (DOJ-AFF)** and **Treasury Forfeiture Fund (TFF)** asset forfeiture programs was about USD 4.6 billion (see table 9), a number that reflects the size of the U.S. economy, the overall risk profile and the extent of forfeiture activity taken by U.S. authorities. The figure fluctuated between USD 9.7 billion and 3.1 billion between 2012 and 2014. From year to year there are one or more very large settlements that cause the annual forfeiture figures to fluctuate.

Table 9. **Total Net Deposits to the Two Federal Forfeiture Funds, FY2012-2014 (in USD)**

	FY2012	FY2013	FY2014
<b>DOJ-AFF</b>	9 536 078 674	2 037 205 905	4 416 227 025
<b>TFF</b>	173 255 617	1 052 796 355	204 500 384
<b>Total</b>	<b>9 709 334 291</b>	<b>3 090 002 260</b>	<b>4 620 727 409</b>

174. U.S. Federal authorities obtained an annual average of 4 851 final orders in criminal cases for the FY2010-FY2015 period (see Table 10 below). Over the same period, the annual average of civil forfeiture orders was 4 919 and some of these orders will relate to on-going criminal prosecutions, but many will not. Other financial outcomes, such as fines and restitution orders not linked to a criminal forfeiture order, are also pursued in many cases. From FY2010-2015, USD 1.3 billion was collected from Federal defendants in restitution ordered to victims.

Table 10. **Federal Forfeitures 2010-2015**

	FY2010	FY2011	FY2012	FY2013	FY2014	FY 2015
<b>Criminal Forfeiture Order Count (more than one asset can be forfeited per order)</b>	4 054	4 628	4 894	5 326	5 121	5 084
<b>Number of assets forfeited pursuant to civil forfeiture judgments (judgments may pertain to multiple assets)</b>	3 470	2 537	7 513	5 552	5 482	2 538

175. The assessors were provided with a useful break down of Federal NCBF orders by district court. This showcased a wide range of outcomes with some courts doing little in the way of civil forfeiture while others obtained significant results. In the course of the on-site, the DOJ confirmed that judge's preferences and those of the U.S. Attorney will partly dictate the use of NCBF within individual Federal districts with some judges being reluctant to use it.

176. The U.S. also provided multiple examples of proceeds and instrumentalities being confiscated in relation to a wide range of crimes, including ML and TF. In the absence of a breakdown of forfeiture by underlying criminal offense, the extent to which confiscation has been obtained in respect of ML and predicate offenses for ML is unclear. It is also unclear how many of the orders relate to foreign predicate offenses.

## Box 12. Confiscation in different circumstances – Illustrative examples of results achieved

**Confiscation involving domestic predicate offenses**

**Roy McAllister (Operation Border Bandits) (2015):** This case stopped a marijuana trafficking business that brought bulk quantities of marijuana from Canada into Vermont, starting in the mid-2000s and continuing until mid-2013. The defendant made lavish expenditures with the proceeds of his drug trafficking. He was charged with filing false tax returns, conspiracy to distribute marijuana and ML. He pleaded guilty to the former two charges and was sentenced to 2.5 years in jail, fined 25 000 and ordered to forfeit almost USD 1 million in property and currency. Agencies involved: CBP, DEA, IRS-CI, ATF, ODETF and USAO/VT.

**Confiscation involving foreign predicate offenses**

**Edwin Fujinaga et al (2015):** This case dismantled a USD 1.5 billion fraud scheme in connection with a Ponzi scheme which defrauded thousands of investors living primarily in Japan. The defendants were ordered to pay over USD 580 million for defrauding clients, and to return over USD 2.3 million in investor funds. Agencies involved: FBI, SEC, DOJ Criminal Division (Fraud Section) and USAO/NV.

**Confiscation involving property that has been moved to other countries**

**LLB Vaduz (2011 -2013):** This case involved a bank in Liechtenstein assisting U.S. tax payers to evade their U.S. tax obligations by opening and maintaining undeclared accounts. Under the terms of a deferred prosecution agreement, the bank agreed to pay more than USD 23.8 million to the U.S. and also forfeited USD 16.3 million which had been paid to the bank in Liechtenstein as fees from the U.S. taxpayers. Agencies involved: USAO/SDNY, Main DOJ-Tax Division and IRS-CI.

**Confiscation involving property of equivalent value**

**Lebanese Canadian Bank (2011 -2013):** The U.S. commenced NCBF against Lebanese Canadian Bank (LCB) for its role in laundering the proceeds of an international drug trafficking network, seeking the seizure of USD 430 million on deposit at a bank in Lebanon that represented a portion of the purchase price paid for the acquisition of LCB's assets by another Lebanese financial institution. As Lebanese law does not allow for the seizure or repatriation of funds in Lebanon as part of a civil forfeiture action, the U.S. seized its correspondent accounts in the U.S. under 18 USC §981(k) and ultimately obtained NCBF of USD 102 million from the former LCB shareholders. Agencies involved: USAO/SDNY and DEA.

177. Domestic asset repatriation and restitution are managed at the Federal level by **DOJ-AFF** and the **TFF**. U.S. authorities prioritize making restitution to victims, and undertaking equitable sharing with Federal/State/local LEAs where they have contributed to the seizures/forfeitures, although this program was suspended at the time of the on-site visit<sup>28</sup>. Between FY 2010-2015, USD 2.9 billion in forfeited assets deposited into DOJ-AFF have been distributed to victims (see Box 13) through

<sup>28</sup> Payments under the program were re-started from April 2016.

remission and restoration. The overall priority of victim compensation and the means by which to do so are set out in guidance distributed to prosecutors, LEAs and support staff. The U.S. provided multiple case examples of victim compensation including in some of the cases cited above under both core issues 8.2 and 7.2; and others cultural property, art and antiquities.

#### Box 13. Restitution – Illustrative examples of results achieved

**Andrea Lorraine Avery (2014):** The case dismantled a multi-state mortgage fraud and money laundering scheme. The main defendant pleaded guilty to conspiracy to commit fraud, mail fraud affecting a financial institution, and conspiracy to commit money laundering. A seven year prison sentence applied as well as USD 10 323 369 in restitution to the FDIC. Agencies involved: IRS-CI, FBI, FDLE, USPIS, USAO/NDFL.

178. The TFF paid USD 93.3 million in restitution to victims in FY 2014, and USD 74.6 million in FY 2013. It also pays tens of millions of dollars each year to State and Federal LEAs and foreign governments for their participation in seizures that lead to forfeiture under TFF. During FY2014, the TFF shared USD 68.5 million with other authorities and another USD 921 000 with foreign countries. Asset sharing with other U.S. authorities went up to USD 408.2 million in FY2013, driven up by high-value cases. This has assisted in ensuring that there are sufficient resources to undertake asset recovery work. DOJ has shared USD 19.7 million forfeited assets with other countries in the last three fiscal years.

Table 11. DOJ-AFF- Distributions and Deposits in USD

Fiscal Year	Forfeiture Victim Compensation	Equitable Sharing Cash/Proceeds Distribution Amount to State and Law Enforcement	Assets Forfeiture Fund Deposits
2007	306 088 353	416 255 221	1 583 388 625
2008	451 672 140	440 432 098	1 327 604 903
2009	143 712 258	394 218 350	1 404 822 898
2010	298 622 572	389 842 469	1 600 370 705
2011	322 080 158	439 368 553	1 684 810 126
2012	1 496 270 214	446 368 553	4 221 909 505
2013	193 807 168	657 220 346	2 084 563 742
2014	294 600 487	425 261 026	4 473 669 260
<b>Total</b>	<b>3 506 853 487</b>	<b>3 609 261 435</b>	<b>18 381 139 764</b>

179. Most U.S. States have their own forfeiture laws which are used independently of Federal law. The overall Federal picture appears to be highly effective given the value of confiscation and the focus on following the money/asset forfeiture as a mean to combat crime and dismantle ML networks. Information provided indicates that State-level LEAs actively pursue confiscation of proceeds of crime, although the data was not as comprehensive as Federal level information and not uniformly available from one State to another.

*Confiscation of falsely or undeclared cross-border transaction of currency/BNI*

180. The authorities also actively pursue confiscation regarding cross-border movements of currency and bearer negotiable instruments (BNI) which have been falsely declared, not declared or disclosed. Their effectiveness is facilitated by special initiatives focused on bulk cash smuggling. The assessment team based these conclusions on: discussions with Customs and Border Protection (CBP); risks as described in the *Southwest Border Counternarcotics Strategy (2013)* and the *National Northern Border Counternarcotics Strategy 2014*; discussions with a range of LEAs and prosecutors at the Federal, State and local levels about what types of confiscation they pursue, in what circumstances, and with what results; and numerous case examples demonstrating that the U.S. is successfully able to confiscate currency/BNI in a variety of circumstances.

181. Falsely or non-declared cross-border movements of currency and BNI in violation of the law can and do result in confiscation and enforcement action. The southwest border is by and large the primary focus of bulk cash enforcement activity by U.S. authorities in line with the country's risk profile. Authorities focus on drug dollars that are being transported by or on behalf of Mexican drug trafficking organizations (DTOs) which dominate the supply and wholesale distribution of illicit drugs in most U.S. drug markets. Seizure of outbound undeclared bulk cash at U.S. southwest border ports of entry have trended down over the past several years according to statistical reporting by CBP. While the figures set out below convey a sense of effective prioritisation of the southwest border in line with the DTO risk, and a sense of volume, the assessment team was not able to fully grasp the weight of other points of entry and how these are prioritised. It is clear from *National Northern Border Counternarcotics Strategy 2014* that drug smuggling and bulk cash smuggling are vulnerabilities for the northern border as well but present a much lower risk as compared to the southwest border. The majority of smuggling activity that takes place along the northern border involves contraband such as narcotics.

**Box 14. Confiscations of illicit cash by CBP (2011-2015)**

- In 2011, CBP seized an annual average USD 34 million in illicit cash leaving the U.S. over the two year period March 2009 through February 2011, of which 97% (USD 64 million) was confiscated along the U.S.-Mexico border – leaving an estimated USD 2 billion of illegal cash seized through other border/entry points.
- The 2012 outbound currency seizure volume compared to 2011 fell to USD 32 million.
- Current statistics reported by CBP (June 2015)<sup>1</sup> continue to illustrate a year-over-year declining trend in outbound currency confiscation along the southwest border region, with 2015 total dollars seized down 42.5% compared to 2014.

**Note:**

1. State of the Southwest Border, CBP Office of Intelligence, June 2015.

182. Effectiveness in this area is enhanced by specialised initiatives which are specifically focused on targeting this type of activity such as the **Bulk Cash Smuggling Centre** (BCSC see IO.1), the ICE-HSI's **Operation Firewall** (in partnership with CBP, it targets the array of methods and means used to smuggle bulk cash) and the **Memorandum of Understanding with the Transportation Security Agency** (TSA - it assists the identification of suspicious movement of bulk cash in commercial air transportation).

**Box 15. Confiscation of falsely/not declared cross-border movements of currency—Illustrative examples of results achieved****Statistics:**

- Since its inception in August 2009, the BCSC has initiated 824 investigations, which have resulted in 648 criminal arrests, 431 indictments, and 319 convictions.
- Between FY2003 and FY2013, ICE-HSI bulk cash smuggling investigations led to the arrests of more than 2,300 individuals and seizures of more than USD 547 million.
- Since its inception in 2005 through March 2012, Operation Firewall has resulted in more than 6,613 seizures totalling more than USD 611 million, and the arrests of 1,416 individuals. These efforts include 469 international seizures totalling more than USD 267 million and 302 international arrests. *Source: 2015 NMLRA.*
- The BSCS MoU with the TSA has yielded 1 083 bulk cash seizures since 2014 totalling USD 43 033 650.

**Cross-Border Bulk Cash Smuggling Operation (2015):** This case resulted in a seizure of USD 824,899 concealed within a vehicle outbound from the U.S. towards Mexico. Agencies involved: HSI, CBP.

**Álvaro López Tardón (Op Las Tapas) (2014):** This case resulted in a seizure of USD 62 250 from one of Tardón's cash couriers who was smuggling proceeds via commercial aircraft.

*Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities.*

3

183. The authorities provided examples of actively pursuing confiscation in line with their risk profile, including cases involving: terrorism (as described in more detail in IO.10); laundering the proceeds of fraud (including healthcare fraud), drug trafficking, and transnational organized crime; and laundering the proceeds of foreign predicate offenses. However, there is very limited data available about what is happening at the State and local levels and Federal forfeiture statistics are not broken down by underlying criminal offense. These information gaps prevented the assessment team from getting a full picture of the totality of the U.S. efforts in this area. Consequently, it is not possible to conclusively assert that overall the authorities give priority to forfeiture of predicate offense and ML activity in line with threat/risks assessments set out in the 2015 NMLRA. At a Federal level it is likely that the emphasis on obtaining high value orders will result in confiscation orders being obtained in drug trafficking and high value frauds. At State and local level, some confiscation activity is undertaken by joint task forces, which are likely to be targeted at priority offenses. Other asset forfeiture activity at State and local levels is likely to mainly target drug trafficking, as this falls within all States' asset forfeiture legislation.

184. The assessment team based these conclusions on: the risks as identified in the NMLRA and national security strategies; a range of Federal LEAs and a number of prosecutors at the Federal, State and local levels about what types of confiscation they pursue, in what circumstances, and with what results; numerous case examples demonstrating successful confiscation of property in a variety of circumstances; and (limited) information about what is happening at the State and local levels.

185. The U.S. investigates and prosecutes ML and underlying ML activity in line with its risk profile as set out in core issue 7.2. All of the cases provided under IO.7 demonstrate that seizure and asset forfeiture are actively pursued in these cases. The authorities are successful in forfeiting assets even in complex and international cases, and are able to forfeit of a wide range of assets. Forfeiture of assets is also prioritised for TF (see IO.9 and IO.10 including cases examples provided there).

186. Although statistics of Federal confiscation orders broken down by offense are not available, the forfeitures carried out by Federal seizing agencies give a sense of volume per broad category of crime (see Table 8), depending on the agencies' remit and responsibilities. For example, the Food and Drug Administration (FDA) is responsible for forfeiture of a wide range of fraud including counterfeiting drugs, cosmetics and pharmaceuticals though healthcare fraud does not fall under its remit. The DEA has responsibility over drug offenses under Title 31 of the U.S. Code. The ATF oversees firearms related forfeiture (weapons not included) as well as proceeds from trafficking including smuggling of cigarettes. The U.S. Marshals (USMS) are the seizing agency for any money judgment but can have their own cases. The U.S. Postal Service (USPIS) will handle forfeiture related to mail fraud, and wire fraud which cover many ML cases. A breakdown of forfeiture carried out by the FBI also highlighted that FBI programs focus on higher risk areas such as complex financial crime, white collar crime, organised crime, criminal enterprise, public corruption, and the Latin American/South West border (for administrative confiscation) generate the largest amount of confiscation.



187. Other indicia give a sense of high prioritisation of confiscation by the U.S authorities notably the setting up of specific confiscation units and/or initiatives to target specific risk or threat. For example, the Kleptocracy Asset Recovery Initiative, established by the U.S. in 2010, currently has USD 2.8 billion in restrained assets, and has repatriated over USD 150 million to countries affected by crimes of corruption. The El Dorado Task Force seized more than USD 58 million primarily from evidence developed in drug ML investigations.

188. In the absence of more detailed national statistics and a breakdown of these by underlying offense type, it is difficult to assert that confiscation orders obtained accurately reflect the AML/CTF risks and national AML/CTF policies and priorities identified by the U.S. authorities. However agency-specific confiscations, FBI-specific data and confiscation achievements of specific task forces and initiatives indicate that they do.

189. **The U.S. is rated as having a high level of effectiveness for IO.8.**



## CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

### *Key Findings and Recommended Actions*

#### **Key Findings**

##### *Terrorism financing investigation and prosecution – TF offense (Immediate Outcome 9)*

1. Disrupting and preventing terrorist attacks before they occur is the top U.S. national security priority. The U.S. effectively approaches the threat of terrorism and its financing from both a global and domestic perspective.
2. Whenever LEAs pursue a terrorism-related investigation against individuals or entities, a parallel investigation is undertaken to identify potential sources of financial support. The U.S. is able to identify different methods of TF and the role played by financing networks, and to successfully investigate and prosecute such activity. The conviction rates are high and penalties applied in TF cases are effective, proportionate and dissuasive.
3. The CFT system is very well integrated into U.S. counter-terrorism structures, which facilitates inter-agency cooperation and coordination, including among Federal, State and local authorities. It also facilitates information-sharing and coordination between intelligence officers and LEAs on issues related to terrorism and TF.

##### *TF related targeted financial sanctions and NPOs (Immediate Outcome 10)*

1. The U.S. has frozen a substantial volume of assets and other funds pursuant to its targeted financial sanctions (TFS) programs and appears also to have kept terrorist funds out of its financial system to a large extent. Terrorism and its financing have the highest level of priority. The application of TF-related TFS is specifically mandated in the February 2015 National Security Strategy and the U.S. takes a leading role promoting their effective global implementation.
2. The U.S. proactively and comprehensively implements TF-related TFS and follows up all designations with a co-ordinated, cross-agency response to thoroughly identify and investigate the individuals/entities concerned. The U.S. has not implemented TFS against all individuals/entities designated by the UN pursuant to UNSCR 1267/1989 and 1988 and not every UN designation is implemented 'without delay' - although the great majority are. In practice, the impact of the missing designations has been minor.
3. There is extensive outreach and guidance to reporting entities and FIs in particular generally demonstrate a good knowledge of TF risk. Risks arising from the lack of beneficial ownership (BO) requirements are significantly mitigated by the inter-agency approach to detection and investigation of TF.
4. Measures applied to non-profit organization (NPOs) are risk-based, and focused on targeted outreach and engagement with NPOs most at risk for abuse by terrorists and the 2015 NTFRA found that concerted action has improved the resilience of the charitable sector to abuse by TF facilitators.

*Proliferation financing (Immediate Outcome 11)*

1. Like TF, proliferation financing (PF) has the highest level of priority. The application of proliferation-related TFS is specifically mandated in the February 2015 National Security Strategy and the U.S. takes a leading role promoting their effective global implementation. The U.S. implements TFS with the same proactive approach to developing proposals for designation as it does in the TF context. The U.S. follows up all designations with a coordinated, cross-agency response to thoroughly identify and investigate the individuals/entities concerned, and implements proliferation-related TFS comprehensively and without delay.
2. The U.S. has frozen a substantial volume of assets and other funds pursuant to its PF sanctions programs. There is extensive outreach and guidance to reporting entities and FIs in particular generally demonstrate a good knowledge of PF risk and are filing SARs related to potential PF. Risks arising from the lack of BO requirements are significantly mitigated by the inter-agency approach to detection and investigation of PF.
3. National coordination and cooperation among the U.S. authorities, at both the policy and operational levels, is a particularly strong feature of the system and mechanisms strongly support and reinforce the application of PF-related TFS by facilitating the identification of new potential targets for designation.
4. However, the U.S. has not implemented TFS in relation to 2 of the 32 individuals/entities designated pursuant to UNSCR 1718, and 29 of the 122 individuals/entities designated pursuant to UNSCR 1737 on the basis that there is insufficient information in relation to these names on which to base the U.S. process. In practice, the impact of these missing designations has been minor.

***Recommended Actions****Immediate Outcome 9*

1. The U.S. should continue its comprehensive CTF efforts, adapting to new threats as they emerge.

*Immediate Outcome 10*

1. Authorities should continue to work to ensure that all domestic designations of UN designated individuals and entities occur and are implemented without delay, and that the challenges posed by deficiencies in BO requirements are overcome by close cooperation and coordination and sharing of information and intelligence.
2. As violations of TF-related TFS are strict liability offenses, the authorities should continue to engage stakeholders on banking challenges that some NPOs may face when working in conflict zones. The U.S. could further improve the quality of NPO supervision.

*Immediate Outcome 11*

1. Authorities should continue to work to ensure that all domestic designations of UN designated persons and entities occur and are implemented without delay, and that the

challenges posed by deficiencies in BO requirements are overcome by close cooperation and coordination and sharing of information and intelligence. The U.S. should continue to enhance inter-agency cooperation and coordination, especially in relation to dual use goods and export controls.

4

190. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The recommendations relevant for the assessment of effectiveness under this section are R.5-8.

### ***Immediate Outcome 9 (TF investigation and prosecution)***

#### *Prosecution/conviction of types of TF activity consistent with the country's risk-profile*

191. The nature, diversity and scale of the TF cases pursued, and the volume of prosecutions between 2010 and 2015, are in line with the U.S risk profile and demonstrate that it is successful in achieving convictions in such cases. The assessment team based these conclusions on: statistics of the number of cases prosecuted and convictions achieved; discussions with prosecutors, the FBI and other LEAs; a review of the NTFRA; and numerous cases demonstrating what types of TF activity are pursued.

192. Between January 2010 and December 2014, the authorities convicted over 100 individuals of one or more TF-related offenses. The offense of knowingly providing material support or resources to a designated Foreign Terrorist Organizations (FTO - 18 USC § 2339B) is most often charged. Between January 2010 and December 2014, 70 individuals were convicted under this statute. During the on-site, specialist prosecutors confirmed that this is because this offense allows for effective TF prosecution and conviction without needing to prove any specific intent on behalf of the defendant to fund terrorist activity/acts. They also commented that some defendants may perceive less stigma in pleading guilty to the offense of '*undertaking unlicensed financial transactions with a Specially Designated Global Terrorist (SDGT)*' (50 USC § 1705) rather than the more explicit offenses of material support to terrorists, where both offenses have been charged.

Table 12. Terrorist Financing prosecutions<sup>29</sup>

Criminal charge	Number of individuals charged					
	2010	2011	2012	2013	2014	TOTAL
<b>18 USC 2339A: Providing Material Support for the Commission of Terrorist Acts</b>						
	9	10	6	4	4	<b>33</b>
<b>18 USC 2339B: Providing material support or resources to designated FTOs</b>						
	23	13	7	6	3	<b>52</b>
<b>18 USC 2339C: 2339C - Prohibitions against the financing of terrorism</b>						
	0	0	0	0	0	<b>0</b>
<b>18 USC 2339D: Receiving military-type training from a foreign terrorist organization</b>						
	4	1	2	0	0	<b>7</b>
<b>50 USC 1705: Undertaking financial transactions (including making/receiving contributions of funds, goods or services) with a SDGT</b>						
	2	0	0	1	0	<b>3</b>
<b>21 USC 960a: Narco-terrorism</b>						
	1	8	1	4	0	<b>14</b>
<b>TOTAL</b>	<b>39</b>	<b>32</b>	<b>16</b>	<b>15</b>	<b>7</b>	<b>109</b>

193. The U.S. provided multiple case examples illustrating how it proactively and aggressively investigates, prosecutes and convicts individuals involved in a wide range of TF schemes. The U.S. uses its broad criminal statutes to prosecute and convict activity that goes beyond merely financing a terrorist act, and includes providing material support to terrorist organizations (e.g. providing equipment, personnel and training). The different types of TF activity in these cases reflect the types of TF activity which were highlighted in the NTFRA. The authorities have also set up specific operations to stem the flow of foreign terrorist fighters.<sup>30</sup>

<sup>29</sup> The data provided in the various tables (Table 12, Table 13 and Table 14) reflect numbers of persons charged/convicted/sentenced with violations of specific TF-related statutes. Because complex terrorism cases often take several years between date of the initial charge and date of the trial/subsequent conviction, there will not be a 1 to 1 ratio of charges and convictions each calendar year. Equally, in complex cases, a conviction and subsequent sentencing can occur in different calendar years.

<sup>30</sup> E.g. collecting funds through the abuse of NPOs ; using MSBs to move funds; and financing terrorism with the proceeds generated from other crimes. These types of TF are highlighted in the NTFRA: p.35-45 (abuse of non-profit organizations), p.46-47 (moving funds using MSBs), p.28-35 (financing terrorism through proceeds generated from other crimes); p.44-45 and 57 (foreign terrorist fighters).



### Box 16. Types of TF prosecuted & offenders convicted - Illustrative examples of results achieved

#### Recent trends:

- The authorities report that targeted actions and outreach in the NPO sector have significantly reduced the misuse of NPOs, while other fundraising trends have consolidated (on-line, self-funding).
- Targeted awareness-raising and outreach has also seen a decline of misuse of FIs, while other means of moving funds have been on the increase.

#### Collection of funds, including through non-profit organizations

**Holy Land Foundation (2002-2009):** This case is one of several examples of the U.S. dismantling TF networks which used large tax-exempt charitable organizations. HLF operated as the chief U.S. fundraising arm of Hamas, a designated FTO, cloaking its financial support for Hamas by funneling money through other organizations in the West Bank and Gaza. HLF's principals were convicted of multiple charges (including providing material support to an FTO, tax and ML violations) and received substantial terms of imprisonment (the longest being 65 years). HLF was ordered to forfeit over USD 12 million. Agencies involved: USAO/NDTX, DOJ-AFMLS, FBI, IRS-CI, ICE-HSI, Department of State, USSS, U.S. Army CID.

**Operation Green Arrow (2007-2013):** This FBI initiative was aimed at stemming the flow of financing from the U.S. to al-Shabaab and other insurgents in Somalia by focusing on U.S.-based grass root fundraisers who purposed to act under the auspices of charitable giving. It resulted in multiple TF prosecutions and convictions. The defendants received sentences ranging from 10 to 20 years imprisonment. Agencies involved: FBI, JTTF, ICE-HSI, NYPD, USAO-SDNY, USAO-MA.

#### On-line fundraising

**Ahmad (2013):** This case shut down a London-based TF cell raising funds online. The defendant was sentenced to 150 months imprisonment for conspiring to provide and for providing material support, including funds, physical items, and personnel to terrorists in several locations including Afghanistan and Chechnya. U.S. residents were solicited and donate funds directly through these sites.

#### Movement of funds through unlicensed money transmitters and MSBs

**Saifullah Anjum Ranjha (2008):** This case is illustrative of U.S. efforts to identify and disrupt unlicensed money transmitters who may facilitate transfers of funds to terrorist groups. In an extensive sting operation, over USD 2 million was supplied to Ranjha and his associate for them to transfer abroad for the alleged benefit of Al-Qaida, al-Shabaab, and the Taliban. Ranjha pleaded guilty to conspiring to ML, concealing TF and operating as an unlicensed money transmitter and was sentenced to over 9 years in prison. The U.S. government seized approximately USD 2.2 million worth of assets. Agencies involved: USAO/DMD, FBI, IRS-CI, ICE-HSI.

**Financing terrorism with the proceeds of other crimes**

**Khan Mohammad (2008):** This case is illustrative of individuals raising proceeds for terrorists via criminal activities. Khan Mohammad was sentenced to serve two concurrent life sentences after being found guilty of several criminal statutes related to drug trafficking, including narco-terrorism charges (21 USC § 960a). This person served as both a local operations commander for the Taliban, coordinating attacks on U.S. and NATO troops, as well as assisting in moving large quantities of opium and heroin from Afghanistan to various destinations, including the United States.

**Khalid Ouazzani (2013):** This case is an example of a fraudulent activity being used to raise funds. The scheme involved submitting false financial information to obtain a loan, the proceeds of which were later provided for the use and the benefit of Al Qaida. Ouazzani was sentenced to 14 years imprisonment after pleading guilty to conspiracy to provide material support to a terrorist organization as well as ML and bank fraud. He was also subject to a fine up to USD 1 million and an order of restitution. Agencies involved: FBI, IRS-CI, Missouri Department of Social Services, Kansas City PD, USAO/WDMO.

**Foreign terrorist fighters**

**Operation Rhino:** This FBI-led operation is aimed at responding to the threat posed by persons traveling from the U.S. to join al-Shabaab in Somalia. Operation Rhino resulted in charges against more than 20 travellers and their facilitators. To date, the DOJ has convicted 10 defendants under this initiative, including facilitators who provided funds to pay for travel and weapons in Somalia. Agencies involved: FBI, JTTF, ICE-HSI, NYPD, USAO-SDNY, USAO-MA.

194. In the course of the on-site visit, the assessment team also discussed the issue of “home-grown terrorists” who do not hail from, work on behalf of, or take inspiration from FTOs. U.S. LEAs and prosecutors provided information and examples as to how they had identified and charged home-grown terrorists such as the Sovereign Citizen group as well as other domestic terrorists inspired by jihadist ideology. The prohibition against providing material support to terrorists (2339A offense), equally applies to domestic terrorists (including “home-grown” terrorists) as well as terrorists with an international connection.

*TF identification and investigation*

195. The U.S. has been successful at identifying TF in a number of ways including through its extensive and sophisticated use of financial intelligence and in the course of terrorism investigations which always incorporate a TF component. The assessment team based these conclusions on: statistics of the number of cases prosecuted and convictions achieved; discussions with prosecutors, the FBI and other LEAs, including specialised units focused on counter-terrorism; a review of the NTFRA; and numerous cases demonstrating what types of TF activity are pursued.

196. The U.S.’s ability to combat terrorism and TF is facilitated by specialised units and initiatives. The task force environment is particularly useful for enhancing information-sharing and expertise, and helping the authorities to conduct financial investigations effectively. Prominent examples of

this are the **FBI Joint Terrorism Task Forces (JTTFs)** which are 104 multi-jurisdictional FBI-led task forces established nationwide to conduct terrorism-related investigations with representatives from Federal, State and local LEAs. Local fusion centers also often support JTTFs and include their own SAR review team. The inter-agency National JTTF (NJTTF) ensures that information and intelligence flows freely among the local JTTFs and beyond. The JTTFs also coordinate closely with **FBI Terrorism Financing Operations Section (FBI-TFOS)** (described in Chapter 1, *Legal & Institutional framework*) which provides financial investigation and TF expertise to JTTFs with less experience in this area. The U.S. reports that FBI-led JTTFs have successfully disrupted more than 100 potential terrorist attacks in the last 5 years.

197. In addition to the powers described in R.31 and under IO.7, LEAs have **special investigative tools** for investigating terrorism and TF, including the *national security letter* (an administrative subpoena) which expands the FBI's authority to compel information for national security purposes and without pre-approval by a judge. Other powerful tools are procedures for requesting judicial authorization for electronic surveillance and physical searches of persons engaged in espionage or international terrorism against the U.S. on behalf of a foreign power, terrorist group or as a 'lone wolf': *Foreign Intelligence Surveillance Act (FISA)*.

198. TF investigations are also supported by **Department of Justice National Security Division (DOJ-NSD)** which oversees terrorism and TF investigations and prosecutions at the Federal level. It provides assistance in the course of the investigation and prosecution and approves all TF prosecutions, in coordination with all 94 U.S. Attorney's Offices (USAOs). NSD has extensive experience of working with the intelligence community and the use of intelligence in court proceedings, including managing sensitive information gathered under FISA. All USAOs work closely with JTTFs to bolster investigation and thus prosecution. The conviction rates achieved are symptomatic of the integrated and concerted approach to TF investigations.

199. The authorities consider outreach to the private sector critical to their CFT efforts. FBI-TFOS spearheads continuous outreach to the private sector, including: annual conferences bringing together 200 to 300 executives from domestic and foreign banks to exchange information on TF trends and threats; and semi-annual meetings with the 20 largest banks in the U.S. (representing 65% of U.S. transactions). JTTFs also conduct their own private sector engagement within their geographic remit. Extensive outreach has resulted in a cooperative information-sharing environment between the public and private sector, and better quality/targeted SARs. Examples of this were discussed during the on-site.

200. The authorities demonstrated numerous successes in being able to identify the specific role played by terrorist financiers (see cases above in Box 16 and below in Box 17).

## Box 17. Identification and investigation of TF - Illustrative examples of results achieved

## Statistics:

- FBI-TFOS initiated over 700 TF investigations since 2010, leading to over 120 convictions for TF offenses.

## Illustrative examples of cases which identified the specific role played by the terrorist financier

**ISIL Facilitator (2015):** A joint investigation and analysis initially highlighted an individual's role in collecting alleged ISIL-related money from approximately 20 countries and sending transfers to receivers in approximately 10 countries, many of whom were already associated with persons in the Terrorist Screening Database (TSDB). The individual's role was further identified jointly by the FBI and the National Targeting Center (NTC) using FinCEN Flash reports compiled from SARs and data submitted by U.S. businesses.

**Rmeiti Exchange (RE) & Halawi Exchange (2013):** RE used a car trade-based ML scheme to launder millions of dollars on behalf of narcotics traffickers & money launderers, and conduct ML activities for and provide financial services to a terrorist organization. Both exchanges operate outside the U.S., and were identified under section 311 of the Patriot Act as being of *primary money laundering* concern. Agencies involved: Treasury (FinCEN), FBI, DEA, CBP, New Jersey State Police.

**Times Square Bombing (2011):** Two unlicensed money transmitters separately transferred funds provided by Pakistani Taliban operatives in Pakistan to help finance the May 2010 attempted Times Square bombing. Although these individuals served as a source of support for terrorism, they did so unknowingly and, therefore, were not charged with terrorism or TF offenses, but were convicted of unlicensed money transmission. Agencies involved: FBI, CBP, NYPD, USAO/SDNY, USAO/MA, JTTF.

**The cases listed above in Box 16** also identified the specific role played by the terrorist financier(s).

*TF investigation integrated with -and supportive of- national strategies*

201. U.S. efforts to combat TF are extremely well integrated with and used to support national counter-terrorism strategies and investigations, including the identification and designation of terrorist, terrorist organizations and terrorist support networks. The assessment team based its conclusions on: the NTFRA, *National Security Strategy* and *National Strategy for Counterterrorism*; discussions with prosecutors, FBI and other LEAs, including specialised units focused on counter-terrorism; and numerous cases demonstrating what types of TF activity are pursued.

202. Preventing terrorists from raising, moving and using funds is a major component of the U.S. *National Strategy for Counterterrorism*, the main objective of which is to disrupt and prevent terrorist attacks before they occur. The U.S. efforts to combat TF are fully integrated into the strategy which means that, as a matter of policy, any terrorism-related investigation against individuals or entities is accompanied by a parallel investigation to identify potential sources of financial support. This is evidenced at the institutional level by the full integration of specialized financial investigation units into departments responsible for investigating terrorism. For example:

- FBI-TFOS** (which has just under 100 staff) is part of the **FBI's Counterterrorism Division** so as to better integrate financial information and investigation into wider counter-

terrorism investigations and prosecutions. FBI-TFOS agents are also embedded within the FBI **Counterterrorism Division's International Terrorism Operations Section (ITOS)** and threat cells, which manage priority threats and investigations.

- b) The prevalence of **JTTFs** across the country with fully-embedded IRS-CI expert forensics accountants demonstrates the high priority given to TF. JTTFs bring together 4 000 personnel from 50 Federal agencies, and over 600 State and local agencies. As noted elsewhere, the multi-agency task force model is very successful and widely-used in the U.S. system.
- c) To address narco-terrorism, FBI-TFOS has agents embedded within the relevant DEA specialist division, and holds regular meetings with counterparts in the DEA. The DEA also has a special **Counter-Narco-Terrorism Operations Center (CNTOC)**—a multi-agency section that coordinates all DEA investigations and intelligence related to narco-terrorism and ML linked to terrorist organizations. As well, the USAO in the Southern District of New York created a combined **Terrorism and International Narcotics Unit** to identify and prosecute global transnational threats.
- d) Central management and integrated monitoring by DOJ enhances the quality of terrorism and TF-related investigations and prosecutions in support of the country's goal to disrupt and prevent terrorism.

203. The U.S. has a comprehensive ongoing process of intelligence sharing. The intelligence produced by the field effectively informs policy priorities. Policy analysis is effectively pushed out to the field on an ongoing basis helping to identify and support ongoing investigations in an integrated fashion. Agency priorities are adjusted to reflect changes in national priorities. For example, there has been a recent focus on ISIL and foreign terrorist fighters (FTFs). Disrupting ISIL's finances is one of the nine lines of efforts in a cross government strategy to combat ISIL. This aims to disrupt ISIL's revenue streams in order to deny it access to funds, limit its access to the international financial system, and impose sanctions on its leadership and financial facilitators to disrupt their ability to operate.

204. In line with these priorities, U.S. LEAs also aggressively target the threat posed by FTFs. Key to this effort has been using financial intelligence to identify and target FTF facilitators and detain potential FTFs prior to travel. The FBI has established a **Foreign Terrorist Tracking Task Force (FTTTF)** which works with foreign partners, including Canada, Australia, and the United Kingdom. It has information sharing agreements with participating agencies, and the private sector to aid in locating terrorists and their supporters who are/have been in the U.S. The FTTTF has access to more than 70 sources of data including lists of known and suspected foreign terrorists and their supporters. It shares data with the U.S. intelligence community and other government agencies, including FinCEN and OFAC, to create a centralized database for use by FTTTF analysts. These efforts are generating concrete results. To date the U.S. government has filed charges in more than 60 FTF cases.

205. Likewise the CBP's **National Targeting Center (NTC)** is working on a FTF project aim to identify individuals traveling from the U.S., Australia, Canada, and the European Union to Syria and Iraq. NTC analysis identifies selectors and associates who may be of interest to law enforcement and

the U.S. intelligence community. As additional selectors and associates are found, NTC shares this information with its U.S. interagency partners, including the NJTTF, the NCTC, and FinCEN.

*Effectiveness, proportionality and dissuasiveness of sanctions*

206. The penalties applied are effective, proportionate and dissuasive. The assessment team based these conclusions on a review of statistics, cases and sentences in this area. Overall, the conviction rate in TF cases is high. Since 2010, over 85% of persons charged with a violation of 2339A and over 90% of persons charged with a violation of 2339B have been convicted of those offenses. In the few instances where a material support charge was dropped pursuant to a plea deal, or could not be proven beyond a reasonable doubt during trial, the defendants were still convicted of other accompanying criminal charges.

Table 13. **Terrorist Financing convictions**

Criminal charge	Number of individuals convicted					
	2010	2011	2012	2013	2014	TOTAL
<b>18 USC 2339A: Providing Material Support for the Commission of Terrorist Acts</b>						
	2	13	8	12	5	40
<b>18 USC 2339B: Providing material support or resources to designated foreign terrorist organizations</b>						
	13	22	17	10	8	70
<b>18 USC 2339C: Prohibitions against the financing of terrorism</b>						
	0	0	0	0	0	0
<b>18 USC 2339D: Receiving military-type training from a foreign terrorist organization</b>						
	1	1	2	1	1	6
<b>50 USC 1705: Undertaking financial transactions (including making/receiving contributions of funds, goods or services) with a Specially Designated Global Terrorist (SDGT)</b>						
	3	0	1	0	1	5
<b>21 USC 960a: Narco-terrorism</b>						
	0	0	5	4	0	9
<b>TOTAL</b>	<b>19</b>	<b>36</b>	<b>33</b>	<b>27</b>	<b>15</b>	<b>130</b>

207. The U.S. courts have imposed substantial sentences (both prison and fines) against convicted terrorist financiers. Any plea bargain would require the defendant to plead to the highest count, which traditionally includes terrorism or TF offenses. The application of sanctions is guided by sentencing guidelines and seem proportionate to the crime committed. When prosecution is successful, the government may request the court applies the special terrorism sentence enhancement which increases both the offense level (with a minimum offense level floor) and the criminal history category (U.S. sentencing guidelines: §3A1.4). It can be difficult to apply to a



terrorism financier as prosecutors must show by a preponderance of evidence that the defendant's conduct was intended to promote a Federal crime of terrorism (which includes the TF and narco-terrorism offenses), and the offense was calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. The judge will look at the intimidation element and try to assess whether the individual is dangerous. Still, terrorism sentencing enhancement has been applied in several TF cases. The U.S. has also imposed penalties on corporations convicted of providing funds to designated terrorist organizations or otherwise facilitating the movements of funds for the benefits of terrorist organizations.

#### Box 18. Sentence applied in TF cases - Illustrative examples of results achieved

##### Statistics:

- Between 2001-2013, providing direct material support to FTO carried an average 12-year prison sentence.
- Carrying out prohibited transactions with SDGTs carried an average 22 years prison sentence to date.

##### Sentences imposed against natural persons - Illustrative case examples

**Donald Ray Morgan and Shelton Thomas Bell** were sentenced to approximately 20 years in prison for attempting and conspiring to provide material support to ISIL as foreign terrorist fighters.

**Holy Land Foundation:** The sentences for the five defendants ranged from 15-65 years depending on their roles and the counts they faced (see Box 16).

##### Sentences imposed against legal persons - Illustrative case examples

**Chiquita Brands (2007):** Chiquita Brands International pleaded guilty in 2007 to violating IEEPA for making 50 illegal payments totalling over USD 825 000 to an organization in Colombia designated as a FTO and a SDGT. As part of the plea, Chiquita Brands was fined USD 25 million.

##### Application of Terrorism Enhancement Sentences - Illustrative case examples

**Khan Mohammad (2008):** The defendant was sentenced to life imprisonment, upon application of the terrorism enhancement, after being convicted of narcoterrorism for providing support to the Afghanistan Taliban. The Court affirmed the imposition of the terrorism enhancement considering that the defendant specifically intended to use the commission from the drug sales to purchase a car to facilitate attacks against U.S. and foreign forces in Afghanistan.

**Betim Kaziu (2014):** The defendant was sentenced to 27 years imprisonment, upon application of the terrorism enhancement, after being convicted of conspiring to commit murder overseas, conspiring to provide material support to terrorism, attempting to provide material support to a foreign terrorist organization, and conspiring to use a machine gun in furtherance of those crimes.

208. Below is a summary of the range of prison sentences applied between 2010 and 2014.

Table 14. Sentencing for Terrorist Financing Convictions (2010-2014)

# of Defendants	Not imprisoned	1-12 Months	13-14 Months	25-36 Months	37-60 Months	61+ Months	Life Imprisonment
<b>18 USC 2339A: Providing Material Support for the Commission of Terrorist Acts</b>							
38	0	0	0	0	2	34	2
<b>18 USC 2339B: Providing material support or resources to designated foreign terrorist organizations</b>							
60	0	0	2	5	8	43	2
<b>18 USC 2339C: Prohibitions against the financing of terrorism</b>							
2	0	0	0	0	0	2	0
<b>50 USC 1705: Undertaking financial transactions (including making/receiving contributions of funds, goods or services) with a Specially Designated Global Terrorist (SDGT)</b>							
5	0	0	0	0	1	3	1
<b>21 USC 960a: Narco-terrorism</b>							
11	0	0	0	2	3	4	2

*Alternative measures used where TF conviction is not possible (e.g. disruption)*

209. The authorities make good use of other criminal justice, regulatory or other measures to disrupt TF activities where it is not practicable to secure a TF conviction. These alternative measures include: pursuing other criminal charges, awareness raising and outreach, the use of targeted financial sanctions and civil enforcement actions. The assessment team based its conclusions on: statistics of disruptions, and discussions with the authorities about current trends in this area; and some illustrative case examples where alternative offenses have been pursued.

210. The U.S. authorities have effectively adopted a multi-agency “all tools” approach to aggressively target TF and terrorist facilitation, disrupt terrorist plots and dismantle terrorist organizations. The U.S. provided several cases where terrorists, would-be terrorist and/or terrorist financiers have been prosecuted under other statutes where a TF offense was not possible. The alternative offenses used have included: identify theft, immigration violations, tax crimes, making false statements, and unlicensed money transmitter. During the on-site, the authorities confirmed that false statement and immigration offenses in particular were especially effective for rapidly addressing the threats of potential terrorists, FTF or TF in the absence of a full-on investigation into a TF offense.

## Box 19. Illustrative Case Examples – Alternative Offenses

**Jonathan Paul Jimenez (2012):** This case involved someone raising funds to engage in FTFs activities via fraud. Jimenez was sentenced to 10 years imprisonment for making false statement to a Federal agency in a matter involving international terrorism and for conspiring to defraud the IRS. In order to fund his travel Jimenez had submitted a false 2010 tax return and obtained a refund from the IRS in the amount of USD 5 587.

**Aftab Ali (2010):** This case illustrates how charges of immigration document fraud and unlicensed money transmitting were successfully applied to sanction a terrorist financier. Ali provided USD 4,900 to Faisal Shahzad (perpetrator of the Times Square bombing attempt) through a 'hawala' transaction. Ali conducted money transmission business transactions (including the above transfer) without complying with Federal registration requirements related to money transmitters. He also entered the country in 2009 and defrauded the government by filing documents to adjust his immigration status in which he knowingly omitted his unauthorized employment. He pleaded guilty to unlicensed money transmitting and immigration document fraud.

211. The OFAC and Department of State designations under E.O. 13224 are also utilized effectively as a tool to disrupt TF activities. Such designations enhance the ability of DOJ prosecutors to pursue criminal charges for financial support provided to terrorists and terrorist organizations. Under E.O. 13224, U.S. persons may not engage in financial transactions with an SDGT unless they have first obtained a license from OFAC, nor may they engage in a transaction to circumvent the E.O., or make or receive any contribution of funds, goods, or services to or for the benefit of an SDGT.

**212. The U.S. is rated as having a high level of effectiveness for IO.9.**

### ***Immediate Outcome 10 (TF preventive measures and financial sanctions)***

#### ***Implementation of targeted financial sanctions for TF without delay***

213. Overall, the U.S. has a sophisticated system to implement targeted financial sanctions (TFS) without delay under the relevant UNSCRs. Using the legal framework described under R.6 (administered by OFAC and the Department of State's Bureau of Counterterrorism) the U.S. has demonstrated its ability to implement TFS within the context of: i) UN designations pursuant to UNSCRs 1267/1989 and 1988; and ii) national designations; and iii) responding to requests from third countries to take freezing action pursuant to UNSCR 1373. A total of 976 persons/entities were designated as SDGTs and remained listed on OFAC's *Specially Designated Nationals and Blocked Persons List* (SDN List) as of 31 December 2015 of which: over 300 were on the 1267/1989 Al-Qaida Sanctions list; 34 were on the 1988 Taliban Sanctions list; and approximately 600 were associated with other terrorist-related threats designated domestically by the U.S. pursuant to UNSCR 1373. A minor shortcoming is that the U.S. has not implemented TFS against all individuals and entities designated by the UN pursuant to UNSCR 1267/1989 and 1988 and not every UN designation is implemented 'without delay' although the great majority are. In reaching its overall conclusions, the assessment team: considered statistics on the number of designations proposed and made, and TFS

applied; and discussed with OFAC, Federal LEAs, and the private sector how targets are identified, how designations are made and communicated to the private sector, and how TFS are implemented in practice.

214. Strong cooperation and collaboration on TF issues among the regulatory, law enforcement, and intelligence communities facilitates the identification of individuals/entities suspected of being involved in TF activities, and who would be appropriate for designation (either domestically pursuant to UNSCR 1373, or at the UN level, or both). Potential designees are closely coordinated, vetted and de-conflicted across agencies to determine if the designation would actually assist in disrupting/impeding the activities of a larger terrorist network, and this process is well-aligned with agencies' operational and policy interests. The U.S. also takes a proactive approach to working with other countries to identify individuals and entities suspected of being involved in TF activities, and proposing and co-sponsoring proposals for designations to the UN.

215. The U.S. system incorporates many elements recommended in the *FATF International Best Practices: TFS Related to Terrorism and Terrorist Financing (R.6)*. Regardless of whether it is also seeking a UNSCR 1267/1989 or 1988 listing, the U.S. often requests countries to take domestic action in accordance with UNSCR 1373 (usually as part of a pre-notification process) to encourage a global response and reach areas otherwise not subject to U.S. jurisdiction. Since 2010, the U.S. has made 141 requests to other countries to take freezing action pursuant to UNSCR 1373 in relation to its own designations.

216. Where UN listings face delays, the U.S. often proceeds with a domestic designation under UNSCR 1373, to minimize the threat posed to the U.S. financial system by the designation target.

217. OFAC proactively and widely communicates designations to FIs immediately, rather than relying only on FIs to check the SDN List themselves. Several communication channels are used for banks (see R.6, criterion 6.5(d)) to facilitate the implementation of TFS without delay. OFAC maintains a hotline which banks, individuals, and organizations call to request guidance about potential sanctions, often in live transactions. This facilitates the freezing of terrorist-related assets and the clearing of false positives.

218. OFAC's SDN list is used by thousands of FIs across the U.S. and around the world to screen real-time transactions and accounts. U.S. regulators are able to enforce requirements imposed on U.S. and correspondent FIs wishing to do business in or through the U.S. Persons outside the U.S. can and often do voluntarily take the same actions that are required for persons under U.S. jurisdiction, and persons engaging in U.S. dollar-denominated transactions may be particularly likely to do so in order to avoid downstream legal complications in connection with the clearing of U.S. dollar-denominated instruments. This global reach of the U.S. sanctions regime reflects the size, complexity and international reach of the U.S. financial system. It is also an effective means of ensuring that U.S. designations pursuant to E.O. 13224 are widely implemented on a global basis, and enforcing U.N. designations pursuant to UNSCR 1267/1989 and 1988 internationally.

219. OFAC administers and enforces compliance with all U.S. economic sanctions programs, including TF-related TFS. Liability for breach of OFAC regulations is "strict liability" (meaning no proof of knowledge or intent are required) which creates a very clear focus on compliance. OFAC's investigative and enforcement authorities are exclusively civil in nature, as distinguished from the

criminal sanctions enforcement authorities exercised by the DOJ, DHS, and Department of Commerce in this area.

220. To complement OFAC's enforcement authorities, the FFRs also examine FIs for compliance with OFAC obligations (see core issue 11.4 for further detail). The 2006 mutual evaluation report raised concerns about the ability of OFAC to monitor compliance with sanctions, given the number of domestic designations (now more than doubled), the huge scope of their application (effectively, all persons in the U.S.) and the limited resources available to OFAC at the time to monitor compliance. Since then, enforcement appears to have become a priority, as is evidenced by a series of highly publicized enforcement actions involving the banks, mostly in relation to proliferation-related TFS (see IO.11 for more details). The evaluation team is satisfied that, while monitoring for compliance remains an ongoing challenge, OFAC is effectively meeting this challenge in collaboration with Federal and State regulators. OFAC, individually or in coordination with other Federal regulators, has also taken civil enforcement action against U.S. FIs for violations of the terrorism-related sanctions programs it administers.

#### **Box 20. Designations proposed/made and TFS implemented**

##### **Designations proposed/made by the U.S. since 2010:**

- Over 100 designations were proposed to the UN under 1267/1988 and 1989 of which 63 were proposed under UNSCR 1267/1989, and 35 were proposed under UNSCR 1988.
- The U.S. co-sponsored or acted as co-designee for 51 designations under UNSCR 1267/1989, and 23 designations under UNSCR 1988.

##### **Implementation of TFS:**

- A total of 976 persons/entities were designated as SDGTs and remained listed on the OFAC list as of 31 December 2015 of which: over 300 are on the 1267/1989 Al-Qaida Sanctions list; 34 are on the 1988 Taliban Sanctions list; and approximately 600 are associated with other terrorist-related threats designated pursuant to UNSCR 1373.
- The U.S. has not domestically designated 5 of the individuals/entities on the 1267/1989 Al Qaida Sanctions list, and 106 of the names on the earlier UNSCR 1988 (Taliban) Sanctions List.

##### **Enforcing compliance with terrorism-related targeted financial sanctions:**

HSBC (2013): HSBC reached a settlement with OFAC and agreed to pay USD 32 400 for processing three transactions in December 2010 and January 2011 totaling approximately USD 40 166 on behalf of a designated person (SDGT).

221. The U.S. has not implemented TFS in relation to all of the individuals and entities designated by the UN pursuant to 1267/1989 and 1988 (as was noted in 2006 during its last mutual evaluation). The U.S. justifies this on the basis that those UN designations (very early Taliban

designations) do not contain sufficient identifying information to make the listing of these names operationally constructive and do not meet the U.S. legal requirement for domestic designation. The U.S. is also of the view that listing these names would reduce the effectiveness of the system by generating an enormous number of matches for which there would be no practical way to ascertain whether funds/other assets of designated individuals and entities were being held. The assessment team considered this justification in the U.S. context including whether such an enormous volume of transactions are processed and cleared daily through the U.S. financial system and its network of correspondent banking relationships that bottlenecks could, conceivably, impact the global financial system. In concluding that this issue constitutes only a minor shortcoming in the U.S. context, the assessment team considered that:

- a) The U.S. has implemented TFS without delay (within a matter of hours) against 88% (135 out of 154) of the individuals and entities designated by the UN pursuant to UNSCR 1267/1989 and 1988 since 2010.
- b) The U.S. designated the entire Taliban group as an SDGT in 1999, whereby all individuals involved in that organization are deemed to be included, took significant action domestically in 1999 to freeze funds belonging to the Taliban as a group, including in relation to approximately USD 265 million held for the Government of Afghanistan in its account at the Federal Reserve Bank of New York (see Box 22 below).
- c) Since its last mutual evaluation, the U.S. has implemented TFS against all individuals and entities subsequently designated by the UN under UNSCR 1988 and almost all individuals and entities subsequently designated by the UN under UNSCR 1267/1989. This reflects that, since 2006, the Security Council has required a more detailed statement of the case and identifying information, which appears to align more closely with the U.S. domestic approach.

222. Not all domestic designations of UN-designated individuals and entities are achieved “without delay” (i.e. ideally within a matter of hours), although the great majority are, thanks to close coordination with the relevant UN committees, which is facilitated by the U.S.’s status as a P5 member of the Security Council. The U.S. reports that since 2010, 88% of the UN-designated individuals and entities have been domestically designated under E.O. 13224 without delay.

223. One challenge to effective implementation of TFS is whether FIs/DNFBPs understand who is the ultimate beneficial owner (BO) of a customer or party to a transaction. While the U.S. does not yet have a categorical requirement to identify the BO of a legal entity customer, the U.S. is able to significantly mitigate this technical deficiency in this context. Specifically, U.S. banks have a longstanding obligation to conduct EDD on customers that pose a high risk due to business activity or jurisdictions. In addition, OFAC requires financial institutions and DNFBPs to identify the ownership structure of customers to ensure they are not doing business with entities 50% owned by one or more sanctioned parties, including in the aggregate. In practice, this includes reviewing the extent to which a designated person may have a minority ownership interest or otherwise exercise control without a majority interest, as these entities may be subject to future designation or enforcement action. The U.S. also uses intelligence analysis and information provided by financial institutions from their due diligence to publicly identify and designate individuals and entities acting for or on behalf of designated persons.



*Targeted approach, outreach and oversight of at-risk non-profit organizations*

224. About 1.4 million tax-exempt organizations and an additional 300 000 houses of worship or similar public charities not required to apply for tax exempt status, account for a significant portion of the financial resources under control of the NPO sector, a substantial share of the sector's international activities, and include the types of NPOs within the FATF definition of *non-profit organization*.

225. The U.S. has in place targeted risk-based approach to NPO outreach, oversight, investigations and enforcement actions which are largely based on regular engagement with NPOs, intelligence, and TF investigations. This approach is broadly effective in terms of identifying, understanding and responding to the TF risks and appears to be generating results. The assessment team confirmed these conclusions through discussions with: service NPOs operating in the U.S., other civil society groups, the IRS, OFAC and Federal/State LEAs on issues including the TF risks facing the sector and emerging trends in this area; and the related risks described in the NTFRA.

226. The U.S. has a clear understanding of the risks of TF associated with the NPO sector, as described in the NTFRA and the U.S. takes a targeted risk-based approach to addressing the specific TF risks facing NPOs. This approach appears to be working. The 2015 NTFRA found that concerted action has improved the resilience of the charitable sector to abuse by TF facilitators. However, the large size and diversity of the U.S. charitable sector and its global reach means the sector remains vulnerable to abuse. Agencies consistently shared the view that U.S. efforts in this area had significantly reduced, but not eliminated, the risks of TF through NPOs.

227. NPOs involved with international funds transfers are considered to be at higher-risk for abuse by terrorists. The U.S. response is for enhanced information gathering from domestic and foreign NPOs seeking tax exempt status in the U.S., and considerably enhanced due diligence on international funds transfers. To facilitate this, the IRS redesigned Form 990 in 2008 to collect more information annually from NPOs concerning their stated mission, programs, finances (including non-cash contributions), donors, activities, and funds sent and used abroad. In line with the risks identified by the U.S. authorities, the extensive Schedule F of Form 990 now includes many categories of reporting requirements for charities with overseas activities.

228. A notable trend identified is individuals supporting various terrorist groups seeking to raise funds in the U.S. under the auspices of charitable giving, but outside of any charitable organization recognized as tax-exempt by the U.S. government. U.S. law enforcement responded to this emerging trend through a nationally coordinated campaign of investigations and criminal prosecutions targeting this specific TF method (see Box 16 - Operation Green Arrow case). Criminal charges and penalties are considered to be the most effective tool to stop this type of abuse, especially in the U.S. where substantial law enforcement resources may be deployed against such facilitators. Designations of NPOs by OFAC may be more effective against overseas entities, where the ability of U.S. law enforcement to arrest and prosecute terrorist facilitators is more limited.

**Box 21. Treasury Designations of NPOs – Illustrative case Examples**

As of 31 March 2016, Treasury and State have designated 56 charities, along with some additional branches and associated individuals, pursuant to E.O. 13224. Of these global designations, 8 relate to charities with U.S. operations. The U.S. has not designated a domestic U.S.-based charity since the Tamils Foundation in 2009. This decrease is consistent with the growing trend of fundraising under false pretences and outside of any charitable organization, and the authorities' increased use of the criminal offense of providing material support to FTOs.

**Al Rehmat Trust:** The Treasury designated a front foreign-based NPO (Al Rehmat Trust), operating in Pakistan pursuant to E.O. 13224 which was controlled by, acting on behalf of, and providing financial support to a UN-designated foreign terrorist organization (FTO) (Jaish-e Mohammed (JEM)).

**Tamil Foundation and the Tamil Relief Organization (TRO):** This case exemplifies the U.S. designations of two U.S.-based NPOs. U.S.-based Tamil Foundation was designated pursuant to E.O. 13224 for being controlled by, acting on behalf of, and providing financial support to a designated terrorist organization (the Tigers of Liberation Tamil Eelam (LTTE)). Over many years, the Tamil Foundation (based in Cumberland, Maryland) and TRO (another NPO designated for acting on behalf of LTTE) had comingled funds and carried out coordinated financial actions. The IRS suspended their tax-exempt status.

229. The U.S.'s ability to detect terrorist abuse of NPOs is facilitated by reporting requirements and regulatory oversight. The *IRS's Tax Exempt/Government Entities Division (TEGE)* has approximately 1,700 staff including approximately 690 examiners who can examine or review applications of tax-exempt organizations, for compliance with the U.S. tax laws and review their reporting forms. Its financial investigations unit composed of forensic investigators and specialists with financial expertise pursues cases of potential misuse of charities. Any potential TF concerns arising from intelligence (including SARs) or investigations can be fed into the TE/GE's examination program, although no statistics or examples were available. More complex illicit finance cases are handled in cooperation with other relevant U.S. government agencies and offices. IRS-TEGE monitors changes to the SDN List, and OFAC concurrently informs the IRS of any new U.S.-based designated charities which, in turn, will suspend the tax-exempt status of any charities which have been designated. IRS-CI can conduct criminal investigations, as they become necessary.

230. In addition to Federal authorities' oversight, all 50 U.S. States and the District of Columbia oversee the practices of charities domiciled/operating in their jurisdictions. Oversight practices vary from State to State and are directed at consumer protection issues. Thirty-nine of the 50 States require any charity raising money in their State to register with them. The statute permits some bilateral sharing of information as appropriate with State regulators, including on issues such as possible TF and fraud. State Attorneys-General have statutory jurisdiction over the charitable assets of these organizations and their fundraising activities.

231. In terms of the possible TF risks arising in the 300 000 or so houses of worship not required to file with the IRS for tax-exempt status, U.S. authorities are of the view that the applicable information requirements (e.g. at the State level), extensive outreach to the religious and other sectors (see below), and intelligence and investigative activity would nonetheless bring any TF concerns to light.

232. The U.S. provides extensive guidance related to dealing with charitable giving, humanitarian assistance and advice on risks associated with various aspects of the NPO sector. Targeted outreach to the sector appears to be a high priority for the IRS, DHS, Treasury (both TFFC and OFAC), the State Department, the FBI and other agencies. The range and intensity of the outreach is not only necessary, considering the huge scope of the NPO sector in the U.S., but is also a strength of the U.S. efforts in this area.

233. During the on-site visit, NPOs supported the view that controls in this area are strictly applied by both government entities and FIs through which NPOs' funds are moving. Positive feedback on the level of outreach by the Departments of Treasury and State was received, but some feedback indicated that the extent of engagement and oversight by regulators, particularly IRS, could be improved. In terms of access to financial services NPOs commented on the impact that strict liability for breaching TFS may have on banks' risk appetites, particularly when humanitarian aid is provided in conflict areas with higher TF risk.

234. Overall, the measures being implemented to ensure that NPOs are not abused by terrorists or terrorist financiers seem to be working effectively. Both the Federal and State level authorities take actions against illegitimate or fraudulent charities, or individuals posing as charities, particularly where they are able to demonstrate that these entities were established to facilitate TF. Measures applied to NPOs are risk-based, and focused on targeted outreach and engagement with NPOs most at risk for abuse by terrorists. Striking the right balance and avoiding the disruption of legitimate NPO activities can be challenging, particularly in higher-risk conflict zones. As violations of TF-related TFS are strict liability offenses, the authorities should continue to work with the NPO community to understand and mitigate the real TF risks that exist, while engaging stakeholders on banking challenges that some NPOs may face when working in conflict zones. The U.S. authorities are aware of the continuing challenges in this difficult area and are encouraged to continue their efforts, including work with the private sector.

#### *Deprivation of TF assets and instrumentalities*

235. The U.S. has frozen a substantial volume of assets and other funds pursuant to its TFS programs and appears also to have kept terrorist funds out of its financial system to a large extent.

236. OFAC is effective at shutting out designated persons from the U.S. system and depriving them of their assets, particularly given the global reach of the U.S. sanctions regimes. Once funds are blocked, they may be released only by specific authorization from OFAC. While the amounts currently blocked/frozen in the U.S. are reasonably large, they are not as large as they were in the past and are perhaps less than might have been expected given the size of the U.S. financial sector. However, the U.S. authorities argue that part of the reason for this is that the preventive nature of its TFS regime (including strict liability for violations and vigorous enforcement), coupled with other

actions taken to combat TF, seem to be having a deterrent effect. The authorities state that TF abuse of the U.S. financial system has decreased over the past 10 years.

237. Additionally, the DOJ uses a variety of tools to pursue and deprive terrorists, terrorist organizations, and terrorist financiers of assets related to TF activities. Forfeiture provisions expressly enable law enforcement to seize and forfeit *all* assets, *wherever* located, of *anyone* engaged in planning or perpetrating acts of terrorism—regardless of whether the property was involved in the terrorist activity or is otherwise traceable to that activity, as required by most other forfeiture statutes. Between 2011 and 2014, individuals convicted of terrorism-related criminal offenses were ordered by U.S. courts to forfeit assets in the following amounts: USD 1.75 million (2014); USD 5.195 million (2013); USD 30.27 million (2012); USD 38 000 (2011). Examples were provided of significant criminal, civil and administrative forfeiture of terrorist related assets and instrumentalities.

#### Box 22. Terrorists deprived of their assets – Illustrative examples

**Statistics:** As of 31 December 2015, blocked property and/or frozen assets in the U.S. relating to SDGTs or FTOs totalling approximately USD 37.6 million, including assets relating to Al-Qaida and Hizballah of approximately USD 13.0 million and USD 8.2 million respectively. OFAC has also blocked real property belonging to identified and designated organizations inside the U.S. that are branches of, or have been determined to provide support to or be owned or controlled by, designated terrorist groups or individuals.

**Action against Taliban-specific assets:** E.O. 13129 (effective 6 July 1999) was issued in response to the use of territory under the control of the Taliban by Usama bin Laden and Al-Qaida as a safe-haven and base of operations. It imposed trade sanctions and blocked property and interests in property of the Taliban and specified related persons if those assets were in or came within the U.S., or were/came within the possession or control of U.S. persons. About USD 265 million were blocked under this program. In 2002, the U.S. President issued E.O. 13268 terminating the emergency with respect to the Taliban because the U.S. military campaign in Afghanistan had ended the Taliban's territorial control. The Taliban and its leader, Mohammed Omar, were added to the E.O. 13224 Annex pursuant to E.O. 13268 which unblocked approximately USD 261.5 million in Afghan assets and turned them over to the Afghan Interim Authority between February and April 2002 as the Authority re-established control over Afghanistan. Also, other funds were unblocked due to licensing actions, delisting actions, and account maintenance/management fees. None of the approximately USD 265 million originally frozen by the U.S. was still blocked by OFAC as of 5 February 2016.

**Illustrative Case Examples of Confiscation in TF cases:** *Saade (2013)* shows the confiscation of all the defendant's assets following his conviction for conspiracy to provide material support or resources to the Taliban and conspiracy to acquire and transfer anti-aircraft missiles. The forfeited property included various items of jewellery, gold wafers, several wristwatches, a cell phone, and approximately USD 13 831.29 of U.S. and Iraqi currency.

*Consistency of measures with overall TF risk profile*

238. The measures implemented by the U.S. are extensive with significant international effects. There appears to be considerable consistency between the measures taken and the overall TF risk profile, as set out in the NTFRA, which notes that the wealth and resources of the U.S. continue to make it attractive to a wide range of terrorist organizations seeking to fund their activities. The central role of the U.S. within the global financial system, and the sheer volume and diversity of international FIs passing through U.S. FIs exposes the U.S. financial system to TF risks that other financial systems may not face. Also, while the vast majority of charitable organizations in the U.S. pose little or no TF risk, for those charitable organizations operating abroad or with overseas branches, particularly in high-risk areas where terrorist groups are most active, the TF risk is more significant.

**239. The U.S. is rated as having a high level of effectiveness for IO.10.**

*Immediate Outcome 11 (PF financial sanctions)**Implementation of targeted financial sanctions related to proliferation financing without delay*

240. The 2015 *National Security Strategy*, which is the government's highest level of priority, discusses applying TFS in response to the threat posed from proliferation of weapons of mass destruction (WMD). The U.S. vigorously implements TFS relating to combating PF. Only minor improvements are needed. The main areas of concern are the impact that deficiencies in beneficial ownership (BO) requirements may have on the ability of FIs and DNFBPs to identify the funds/assets of designated individuals/entities, and the fact that the U.S. has not domestically designated all of the individuals/entities designated by the UN.

241. Using a variety of authorities described in R.7 (particularly Executive Order (E.O.) 13382 on *Blocking Property of WMD Proliferators and Their Supporters*), the U.S. has designated over 700 persons and entities for supporting or facilitating WMD proliferation. OFAC's *WMD Proliferators Sanctions Regulations* (31 CFR Part 544), prohibit U.S. persons, meaning any U.S. citizen, permanent resident alien, entities organized in the U.S. (including their foreign branches) and any individual or entity in the U.S., from engaging or dealing in any transaction involving any person whose property or interests in property are blocked under E.O. 13382. Prior to the implementation of the Joint Comprehensive Plan of Action (16 January 2016), the U.S. had domestically sanctioned over 700 individuals and entities in connection with, inter alia, Iran's nuclear and ballistic missile program and support for terrorism, significantly more than on the U.N. list. The U.S. had also designated over 130 Democratic People's Republic of Korea (DPRK) individuals and entities involved in WMD proliferation or who are affiliated with the Government of North Korea, which is also significantly more than on the U.N. list.

242. OFAC advised the assessment team that the overwhelming majority of UN-designations are implemented in a timely manner. The U.S. implemented 90% (138 of the 154) of the UN DPRK-related and Iran-related listings without delay (within a matter of hours). As noted in R.7, criterion 7.1, the U.S. membership of the UNSC ensures that it is involved in all UN designation



processes and can coordinate its domestic process to coincide with the UN designation. OFAC indicated that, while the domestic designation process normally takes weeks or months, in extremely urgent cases, it can be started and finished within a few days.

243. The U.S. has designated 30 of the 32 individuals and entities on the UNSCR 1718 Sanctions List, and 93 of the 122 individuals and entities on the UNSCR 1737 Sanctions List. It justifies the gaps primarily on the basis that there is insufficient information in the UNSC process on which to base the U.S. process. The impact of these missing designations appears to be minimal although there does not seem to be any technical barriers to designating the missing persons. In the case of the missing 1737 designations, all of the 29 persons not designated by the U.S. are Iranian individuals and entities physically located in Iran. Given the comprehensive U.S. economic and trade embargo on Iran in place since 1995, these individuals and entities are already generally cut off from the U.S. financial system, and U.S. persons are largely prohibited from doing business with them. In practice, U.S. FIs would conduct additional diligence on any transaction involving individuals or entities located in Iran, and FIs are encouraged in OFAC guidance to contact OFAC in relation to any entities they suspect are owned or controlled by the Government of Iran that do not appear on OFAC's SDN List.

244. While E.O. 13382 is the primary authority for imposing TFS relating to WMD proliferators and their networks, the U.S. can also use country-specific authorities to target entities and individuals involved in proliferation-related activities: E.O. 13687 on *Imposing Additional Sanctions With Respect To North Korea* was issued in 2015, and broadens Treasury's authority to increase financial pressure on the Government of North Korea; and E.O. 13608 on *Prohibiting Certain Transactions With and Suspending Entry Into the U.S. of Foreign Sanctions Evaders With Respect to Iran and Syria* allows for additional targeting with respect to those countries.

245. Designations are communicated effectively to FIs and DNFBPs, as described under IO.10. As well, OFAC often sends e-mails informing relevant government agencies of designations. Although changes to the list are not always automatically communicated to relevant Federal, State, and local agencies which may have information about non-financial assets subject to TFS, they are immediately available on OFAC's public website, and all such agencies are U.S. persons with the same obligation to comply with TFS that private citizens do.

246. There are two areas of strength in the TFS regime which go beyond the strict requirements of the FATF Standards but which are relevant to and enhance its overall effectiveness: the international effects of the U.S. sanctions regime (as described in IO.10); and the effective integration of the TFS regime into the U.S.'s broader counter-proliferation efforts (outlined below). Reflecting the size, complexity and international reach of the U.S. financial system, and the requirements imposed on U.S. and correspondent FIs wishing to do business in or through the U.S., the OFAC sanctions regime has a positive effect on the implementation of UN sanctions *in other countries*, making it more difficult for UN-listed individuals and entities to raise, move and use funds or to procure financial services. This in turn has a preventative or hardening effect for the U.S. implementation of TFS, as it helps to keep the funds/other assets of designated persons/entities out of the U.S., and also provides further information and intelligence to help to identify networks and/or funding channels associated with proliferators.



*Identification of assets and funds held by designated individuals/entities and prohibitions*

247. The U.S. has had significant success in identifying the funds/other assets of designated persons/entities, and preventing them from operating or executing financial transactions related to proliferation (see Box 24). The U.S. employs a comprehensive process to identify and designate persons/entities and implement TFS programs, coordinated by the Departments of the Treasury and State. Treasury's Office of Intelligence and Analysis (OIA) plays an important role in helping OFAC to identify potential targets and take effective follow-up action by analysing all-source information to identify the specific financial vulnerabilities of WMD proliferators and their support networks. OIA engages as appropriate with the broader U.S. intelligence community (of which OIA is a full member), and with international partners.

**Box 23. Illustrative Example in Identifying Individuals and Assets**

- As of 31 December 2015, the U.S. had frozen approximately USD 1.98 billion of assets related to the government of Iran including assets related to entities involved in Iran's proliferation activities.
- The U.S. has frozen approximately USD 35 million of assets related to the government of the DPRK including assets related to entities involved in the DPRK's proliferation activities.

**Karl Lee (2007-present):** Karl Lee and his primary business were designated pursuant to E.O. 13382 in 2006 and 2009 respectively for providing supplies to entities affiliated with Iran's ballistic missile program and for contributing to Iran's nuclear program. Both were added to the SDN listing. Lee was forced to operate much of his business covertly using other companies to conceal his activities. In 2014, he was indicted on multiple criminal charges, including violations of economic sanctions by using U.S. based FIs to engage in millions of dollars of otherwise-prohibited U.S. dollar transactions, conspiring to commit fraud and money laundering and wire fraud in connection with illicit transactions. U.S. authorities also announced the seizure of over USD 6 895 000 in funds attributable to the Lee front companies and the filing of a civil complaint seeking the forfeiture of those funds. These actions were complemented by concurrent OFAC designations (SDN listing) of eight additional front companies used by Lee and the addition of nine China-based suppliers to the Department of Commerce Entity List.

**Bank Melli<sup>1</sup> (2007):** Bank Melli was designated pursuant to E.O. 13382 for providing banking services to entities involved in nuclear and ballistic missile programs, including entities listed by the UN for their involvement in those programs. In 2008, OFAC further designated two shell companies, Assa Corp and Assa Ltd, for providing support to Bank Melli. Through these companies, Bank Melli held a 40% ownership of an office tower located at 650 5th Avenue. U.S. authorities filed a complaint seeking forfeiture of this share, and later filed for forfeiture of the remainder 60% ownership held by Alavi Ltd, based on its support to Bank Melli, in violation of TFS. In 2013, U.S. courts ordered forfeiture of 650 5th Avenue and bank accounts related to building, resulting over USD 500 million being seized, and an income stream used to support proliferation activities being closed down.

**Note:**

1. Bank Melli is no longer on the OFAC SDN List because they were delisted pursuant to the Joint Comprehensive Plan of Action (JCPOA). They are now on the E.O. 13599 List but are no longer considered designated.

4

248. The designation process is only an initial step in a coordinated, cross-agency response to proliferation activities which begins with a thorough investigation of the person/entity involved in proliferation activities, and includes engagement with partner governments to shut the activity down. If this is unsuccessful, the U.S. may designate the person/entity, but continue to investigate its proliferation activity. Such investigations help to prevent designated persons/entities from operating or executing proliferation-related transactions, and assist in the identification of other persons/entities for designation.

249. The National Security Council (NSC) manages the inter-agency policy making process for counter-proliferation, and Treasury's involvement ensures that PF is a part of that framework. Inter-agency coordination extends to operational cells, such as the DHS's Export Enforcement Cooperation Center (E2C2), which aims to enhance enforcement efforts and minimize enforcement conflicts by coordinating efforts to detect, prevent, disrupt, investigate, and prosecute violations of U.S. export control laws, including proliferation-related activity. Through these coordinating bodies, U.S. agencies share intelligence and law enforcement information related to countering proliferation and its financing, and deciding on the best response. This enhances the effectiveness of the TFS regime. The Department of State also coordinates U.S. government interdiction efforts across the policy, enforcement and intelligence communities through its four State-chaired interagency working groups focused on nuclear, ballistic missile, chemical and biological weapons, and conventional arms interdictions, and a CP finance team.

250. Within DHS, the Counter-Proliferation Investigations (CPI) program of Immigration and Customs Enforcement (ICE) oversees a broad range of investigative activities related to export violations. It prioritizes programs targeted at trafficking in WMD materials, sensitive dual-use commodities, and technologies sought by proliferating countries and terrorist groups.

251. The Office of Export Enforcement (OEE) (see IO.1) works cooperatively with the exporting community to prevent violations, and conduct investigations to gather evidence supporting criminal and administrative sanctions. BIS alerts exporters and FIs of entities of concern through the development and publication of specific lists containing unique requirements for dealing with such entities (i.e. the Denied Persons List, the Entity List, and the Unverified List).

252. OFAC has provided training and outreach to LEAs and has a hotline for law enforcement on TFS issues. Several components of the DOJ also contribute to inter-agency counter-proliferation efforts. The FBI's Counterproliferation Center (CPC) combines three CP-related components into a single jointly managed entity at FBI Headquarters to disrupt global proliferation networks: the WMD Directorate (which provides scientific expertise); the Counterintelligence Division (which provides operational expertise); and the Directorate of Intelligence (which provides analytical expertise). The FBI's work feeds into the efforts of OFAC to monitor for compliance with TFS requirements, and sharing of information is common.

253. FinCEN plays an important intelligence support role in investigations of TFS violations, and by issuing public and non-public advisories on sanctions issues to reporting entities. FinCEN has worked to refine its business rules to detect SARs that may relate to PF, and the FBI makes use of FinCEN data (to which it has direct access) to complement other sources of information.

254. The assets of designated persons/entities must be frozen immediately and reported to OFAC within 10 days, and U.S. persons (including FIs/DNFBPs) are generally prohibited from engaging in financial transactions with those persons/entities. The obligation to freeze (block) property is very broad, as described in R.7, criterion 7.2(b). Under OFAC's "50% Rule", any entity owned 50% or more in the aggregate by one or more blocked persons/entities is also considered blocked, regardless of whether it is listed on OFAC's *SDN List*. The 50% Rule limits the ability of designated persons/entities from acting through front companies in which they have an ownership interest, even if that front company has yet to be designated. OFAC expanded the reach of the 50% Rule in 2014 by including aggregated ownership, directly or indirectly, by one or more blocked individuals/entities.

255. Blocked property may include, but is not limited to, bank accounts, financial portfolio holdings, trusts, real estate (commercial or personal), vehicles, and other physical items. Where appropriate, OFAC issues licenses to allow for the effective management of real estate while it is subject to blocking. OFAC can also license or authorize access to frozen property or accounts on a case-by-case basis to ameliorate the effects of the designation, permit access by a designated person to his assets to the extent necessary for basic or extraordinary expenses, and authorize transfer into the U.S. of non-frozen assets which prevents them from being frozen upon receipt by a U.S. person. The evaluation team was satisfied that the framework for and implementation of the licensing regime is in accordance with the international standards.

256. OFAC has additional powers to:

- a) issue *targeted blocking orders* to interdict funds belonging to a designated person transiting the U.S. financial system
- b) serve *blocking notifications*, concurrent with a designation, on U.S. persons who OFAC may have reason to believe have extensive involvement with the designated person/entity or who may have a high likelihood of dealing in the blocked property or interests in property of such persons/entities, and
- c) issue *cease and desist orders* to U.S. persons regarding conduct that is prohibited by any sanctions program—such as engaging in a dealing in blocked property or with a designated person/entity—when OFAC has reason to believe that a U.S. person has engaged in such conduct, such conduct is ongoing, or may recur.

257. Under E.O. 13608, Treasury has the authority to impose sanctions where it appears that a *foreign* person violated U.S. sanctions on Iran (or Syria) but may not meet the E.O. 13382 designation criteria. This enables the U.S. to limit the risk to its commercial and financial systems posed by foreign persons determined to have violated U.S. sanctions. An EO 13608 designation also allows Treasury make public globally such foreign persons' activity and the risk of similar future activity. Treasury has designated 13 entities linked to Iran under E.O. 13608.

258. In addition to using TFS, FinCEN may require U.S. FIs and domestic financial agencies to take certain “special measures” if the Director of FinCEN finds that a foreign jurisdiction, foreign FI, class of transaction, or type of account, is of *primary money laundering concern* (see s.311 of the PATRIOT Act). A number of factors, including evidence that WMD proliferators have transacted business in the jurisdiction, may bring FinCEN to more closely consider that foreign jurisdiction. For example, in November 2011 FinCEN issued a Notice of Finding under section 311 indicating it had reason to believe that: Iran directly supported terrorism and was pursuing nuclear/ballistic missile capabilities; relied on State agencies or State-owned or controlled FIs to facilitate WMD proliferation and financing; and used deceptive financial practices to facilitate illicit conduct and evade sanctions. The practical effect for U.S. FIs was to provide additional guidance to help them identify transactions and actors of concern.

259. DOJ can use asset forfeiture laws to seize and forfeit significant assets that would otherwise be used to provide support to WMD proliferators. For example, one forfeiture provision allows for the forfeiture of any property constituting, derived from, or traceable to any proceeds obtained from an offense against a foreign nation, or any property used to facilitate an offense involving trafficking in nuclear, chemical, biological, or radiological weapons technology or material. In 2013, DOJ obtained the forfeiture of substantial U.S. assets controlled by the Government of Iran, including an office building in New York City valued at USD 525 million, seven additional properties and bank accounts (*Case: 650 5th Avenue (2009-2014) - New York, NY*).

#### *FIs and DNFBPs’ understanding of and compliance with obligations*

260. The obligations arising from the OFAC listing process apply equally to all U.S. citizens and businesses, including all FIs and DNFBPs. Although wilful and inadvertent breaches of the requirements do occur, the competent authorities report that, in general, TFS are being implemented well by obliged entities. During the on-site, the assessors discussed TFS with a wide range of FIs/DNFBPs and, overall, they appear to be well understood and implemented.

261. The obligation of FIs to implement TFS is an absolute strict liability one. Still, OFAC recommends that FIs understand their risk, context and potential vulnerabilities to effectively comply with TFS requirements. Depending on the institution’s size and sophistication, and the specific financial products/services it offers, many U.S. FIs/DNFBPs use software in order to screen their customer database, in-process transactions, and other pertinent information in an effort to identify the involvement of, or property belonging to, persons, countries, or regions subject to OFAC’s sanctions programs.

262. One challenge to effectively implementing TFS is whether FIs/DNFBPs are implementing CDD measures sufficient to understand who is the ultimate BO of a customer or party to a transaction. This is the same issue discussed in IO.10 in relation to how well the private sector is implementing terrorism-related TFS. As noted under IO.10, the U.S. significantly mitigates this risk in this context.

263. OFAC conducts substantial outreach to FIs and other entities to explain its sanctions programs and ensure compliance, and maintains a hotline which banks, individuals, and organizations call into daily requesting guidance, often with questions about potential sanctions for live transactions. OFAC receives well in excess of 90 000 calls on its hotline each year, and responds to thousands of inquiries

each year through its compliance email address. It has also published more than 450 FAQs dealing with questions across all sanctions programs, and issued specific guidance to help FIs and other businesses comply with WMD proliferation-related TFS by identifying potential sanctions evasion activity.

264. FinCEN has also issued guidance to help FIs understand the activity-based financial prohibitions and vigilance provisions in WMD-related UNSCRs. In June 2010, it issued an advisory on the continuing illicit finance threat emanating from Iran which incorporated aspects of the FATF guidance on activity-based financial prohibitions. Similarly, in July 2013, FinCEN issued an advisory on DPRK which referenced the latest FATF guidance in an effort to clarify DPRK's specific risk associated with diplomatic personnel and cash couriers. FinCEN can use the powerful information gathering and sharing mechanisms available under section 314 of the PATRIOT Act (see IO.6) to identify and report activities that may involve PF.

265. The FBAs, which have also signed an MOU for sharing OFAC related information, are responsible for examining to ensure compliance by U.S. banks and U.S. branches of foreign banks with OFAC sanctions programs. The FBAs also provide guidance to these institutions.

266. Other U.S. government agencies also work with FIs to improve their understanding of how to detect proliferation-related financial activity. For example, the **FBI's WMD Directorate** conducts outreach to FIs (including on-site visits by FBI personnel) on how to identify PF activity and drafts useful SARs that can be used by LEAs to further proliferation-related investigations. The FBI's WMD Directorate is also working with FinCEN on guidance for FIs on how to identify PF activity. These extensive outreach, guidance and regulatory efforts appear to have been successful in assisting U.S. financial and other institutions to understand and comply with TFS and to identify transactions that may involve designated persons/entities. FIs met by the evaluation team demonstrated a good understanding of their obligation to implement TFS, particularly in the banking sector, where proliferation-related assets are most likely to be found. To a lesser extent, the DNFBP sectors also demonstrated awareness of these obligations.

#### *Competent authorities ensuring and monitoring compliance*

267. OFAC effectively administers and enforces compliance with all U.S. economic sanctions programs. Its *Economic Sanctions Enforcement Guidelines* (the Guidelines) set out the range of enforcement responses available to OFAC, the general factors that OFAC may take into consideration when determining the appropriate administrative action, and the method for determining an appropriate civil monetary penalty for a violation, given the particular facts and circumstances. OFAC's investigative and enforcement authorities are exclusively civil in nature, as distinguished from the criminal sanctions enforcement authorities exercised by the DOJ, DHS, and the Department of Commerce.

268. While OFAC is not itself a regulator, its basic requirement is that all U.S. persons including FIs not violate the laws that it administers. OFAC has entered into memorandums of understanding (MOUs) with the following regulators for the sharing of OFAC information: the FBAs, the Internal



Revenue Service (IRS)<sup>31</sup>, and over 30 State banking regulators. The FFIEC Manual establishes policies and procedures for U.S. bank examiners in examining for compliance with OFAC requirements and obligations. OFAC and the FBAs work closely together and coordinate joint enforcement actions against certain FIs, and/or exchange information regarding upcoming enforcement actions or examinations that identify issues with a particular FI's OFAC compliance program. OFAC has conducted training for bank, MSB and other examiners at the Federal and State levels.

269. The FFIEC Manual notes that as a matter of sound banking practice and in order to mitigate the risk of non-compliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program that is commensurate with their OFAC risk profile. Evaluation of TFS compliance is frequently included in BSA/AML examinations including a review by examiners of how the bank screens names against the OFAC SDN List, both for accountholders and account parties other than accountholders (which may include beneficiaries, guarantors, principals, beneficial owners or nominee shareholders), and the process for blocking/rejecting transactions involving designated persons/entities. Supervisors have identified a need for some supervised entities to do more to detect assets of entities acting on behalf or at the direction of a designated person/entity and report any failures to do so to OFAC.

270. Since 2007, the FBAs, in concert with OFAC, DOJ, and other State and local LEAs and regulators, have pursued enforcement actions against multiple FIs for failure to maintain effective OFAC compliance programs. For example, in March 2015, the BGFERS announced an enforcement action and imposed a USD 200 million fine against a foreign FI because, among other reasons, it “lacked adequate risk management and legal review policies and procedures to ensure that activities conducted at offices outside the United States complied with applicable OFAC Regulations.”

271. OFAC conducts its own civil investigations and, if appropriate, imposes administrative penalties on U.S. persons, including FIs that fail to properly block/freeze funds, assets, property, or interests. Depending on the underlying statutory authority, civil monetary penalties can range up to USD 1,075 000 for each violating transaction. Additionally, in appropriate circumstances OFAC may refer a matter to the appropriate LEAs for criminal investigation and potential prosecution. Criminal penalties for wilful violations can include fines ranging up to USD 1 million and imprisonment of up to 20 years. OFAC, individually or in coordination with other Federal regulators, has taken civil enforcement action against FIs and other actors for apparent violations of proliferation-related sanctions although the vast majority of enforcement actions have not involved imposing civil monetary penalties however see box below for case examples of public enforcement activity.

---

<sup>31</sup> OFAC has also delegated to the IRS (Treasury Directive 15-43) authority to conduct reviews for compliance with U.S. economic sanctions. [IRS OFAC compliance Exam Procedures](#).



**Box 24. Illustrative examples of OFAC PF-related public enforcement activity.**

-In March 2015, a foreign FI reached a settlement with OFAC and agreed to pay approximately USD 258 million for multiple apparent violations of U.S. economic sanctions laws. A small subset of these apparent violations included the processing of 142 U.S. dollar transactions through the U.S. that appeared to have been for or on behalf of, or otherwise contained an interest of, a sanctioned party between September 2008 and January 2010.

-In June 2015, a U.S. company settled with OFAC and agreed to pay USD 391 950 for shipping goods purchased by a customer in China on a blocked vessel in April 2009, and for several financial transactions associated with the shipment that were also apparent violations of U.S. economic sanctions laws.

4

272. **The U.S. is rated as having a high level of effectiveness for IO.11**



## CHAPTER 5. PREVENTIVE MEASURES

### *Key Findings and Recommendations*

#### *Key Findings*

1. The financial sector in the U.S. is huge and complex with a large number of institutions. Covered institutions, particularly banks, securities sectors, and MSBs have an evolved understanding of ML/TF *vulnerabilities* and obligations and have put in place systems and procedures (some quite sophisticated) to understand, assess and mitigate these vulnerabilities. Investment advisers (IAs) are not directly covered by BSA obligations. Some IAs, however, are indirectly covered through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements. Non-coverage of the remainder of the sector is a significant vulnerability identified by the U.S. authorities.<sup>32</sup> Life insurance companies appear to understand the vulnerabilities associated with the products covered by the AML regulations.<sup>33</sup>
2. There are TC gaps, specifically exemptions and thresholds, which are not in line with the risks especially in the context of the U.S. as one of the world's largest financial systems. Although the NMLRA notes structuring as a risk, the SAR reporting thresholds do create opportunities for structuring which, while the U.S. argues they exist by design, were originally not subject to a ML/TF risk assessment but put in place on the basis of relief from regulatory burden. Overall, the TC gaps, exemptions and thresholds in the BSA regime collectively soften the deterrent value of preventive measures. This is compensated, to an extent, by the LEAs' ability to access SAR and other FIU data directly, which is a strong feature of the system.
3. In the DNFBP sector, casinos have developed a good understanding of risks and obligations and apply preventive measures. There is increased focus from the authorities on the sector due to identified vulnerabilities. However, apart from casinos (and to some extent, dealers in precious metals and stones), no other DNFBP sector is comprehensively covered under the AML/CFT framework. All nonfinancial trades and businesses in the U.S have the Form 8300 large cash transaction reporting obligation, allowing voluntary reporting of suspicious transactions, are subjected to targeted financial sanctions and can be subject to a GTO. However, the understanding of risks in the DNFBP sector, other than casinos, is uneven. Addressing the regulatory gaps of certain minimally covered DNFBP sector would improve availability of financial intelligence and strengthen the deterrence factor of U.S. preventive measures.
4. The SAR reporting thresholds make it optional for smaller value suspicious transactions to be reported to FinCEN, and this gap is only somewhat mitigated by the obligation to report some transactions immediately to LEAs and file a SAR. Further, the 60/30 day period for

<sup>32</sup> Investment adviser Notice of Proposed Rulemaking (NPRM)

<sup>33</sup> The "covered products" are those the Treasury Department identified as presenting a sufficient AML risk to justify regulation. "Covered products" include: permanent life insurance policies, other than group life insurance policies; annuity contracts, other than group annuity contracts; and any other insurance product with features of cash value or investment.

reporting suspicious activity cannot be said to be promptly; however, in practice the median time taken by reporting entities to file SARs is 17 days; within the 30 day window.

5. Lack of BO obligations remains a significant gap in the regulatory framework, though FIs, such as banks and broker-dealers seem to be taking steps to identify BOs as part of their risk management efforts.
6. Information exchange is happening actively and is facilitated by the USA PATRIOT Act between authorities and the financial sector, and among FIs. This is an important feature of the U.S. system.

### ***Recommended Actions***

1. The U.S. should introduce beneficial ownership preventive measures as soon as possible, continuing previous efforts to bring these regulations into force.<sup>34</sup>
2. The U.S. should finalize its current rulemaking process to bring IAs under the comprehensive AML/CFT framework.
3. On the basis of a specific vulnerability analysis, appropriate AML/CFT obligations particularly relating to CDD and SAR filing, should be imposed on lawyers, accountants, and trust and company service providers as a matter of priority. After analysis of the current GTO outcomes, appropriate action should be taken to address the ML risks in relation to high-end real estate.
4. FinCEN, IRS-SBSE and State regulators should continue their focus on casinos, including the IRS-SBSE examination work, and expand it to include some of the smaller and less sophisticated players.
5. The U.S. should operationalise casinos' participation in information sharing under the USA PATRIOT Act s314(a) and further encourage their use of s314 (b) for better information sharing.

273. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The recommendations relevant for the assessment of effectiveness under this section are R9-23 and elements of R1, 6 and 29.

### ***Immediate Outcome 4 (Preventive Measures)***

274. In terms of risk and context, not all sectors are of equal importance in the U.S. system. As a result, the assessors did not place the same weight on the impact of implementation issues (both positive and negative) equally across sectors. The assessors' views of the relative importance of each sector, based on risk and context are outlined below, and informed the overall conclusions about the implementation of preventive measures.

<sup>34</sup> Since the on-site, the Final CDD Rule that includes a BO requirement was published on 11 May 2016. The implementation period for the Rule is two years. (see <https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx>)

275. The **banking sector** plays a predominant role in the U.S. and the international financial system. The global dominance of the U.S. dollar generates trillions of dollars of daily transaction volume through U.S. banks, exposing them to significant ML/TF vulnerability. The sector is enormous with a large number of banks of varying size and diversity. The complex regulatory regime (multiple supervisors and Federal/State regulation) creates challenges for the sector's implementation of AML/CFT requirements. Three categories of State-licensed and supervised banks are not subject to an AML Program requirement, but this is a minor gap as these banks do have CIP, CTR, and SAR requirements and the size of this sector is relatively very small.<sup>35</sup>

276. Next in line in relative importance is the securities sector, which is also huge in asset size with a large number of players. It comprises several sub-sectors, the principal ones being the broker-dealers, mutual funds and IAs. In the U.S., IAs manage customer assets valued at over USD 67 trillion, and are not directly covered by BSA obligations. Some IAs, however, are indirectly covered through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements. To that extent, the risk is also partially mitigated in that IAs do not execute transactions on their own, but instead do so in conjunction with FIs that are already subject to BSA requirements, and many do not generally have physical custody of client funds or securities. Nonetheless, as underlined by the U.S. authorities in their Notice of Proposed Rulemaking, *"such broker-dealers and banks may not have sufficient information to assess suspicious activity or money laundering risk"* and *"such gaps in knowledge make it possible for money launderers to evade scrutiny more effectively by operating through IAs rather than through broker-dealers or banks directly"*. Accordingly, U.S. authorities state that *"IAs may be uniquely situated to appreciate a broader understanding of their clients movements of funds through the financial system because of the types of advisory activities in which they engage"* and that *"IAs have an important role to play in safeguarding the financial system against fraud, money laundering."* Consequently, given the enormous size of the sector in terms of number of entities and assets under management, FinCEN has issued a proposed rule to impose AML Program and SAR reporting requirements on IAs. FinCEN has identified this sector as one of its top priorities for rule making<sup>36</sup>.

277. **MSBs** operating in the U.S. are large in number and diverse in size and nature, ranging from large and sophisticated entities to small operations. This is also an important sector, given the vast volume of cross-border remittances processed annually.

278. The **casino sector** in the U.S. is large, and has been identified in the NMLRA as being high risk. Casinos are subject to a robust AML/CFT regime, and in recent years, this sector has had an increased focus on preventive measures.

279. In relation to **DNFBPs** other than casinos, only **dealers in precious metals and stones** have BSA requirements, including AML programs, but not SAR reporting. Large cash transaction reporting (Form 8300) requirements, including the ability to voluntarily report suspicious transactions, and

<sup>35</sup> FinCEN has a rulemaking nearing completion to address this issue (see <https://www.gpo.gov/fdsys/pkg/FR-2016-08-25/pdf/2016-20219.pdf>)

<sup>36</sup> In August 2015, FinCEN proposed a rule requiring certain IAs to establish anti-money laundering (AML) programs and report suspicious activity to FinCEN pursuant to the Bank Secrecy Act (BSA). FinCEN also proposed to include IAs in the general definition of FI.

targeted financial sanctions laws apply to all businesses in the U.S. including DNFBPs, and they can be subject to a Geographical Targeting Order (GTO). Although GTOs are not preventative measures and are temporary in nature, they are a comprehensive tool that the authorities can use to gather information on vulnerabilities. Trust companies (professional trustees) are defined as FIs for the purposes of the BSA and are therefore covered by AML/CFT requirements applying to FIs.

280. **Lawyers, trust & company service providers (TCSPs), and to a lesser extent, accountants** can play an active role in preparation for and the formation and activities of legal persons and legal arrangements, though they are not required to form companies in the U.S. Lawyers also play a role in real estate and other transactions. Legal persons (and to a lesser extent, legal arrangements) are at risk of abuse by criminals and terrorist financiers, and are often used in complex ML schemes. Real estate is used as an investment vehicle by legal persons for concealing and laundering criminal proceeds. Given these vulnerabilities, the fact that lawyers, TCSPs, and to a lesser extent, accountants are not subject to an appropriate range of AML/CFT requirements is a serious gap; however minimal obligations noted in paragraph 279 above as well as the ethical obligations placed on lawyers and accountants, mitigate some of these risks.

281. **Real estate agents** are involved in negotiating transactions and, therefore, fall under the *FATF Recommendations*, but are not subject to comprehensive AML/CFT requirements. In addition, there are other gatekeepers in the sector which have not been risk-assessed (e.g. cooperative associations and condominium associations who also play an active role). The U.S. considers that the gap is mitigated by the fact that real estate agents do not handle financial transactions directly. However, as noted in the TC annex at c.22, State laws require real estate agents to keep financial transaction records so it is doubtful they are not involved in financial transactions. The U.S. also asserts that the risk in the real estate sector is mitigated because RMLOs and banks in the context of mortgage financing are covered by AML/CFT requirements. However, for the reasons noted further below, the assessors do not agree this is an effective strategy. Further, lawyers would generally handle the financial aspects of such transactions. In addition, particularly at the high-end of the market, purchasers often use legal persons to hold real estate and the opaqueness of legal persons (see Chapter 5) is a vulnerability which can be exploited by illicit actors.

282. **Life insurance companies**, agents and brokers represent a low risk in the U.S. context, as do **dealers in precious metals and stones**. The principal financial products in the life insurance sector assessed as vulnerable to ML and TF are investment/savings products associated with life insurance policies. These insurance products can be accessed by the policy owner to add or withdraw cash or other assets and in this respect they are similar to deposit accounts and investment accounts at securities dealers, and are subject to AML program obligations. The AML Program Rule *inter alia* requires development of internal policies, procedures, and controls to ensure compliance with all AML obligations; the designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs.

283. The lack of comprehensive AML/CFT obligations on the FIs/DNFBPs listed above has a negative cascading impact on the effectiveness of preventive and supervisory measures (IO.3 and IO.4), and in the analysis of technical compliance (R.10 to 13, 15 to 23, 26, 28 and 34-35). Other technical deficiencies in the legal framework also impact how effectively FIs/DNFBPs are



implementing AML/CFT measures. Of these, the most important is that FIs/DNFBPs are not required to systematically collect and verify BO information in all cases; although FIs met during the on-site do collect but not verify BO. This has a negative impact on effectiveness, particularly for Core Issues 4.2, 4.3, and 4.4.

284. The assessors based their conclusions on IO.4 on, *inter alia*: discussions with a range of types and sizes of FIs and DNFBPs correlating to the sectors defined by the FATF on how they understand, manage and mitigate their risks, and how they implement preventive measures (prescribed or otherwise); reviews of their internal manuals and procedures; discussions with supervisors, regulators and SROs about their supervisory manuals, their understanding of risks and how well each sector is managing risks and complying with AML/CFT requirements, reviews of the NMLRA, NTFRA and other risk material and industry guidance.

### *Understanding of ML/TF risks and AML/CFT obligations*

285. Covered FIs/DNFBPs are required to develop and implement an AML/CFT program that is commensurate to their risk exposures. They identify, assess and periodically review their risks, in line with their own line of business, customer base, products and services offered, and geographic footprint. Generally, amongst the FIs met with at the on-site, the AML/CFT program requirements appear to be well understood in principle, and in practice this facilitates the development of an understanding of risks. However, beyond the basic AML/CFT Program Rule (which applies to all Covered FIs/DNFBPs), other prescribed requirements vary across sectors.

286. The banking and securities sectors have the most comprehensive AML/CFT obligations. MSBs and casinos are also subject to extensive AML/CFT requirements and basic customer identification requirements, based on ML/TF risk, apply. Other sectors (e.g. dealers in precious metals and stones, lawyers, accountants, TSCPs, and real estate agents) are minimally covered (see paragraph 279). These sectors were deemed by the U.S. to pose a low risk- a view shared by those sectors. The following are some examples of how different sectors understand their risks and relevant AML/CFT obligations.

287. Institutions in the **banking sector**, a key gatekeeper to the U.S. financial system, generally have a strong understanding of their ML/TF risks and AML/CFT obligations, and have in place AML policies and procedures commensurate with that understanding of risk. The FFIEC Manual sets out a menu of potential risks, but makes it clear that such risks will vary from bank to bank according to the organization's line of business, customer base, products and services offered, and geographic footprint. Banks are required to review their risk assessments periodically and typically do so annually. They are also required to update their risk assessments to identify changes in their risk profiles. Risk self-assessment reports include an evaluation of data pertaining to the bank's activities (e.g. number of domestic and international funds transfers, locations of business area and customer transactions) and customers, including CDD information. Banks risk rate their customers, as part of their compliance program. Banks met during the on-site demonstrated that their understanding of ML/TF risks and obligations has penetrated to all levels (including senior management), and generally is not limited to the staff directly responsible for executing the day-to-day AML/CFT responsibilities. The BSA/AML risk assessment is usually reviewed with the direct involvement of

senior management to determine that it is adequate, and risks are properly identified and mitigated via the AML program. Boards of directors, chief executives, and senior managers are informed on a regular basis of the AML/CFT program and related controls.

288. In the **securities sector**, broker dealers are subject to similar requirements and, as in case of banks, the level of risk and the specifics of each broker-dealer's AML program vary, depending on the size, activities, products offered, and customer base.

5

289. **MSBs** met on-site had in place AML/CFT programs based on an analysis of risk, including agent risk, and demonstrated a good understanding of sector risk and their own operational risk. Their boards and senior management are trained and are part of the approval process for risk assessments and programs. State regulators confirmed that MSBs have an understanding of their risks and apply appropriate measures. The unregistered remitter initiatives of the U.S. authorities (detailed in IO.3), including enforcement actions resulting therefrom, have mitigated the risk in relation to smaller entities.

290. The **casinos** met on-site had a good understanding of risks and obligations. The American Gaming Association (AGA) works to assist the sector by putting out useful best practices guidance. The recent study on *Investing in America's Financial Security: Casinos' Commitment to AML Compliance* commissioned by the AGA provides a good picture of the understanding of the casino sector and the mitigating measures they have put in place.

291. In the **life insurance sector**, assessors met with a large company that had a good understanding of its ML/TF risks associated with insurance products with features of cash value or investment, which are the products covered by the U.S. AML rules. The company applies a group wide approach to assess its ML/TF risks.

292. During the on-site, the assessors developed the following concerns about certain disconnects between how FIs/DNFBPs and the authorities understand ML/TF risks and corresponding obligations:

293. **Residential Mortgage Lenders and Originators (RMLOs):** The risks of ML through the real estate sector are well documented in the NMLRA (and the 2005 NMLTA before that). The authorities (including FinCEN) informed the assessors that these risks are dealt with at the intersection of the real estate and financial sectors, by applying AML/CFT requirements to RMLOs—a sector which handles the financing of a majority of retail real estate transactions processed in the U.S. However, the assessors believe this approach is incomplete. First, RMLOs only represent one side of a real estate transaction (the purchaser) and thus do not have the broader oversight on all parties to the transaction. Second, RMLOs met on-site did not appear to have a holistic understanding of the risks of ML, or the potential importance of their role in addressing it. Third, those RMLOs in fact considered their sector as low risk with regard to ML/TF, and their awareness of AML/CFT obligations (particularly relating to PEPs) appeared to be limited. Finally, low understanding of risks is reflected in the very low number of SARs being reported by them, most of which were related to mortgage fraud. Overall, RMLO's approach to AML/CFT requirements is mostly compliance (rules) based, and exchanges with their regulators seem to be very limited.

294. The assessment team accepts that for RMLOs, their biggest risk is mortgage fraud. However, there is a significant risk that high-end real estate is used for ML purposes. The assessment team notes that in January 2016 FinCEN put in place a GTO to collect data on certain high-end real estate sales in two major urban markets. The GTO targets purchases with cash or monetary instruments with no use of borrowed funds; with a view to collecting information which will allow FinCEN to consider appropriate preventive measures in relation to high-end real estate, thus acknowledging the gap that exists.<sup>37</sup>

295. **Lawyers:** The ABA itself has an understanding of the ML/TF risks and has issued good voluntary best practice guidelines. The ABA itself accepts that there is an inconsistent understanding of risk across this very large sector. It is also not clear that lawyers comply with the best practice guidelines as they are not enforceable. Ethical standards, educative efforts and criminal and disciplinary sanctions imposed against complicit lawyers may mitigate the risk to a limited extent, though it does not address the concerns arising out of lack of comprehensive preventive measures.

296. **Company formation agents** did not demonstrate adequate awareness of the risks to which they are vulnerable, possibly equating these risks with OFAC requirements. **Accountants** similarly did not display an understanding of their vulnerability to abuse by criminal elements.

297. **Dealers in precious metals and stones:** The Jewellers Vigilance Committee (JVC) has done awareness-raising on ML/TF issues, and developed guidance and compliance tools which, in the view of the industry representatives met during on-site, are helpful. However, this sector comprises a large number of entities (many of them small, family-run business), not all of which are members of the JVC or have access to its resources (available for purchase). There is a scope for further improvement in understanding of risks and obligations, as noted during on-site discussions with the sector.

298. **Real estate agents** took the view that because ML risk only exists where transactions are processed directly, and as they have no role in accepting funds or closing/settlement of deals, they are not vulnerable. However, they are involved in negotiating transactions and do undertake some due diligence on prospective buyers, primarily to satisfy themselves about their capacity to pay. Real estate agents are also subject to State obligations to keep financial records. Whilst on-site, the assessors met with other real estate sector service providers in the high-end market, notably condominium associations and cooperatives, who can apply conditions to transactions including the prohibition of mortgage financing, particularly in the high-end market.

### *Application of risk mitigating measures*

299. Regulated entities across a broad range of sectors seem to be mitigating their risks through their AML programs. Interviews with the private sector reflected the commitment of Covered FIs/DNFBPs to appropriately staff their AML units, and many of the compliance officers met by the

<sup>37</sup> Since the on-site further GTOs have been put in place, extending the scope from Manhattan and Miami-Dade County, to include (1) all boroughs of New York City; (2) Miami-Dade County and the two counties immediately north (Broward and Palm Beach); (3) Los Angeles County, California; (4) three counties comprising part of the San Francisco area (San Francisco, San Mateo, and Santa Clara counties); (5) San Diego County, California; and (6) the county that includes San Antonio, Texas (Bexar County).

assessors had prior experience as former employees of Federal or State agencies involved in AML/CFT supervision/enforcement. All interviewees mentioned that they exercise full co-operation with, and receive useful information from LEAs, which is a positive aspect considering the predominant role that LEAs play in the AML/CFT regime.

300. **Banks** seem generally to have integrated risk mitigation measures into their day-to-day operations, and larger banks appear to have developed a leadership role on many sophisticated controls in the sector. Banks have been taking a “top-down” approach to foster and maintain a culture of compliance throughout their organizations. The American Bankers Association (the largest industry association of bankers in the U.S.) has also issued guidance to its members stating “[the] most important baseline of an effective AML program (or any compliance program, for that matter) is the board of directors’ and senior management’s support for maintaining a culture of compliance throughout the entire institution.” Training can be customised to the business line or operational function to maximize its effectiveness and relevance. For example, banks and other depository institutions provide different training programs to front line staff than to back office personnel, given that tellers and operations clerks, for instance, are exposed to different ML/TF risks.

301. The FBAs and State banking supervisors routinely examine banks to ensure that ML/TF risks are appropriately identified and adequately mitigated, in line with supervisory expectations. Regular supervisory reviews of AML/CFT programs are conducted, either as part of broader prudential supervision or in standalone work components. The examinations conform to the FFIEC Manual requirements, focusing on a bank’s compliance with laws and regulations as well as ensuring that the bank’s compliance program keeps pace with changes in its business model and operations and the resulting risk profile mitigated by an adequate risk management. Any control issues identified during on-site examination are communicated to management and board of directors in the form of supervisory reports/letters that detail findings and conclusions. Banks generally seem to apply BSA CIP obligations, as a starting point for CDD, which is then supplemented on the basis of the identified ML/TF risk. This is consistent with the CIP and other CDD elements prescribed for the banking sectors.

302. Regular review of the AML program by the FBAs encourages a dialogue between the bank and the examiners which leads to a clearer understanding of the required measures. However, representatives of the banking sector noted that, despite regular engagement with and extensive guidance from their supervisors, they often tend to better understand regulatory expectations based on the contents of the formal enforcement action orders issued against other institutions, when published.

303. The FBAs have identified some common areas of improvements for banks. For example, FIs have been encouraged by the FBAs to develop their knowledge of the purpose of the relationship with their customers, improve their monitoring systems through validation and testing and align them with their risk profile. In most cases, banks tend to implement these incremental improvements in the course of normal business, without the need for additional supervisory action.

304. **In the securities sector**, the situation is very similar to the banking sector, including how a culture of compliance is fostered within institutions, and how controls issues are communicated by

the supervisors to the management and board of directors of broker dealers. The SEC and FINRA also issue risk alerts and guidance, and meet regularly with industry groups.

305. **MSBs** met with at the on-site apply measures even in circumstances where the BSA does not specifically require them (e.g. screening for PEPs, applying measures to money transfers below the USD 3 000 threshold). MSBs with agent networks apply mitigating measures to deal with their agent risk, including due diligence.

306. For **casinos**, the recent AGA research study supports the view that the gaming industry has taken significant steps to comply with AML/CFT requirements and to prevent potential ML and TF in the last five years. This industry specific-survey, validated through in-depth interviews with various industry participants, LEAs and supervisors, indicates that casinos have not only increased their compliance spending but have also put in place mitigating measures above the requirements of the BSA based on their risk. This was confirmed by on-site discussions with casinos and their regulators. Casinos are covered by the regulations implementing s.314(a) and 314(b) of the USA PATRIOT Act for information sharing. However, casinos and FinCEN both indicated that they are not yet operational participants in the s.314(a) arrangements, and casinos themselves did not appear to understand that they are covered by s.314(b). Use of the procedures provided for by these provisions could increase the effectiveness of preventive measures in casinos.

307. **Life insurance companies** have more limited AML programs corresponding to the assessed lower risk environment. However, a major life insurer interviewed by the assessors applies a group-wide approach to risk (they operate in 50 countries) and applies a sophisticated domestic and non-U.S. approach to risk assessment. State insurance laws define permissible investments for life insurance companies. Prudential examinations conducted by the states include a detailed review of investments. Insurance companies exercise oversight over their agents and brokers: captive agents are treated as employees, and brokers (which service in the aggregate around 50% of the U.S. life insurance market) are subject to oversight and required to apply company standards.

308. **Dealers in precious metals and stones** comply with AML program and record-keeping requirements. DNFBPs (other than casinos) appeared to have a mixed understanding of their ML/TF risks, nor had many implemented adequate mitigating controls. In some cases this reflects the perceived low risk of the sector by the industry, and thus a specific vulnerability analysis by authorities is needed. In some cases, particularly the *accounting* and *legal* professions, industry practices assist in mitigating risk but not to the requisite extent. The ABA has issued voluntary guidance on AML but there is no evidence of the extent to which practitioners apply the guidance.

309. Neither the **real estate agents** nor the **RMLO sector** appeared to understand what the ML risks in relation to high-end real estate are or what the appropriate mitigation measures would be (see paragraph 293 and 298).

#### *Application of enhanced or specific CDD and record-keeping requirements*

310. Implementation of enhanced or specific CDD and record-keeping requirements varies widely across and within sectors. Generally, regulated entities customize their on-boarding measures, depending on the products and services that prospective customers may receive. These measures



are primarily designed to mitigate the risks arising from an organization's specific business models and customer base. On-boarding controls also differ by the type of prospective customer, as in some instances enhanced due diligence may be required (e.g. when on-boarding customers who are PEPs).

311. As an example, **banks**, in addition to the CIP requirements, obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification. This allows the bank to determine the customer's risk profile at account opening. If there is indication of a potential change in the customer's risk profile (e.g. expected account activity, change in employment or business operations), the bank will generally reassess the customer risk rating for a potential change. This information serves to develop parameters that assist in the identification of potential red flags. FBAs demonstrated that they can easily access the data related to a customer or transaction, during examinations and that the regulated entities are well aware of the five year record-keeping obligation. In practice, the assessors heard instances of banks offering private banking services (which are attractive to high net worth customers) extending PEPs requirements (including domestic PEPs) to all of their deposit accounts, even though this is not technically required by law or enforceable means. These regulated entities apply risk-based controls to verify new customers' identity and source of funds based on their business models and ML/TF risks they are exposed to.

312. **Life insurance companies** mostly tend to flag clients that trigger SAR filings as high risk. Most SARs filed from this sector concern fraud perpetrated against the insurance companies. There is a general belief in the life insurance sector that the insurance products covered by the AML rules are lower risk than banking investment products, even though they are similar. This is likely because of the additional due diligence applied by insurers (beyond what is required of banks) when selling insurance products, and the fact that it is not common for policies to be purchased or investments made with cash. **MSBs** interviewed by the assessors prohibit dealings with certain types of businesses (based on their own internal criteria) and apply EDD to identified high risk businesses.

313. In general, **casinos** determine and apply CDD measures and other controls to mitigate differing levels of risks. **Dealers in precious metals and stones** also have an AML Program requirement which is applied in accordance with their relatively lower risk. **Lawyers, accountants**, and **trust and company service providers** have no requirements to apply CDD measures, enhanced or otherwise. There is no evidence that, in practice, they make any more enquiries about customers than is absolutely necessary, unless they are paid in or asked to handle cash or monetary instruments in amounts that aggregate to more than USD 10 000 in which case the reporting requirement includes verified customer identifying information.

### *Beneficial Ownership<sup>38</sup>*

314. Despite the absence of a legal requirement conforming to the FATF standard to determine beneficial ownership (see R.10), FIs met on-site indicated that they generally make attempts to at

<sup>38</sup> Since the on-site, the Final CDD Rule that includes a BO requirement was published on 11 May 2016. The implementation period for the Rule is two years. (see <https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx>)



least know who beneficial owners are. This trend is strongest in the banking sector; however, verification of BO information is still identified as a weakness and work in progress across the financial sector.

315. *FIs in the banking and securities sectors* conduct due diligence to ascertain BO, specifically in accordance with the joint guidance on BO published in 2010 by FinCEN, the FBAs and the SEC (see [link](#)). The guidance was issued to clarify and consolidate existing regulatory requirements, but does not alter or supersede previously issued regulations, rulings, or guidance related to CIP requirements. In accordance with this guidance, **banks** indicated that as part of their AML compliance program, they establish and maintain CDD procedures that are reasonably designed to ascertain the identity of BOs, based on their evaluation of the risk pertaining to the account. The FFIEC Manual (p57-58) also states that in the course of conducting enhanced due diligence for high-risk customers, the bank should consider obtaining, both at account opening and throughout the relationship, information on individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors. The extent to which, they verify the identity of these persons (who may or may not be the BO) seems to be very limited, and in any event the requirement does not conform to the FATF standards (see TCA discussion). The authorities have demonstrated that there are certain enforcement actions against banks for not obtaining prescribed BO information based on risks, which tends to indicate that banks understand the risk posed in this area, and this is important to their assessment of risk. **Broker dealers** carry out CDD on their customers.

316. In the **MSB sector**, even though there are no specific requirements, institutions, which deal with legal entities as well as individual customers, do make some effort to at least understand the BO of the entity/customer. In the **life insurance sector**, BO is less of an issue since life policies are issued on the lives of natural persons.

### *Transaction Monitoring*

317. **Banks, broker dealers and MSBs** met by the assessors during the on-site have developed processes allowing for effective and robust transaction monitoring. Regardless of the size of the organization or the level of system sophistication, regulated entities develop tailored transaction monitoring parameters. Some FIs work with specialized organizations to develop their monitoring rules. The rationale and basis of such parameters are documented and made available to auditors and regulators for review and testing.

318. Regulated entities generally devote dedicated staff resources to investigating and evaluating the alerts generated by the monitoring systems. AML officers are responsible for determining whether the transactions flagged by the monitoring system are suspicious based on available information, and often use the information generated through on-boarding processes, publicly available information and commercial databases to inform their assessment. It is also a standard practice to reach out to customers to request additional information or supporting documentation that could validate the stated purpose of the transactions and reasonably ascertain the legitimacy of the activity.

319. Because of FinCEN's focus on **casinos**, more robust monitoring of activity is occurring, as demonstrated by increases in both quantity and quality of CTR and SAR reporting by casinos.

**Dealers in precious metals and stones** monitor transactions for the purposes of meeting CTR reporting requirements. **Other DNFBPs** are not comprehensively covered and do not routinely monitor transactions other than for purposes of meeting cash transaction reporting requirements.

#### *Risk Mitigation when Customer Information is unavailable*

320. **Covered FIs** routinely refuse to bank a customer or process a transaction until they have been able to determine the legitimacy of the activity and of the funds and parties involved. Depending on the collected information, they may also file a SAR even though refusing to open an account or process a transaction is not an explicit trigger for a SAR filing. If the activity identified requires immediate law enforcement attention, the FI is required to notify law enforcement by phone and file a SAR. In the DNFBP sector, **casinos** have systems and procedures in place, regarding matters to be taken into account in deciding not to accept or carry out a transaction. This was reflected in discussions with State regulators and the recent survey of the sectors. **Dealers in precious metals and stones** met with at the on-site noted that they tend to have long term relationships with their customers but that processes are in place where issues arise. **DNFBPs** (other than casinos and dealers in precious metals and stones) have practices relating to knowing their customer (notably **accountants**), and others have voluntary guidance (such as that put out by the ABA for **lawyers** and National Association of Realtors (NAR) for real estate agents). However, it is not clear to what extent the voluntary guidance is applied within these sectors.

#### *Application of EDD measures*

321. Industry practices and the extent to which enhanced due diligence (EDD) measures are implemented vary across sectors. **Banks and broker dealers** generally apply effective measures that are commensurate with their level of risk. They recognize that their level of risk is not the same across the customer and product spectrum and, accordingly, apply enhanced measures to mitigate and manage those customers, products, and serviced regions deemed to represent higher risk. The measures applied generally align to the BSA and as detailed in specific sections of the FFIEC Manual. On the whole, **MSBs** met with during the on-site have in place appropriate AML programs, as do the **casinos**. Below is an indication of how Covered FIs/DNFBPs in general are implementing EDD in the specific circumstances described in Core Issue 4.4.

322. **Politically exposed persons (PEPs)**: Banks and broker dealers tend to go beyond the legal requirements and apply a foreign PEP determination to all accounts, including processes to flag domestic PEPs, following a risk based approach. However, RMLOs do not seem to be aware of the PEPs requirement. The MSBs met with during the on-site cover foreign PEPs and apply EDD. Casinos also reported treating PEPs as higher risk, including domestic PEPs on occasion. Life insurance companies mostly tend to automatically flag PEPs as high risk.

323. **Correspondent banking**: Banks providing correspondent banking services have specific measures for monitoring transactions flowing through them including EDD for foreign correspondent relationships as required by the BSA, and monitoring all transactions through the bank for suspicious activity and SDNs (sanctions).

324. **New technologies:** Banks and broker dealers apply EDD in accordance with the BSA Manual and incorporate new information to ensure that their AML/CFT programs are addressing higher risks. Banks incorporate information from advisories, guidance, and other forms of outreach from FinCEN, FBAs, and law enforcement. MSBs generally apply EDD to products based on or delivered by new technologies, such as virtual currency.

325. **Wire transfers:** Banks apply appropriate measures to comply with the record-keeping and travel rule's requirements. Some banks apply the record-keeping and travel rules to all wire transfers, as opposed to only those above the USD 3 000 threshold, in order to streamline their operational processes. Additionally, some banks also generally obtain and include all originator and beneficiary information. Some MSBs are also applying cross-border wire-transfer requirements below the threshold. Overall, these measures help mitigate TC gaps to some extent.

326. **Targeted financial sanctions (TFS):** Sanctions obligations appear to be very well understood and implemented, particularly by FIs. Banks have implemented OFAC programs to freeze or block transactions related to TFS. Most U.S. banks use interdiction software to screen their customer database, in-process transactions, and other pertinent information to identify the involvement of, or property belonging to designated persons, countries, or regions subject to OFAC's sanctions programs. Banks regularly cooperate in investigations, and provide information on transactions that may point to designated persons/entities. All U.S. businesses are required to screen against the OFAC lists, and according to the evidence seen by the assessors do so.

327. One challenge to effective implementation of TFS is that FIs/DNFBPs do not always implement CDD measures sufficiently in order to understand who the ultimate BO of a customer or party to a transaction is. As a result, screening tools cannot assure a sanctions list match. This issue was raised with U.S. authorities, in particular OFAC, who were aware of the risks (and the reality) of designated persons seeking to hide behind front companies, other natural/legal persons or aliases. While this remains a constant challenge, the inter-agency approach taken by the U.S. authorities to the sharing of information and intelligence (including with regulators, law enforcement and various agencies involved in imports/exports) helps to mitigate this significant risk somewhat. To provide further information, Treasury and other U.S. government agencies conduct extensive formal outreach and share information with FIs. For example, OFAC provides well over 100 presentations each year to a variety of industry groups and affected organizations, including through conferences, panels, and webcasts, to ensure that TFS obligations are understood.

328. **Higher risk countries:** FIs are well aware of higher risk countries identified by FATF, and apply EDD broadly to most customer relationships based in/connected to countries on the lists. FinCEN publishes advisories cross referencing the FATF public statements. MSBs with networks of agents and agents, branches or counterparts outside the U.S. have processes in place relating to higher risk countries. The same applies to the life insurance company sector, as major insurance companies have subsidiaries or branches outside the U.S.

*Reporting obligations and tipping off*

329. Overall, most covered FIs/DNFBPs implement their reporting obligations adequately. The reporting requirements related to TF are being particularly well implemented which reflects the high awareness of this issue that most sectors demonstrated during the on-site visit.

Table 15. **Number of SAR filings by financial institution (2010-2015)**

By	2010	2011	2012	2013	2014	2015*
Depository institutions	697 367	798 688	896 610	981 429	886 923	439 889
MSBs	596 494	685 009	640 419	616 761	771 025	441 383
Casinos and Card Clubs	13 987	17 627	23 401	31 919	46 575	24 900
Securities and Futures	18 758	19 903	22 437	18 808	22 448	10 492
Life Insurance Companies	N/A	N/A	726	3 066	2 897	569

\*Data for 2015 included SARs filed from January 1 through June 30, 2015. For life insurance companies the period is from January 1 through March 31, 2015.

330. SAR filings across some of the biggest sectors in the U.S. show a healthy trend, and the authorities confirmed that defensive filings are not an area of significant concern. LEAs were also generally positive about the quality of SARs being filed. While reporting entities have a window of 30/60 days to file SARs (see R.20), there is a requirement to report matters requiring immediate attention to LEAs immediately and follow up with a timely SAR. Authorities reported that approximately 11 percent of all SARs are filed the same day the suspicious activity is identified. The median amount of time within the 30 day SAR filing window from the identification of new suspicious activity to the filing of a SAR is 17 calendar days. The above statistics demonstrate the following trends:

- Banks and MSBs contribute almost 96% of the total SAR filings. The rest are contributed by casinos, the securities and futures sector and the life insurance sector.
- The level of SAR filings by the securities and futures sector appears to be low, given the size of this sector, the intensity of its activities and the size of the financial system in the U.S. The level of SARs filed by credit unions also seems to be low within the depository institutions. Since a further breakdown of statistics is not provided, it has not been clearly established whether SAR filings by institutions within and across certain sectors (such as credit unions, RMLOs) are happening at an appropriate level.
- Levels of SAR reporting by MSBs have remained constant at around 40-45% of all SARs.

- Casino SAR reporting has tripled from under 1% of total SARs in 2007 to around 3% in 2014, which may reflect the increased focus by FinCEN and the IRS on casino compliance.

331. DNFBPs (other than casinos) are not required to report SARs, but are subject to the Form 8300 reporting obligation (see above and TC annex). Form 8300 requires reporting entities to report related transactions involving currency or monetary instruments over USD 10 000 and allows the reporting entity to voluntarily use the form to report suspicious transactions made in cash. Somewhere around 2% or less of Form 8300s filed each year includes an indication of suspicion. It is worth noting that this form of reporting applies to all non-financial trades and businesses in the U.S., not just DNFBPs. It is also worth noting that although some 4% of Form 8300s filed by attorneys indicated suspicions, the ABA was strongly of the view that mandatory SAR reporting should not apply to attorneys because of the breadth of legal professional privilege and because of the ability of attorneys to withdraw from a relationship where illegal activity is apparent.

332. Banks, security broker dealers and MSBs meet their reporting obligations by various means appropriate to their level of risk, such as developing computerized monitoring systems, staff capacity building, and ongoing reviews of their AML program. FIs have demonstrated that their transaction monitoring is tailored to their activities and risks which permit them to report suspicious transactions and activity, including structuring.

333. Regulated entities are increasingly working with law enforcement to enhance their ability to detect possible TF and other criminal behaviour, and ensure that reports are of good quality, accurate and filed expeditiously, and that detection efforts are well calibrated to address risks.

#### Box 25. **Public/private engagement on SAR reporting**

A clear example of how FIs have deployed customized parameters to detect suspicious activity can be observed by analyzing the types of FI reporting transactions potentially involved in human trafficking. After FinCEN published its advisory pertaining to human trafficking and human smuggling in September 2014, the number of human trafficking related SARs increased by 700% over the same period in the previous year. This change in SAR filing behaviour reflects the ability of FIs to adjust their monitoring systems to better capture particular types of suspicious activity and manage risks.

334. Detecting possible TF transactions is a priority focus, in line with the country's risks. The private sector has good collaboration with the FBI on how to better identify TF. FIs/DNFBPs with a SAR filing obligation are required by law to notify law enforcement by phone immediately and file a timely SAR when they identify a situation involving a violation requiring immediate attention, irrespective of any threshold. Furthermore, up to June 2015, FinCEN's FI Hotline has received 212 calls from FIs seeking to promptly and directly alert FinCEN and law enforcement of possible instances of TF. By comparison, during 2014, FinCEN received 108 calls for the entire year (see IO.6 and IO.9). MSBs and casinos both indicated that they use the TF hotline and have relationships with law enforcement agencies enabling them to report directly, where appropriate. Reporting entities

are not required to use the FinCEN Hotline to notify law enforcement. The U.S. does not have figures for the number of immediate notifications made directly to law enforcement.

335. Although public/private engagement is clearly taking place, all sectors expressed the desire for more input from the authorities to facilitate the identification of suspicious transactions and customers who should raise concerns. They would also appreciate more sectoral and horizontal information regarding the risks their activities are exposed to.

336. Reporting entities use section 314(b) of the USA PATRIOT Act to share information related to “possible terrorist or ML activities” with one another, under a safe harbour that offers protections from liability. FinCEN strongly encourages participation in 314(b) information sharing which is a voluntary program. This mechanism helps reporting entities to better identify and report suspicious transactions related to ML, associated predicate offenses (e.g. human trafficking), and TF. Currently there are over 4 500 financial institutions that have registered to participate in 314(b).

#### *Suspicious transaction reporting below the threshold*

337. While there are thresholds related to SARs, these are partly mitigated by the immediate filing requirement, which the U.S. authorities advise applies regardless of threshold. 8.37% of SARs filed relate to transactions below the relevant thresholds. As noted in R.20, the reporting thresholds are a technical deficiency (see R.20), which may limit the amount of financial intelligence available (IO.6).

338. From 1 July 2013 through 30 June 2015, FinCEN received 3,157 SARs noting potential TF. MSBs filed the largest number (1 513), of which 19% were below the USD 2 000 threshold. Banks filed the next largest number (1 302), of which 15% were below the threshold. For casinos and card clubs, the percentage of filings below thresholds was greater. The obligation to immediately report suspicious activities that require immediate attention regardless of threshold is expected to mitigate concerns about what effect the reporting thresholds are having on implementation. However guidance by the U.S. authorities, on the scope of this immediate reporting requirement and its interaction with the existing thresholds is needed, to ensure efficient implementation of this requirement and avoid gaps in the reporting obligations. The following table provides a snapshot of TF related SARs below and above thresholds:

Table 16. TF SARs by industry (July 1, 2013- June 30, 2015)

SARs	Casino/ card clubs	Depository institution	Insurance company	MSBs	Other	Securities/Futures
Below Filing Threshold	31	191	3	285	101	12
Above Filing Threshold	9	1 111	3	1 228	167	16

#### *Tipping Off*

339. To prevent tipping off, Covered FIs and DNFBPs, and their current and former directors, officers, employees, agents, and contractors, are prohibited from disclosing SARs, or any information that would reveal the existence of a SAR and could be subject to civil and criminal penalties for the



unauthorized disclosure of a SAR. FinCEN has published an advisory, reminding FIs of their obligations<sup>39</sup>. Discussion with authorities' during on-site did not indicate any concerns with regard to confidentiality provisions.

#### *Internal controls and legal/regulatory requirements impeding implementation*

340. Industry practices and the quality of internal controls vary across sectors. **At the group level, banks and securities dealers** operating in multiple jurisdictions have sophisticated firm-wide internal control programs calibrated towards understanding the risks of operating in each jurisdiction, and how those risks affect the bank's operations in the U.S. These firms dedicate substantial resources (budgets, staffing) to AML/CFT risk assessment and compliance activities and their internal audit groups are responsible for auditing compliance. The assessors' discussions with a large **insurance company** operating in multiple jurisdictions suggest that a similar approach is taken in that sector. Discussions with a **casino**, casino regulators and the AGA reveal that mainstream casinos have been improving their internal controls and procedures for group level compliance.

341. The Federal regulatory agencies advised the assessors that, in the **banking and broker dealers sector**, failures or weaknesses in internal controls is one of the most commonly cited deficiencies identified in compliance examinations. However, as noted in Chapter 6 below, in such cases, the regulators conduct close monitoring to ensure that such institutions implement the required corrective measures and improve their compliance in this area.

342. **MSBs** also have extensive internal controls and procedures, and apply these to their networks of agents. Many of these controls go beyond the explicit BSA requirements, including broader risk assessment and more comprehensive AML programs that deal with operating risk, including agent risk.

343. As **DNFBPs** (other than casinos and dealers in precious metals and stones) are not required to implement internal controls (see R.23), they generally do not do so in practice. Some DNFBPs met with by the assessors explained that they have implemented internal processes in order to comply with industry guidelines or SRO requirements, some of which touch on topics relevant to the risks of ML/TF. On the whole, however, the lack of internal controls, particularly in those DNFBPs with a significant role in relation to high-end real estate and in advising on and creating legal persons, is a major gap.

#### *Legal/regulatory impediments to implementation*

344. **At the group level**, inconsistent application of data protection and privacy laws in some foreign countries was cited by some FIs as creating legal hurdles which may impede the implementation of ML/TF risk management group-wide. During the on-site, FIs confirmed that they cannot inform their foreign branches or subsidiaries of having filed a SAR, even if the SAR is linked to a customer of the foreign operation. This issue makes it more difficult for FIs to understand and

<sup>39</sup> See FinCEN Advisory issued on 2 March 2012, SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions., available at <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a002>

mitigate their risks, and meet their foreign STR filing obligations effectively across the group. FinCEN guidance of 2010 provides that depository institutions, securities broker-dealers, mutual funds and FCM and IBs that have filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, provided the affiliate is subject to a SAR regulation. Neither *MSBs* nor *casinos* cited any legal or regulatory requirements impeding AML/CFT compliance.

345. **The U.S. is rated as having a moderate level of effectiveness for IO.4.**

## CHAPTER 6. SUPERVISION

### *Key Findings and Recommended Actions*

#### *Key Findings*

1. The regulatory and supervisory framework in the U.S. is highly complex and multi-faceted, involving a number of authorities both at the Federal and State levels. FBAs and some of the State regulators have effective processes to understand ML/TF risks. Entry criteria in the financial and casino sectors are generally robust and examination programs, follow-up and enforcement actions are often coordinated at the Federal and State level.
2. In the life insurance sector the situation is similar, except that the overall quality of supervision for AML/CFT requirements is less intensive and is often not followed up with written findings. State insurance supervisors do not appear to have a comprehensive view of ML/TF risks; however the assessors have placed a low weighting on this as there appears to be relatively few instances of ML/TF identified in this sector, and also because of the ability of FinCEN to enforce compliance.
3. The process of coordinating MSB examinations between FinCEN, IRS SBSE and the States is positively evolving. FinCEN and IRS-SBSE have taken initiatives to address unregistered money remitters through outreach and enforcement actions, which have been effective.
4. Other than casinos and dealers in precious metals and stones, DNFBPs are not supervised for AML/CFT compliance. While there are some voluntary guidance and outreach efforts by the ABA, and the National Association of Realtors the lack of enforceable obligations is an impediment in assessing the extent to which that guidance is applied or is having the desired impact.

#### *Recommended Actions*

1. Minimally covered sectors exposed to high risks such as IAs, lawyers, accountants, trust and company service providers (except for trust companies), and high-end real estate agents are currently subject to only Form 8300 and targeted financial sanction compliance monitoring. They should be brought under the BSA/USA PATRIOT Act supervisory framework as a priority. As recommended in Chapter 5, they should be responsible for implementing appropriate AML/CFT obligations, which will generate financial intelligence for FinCEN and LEAs. The outcomes of the GTOs currently in place should be analysed and used to develop appropriate regulatory measures.
2. While the FFIEC Manual is acknowledged as a good example of coordinated supervisory efforts to promote a common understanding of ML/TF risks and BSA obligations, there is a need for more and ongoing guidance from supervisors to industry on their regulatory expectations. This applies to other sectors as well. In particular, guidance on the immediate SAR reporting requirement, its interaction with the existing thresholds is needed to ensure efficient implementation of the requirement and avoid gaps in the reporting obligations.
3. The Federal authorities and the State insurance supervisors should consider whether

elements of the FFIEC Manual could be applied to life insurance companies' Covered Products AML programs, given the similarity of the vulnerabilities. State life insurance regulators should also improve their understanding of the risks and enhance their supervisory programs, in particular by ensuring that they provide written AML/CFT supervisory examination letters as part of their supervisory processes.

4. Each FBA and State banking agency should continue to develop appropriate supervisory tools to improve the effective application of the risk-based approach in supervising and tailoring examinations in order to address identified risks that are specific to each FI.
5. Three categories of non-Federal State chartered banks should be subject to an AML Program requirement in addition to their reporting obligations.<sup>40</sup>
6. Guidance should clarify that broker dealers are required to conduct a risk assessment to comply with the AML program. This will help clarify and strengthen the expectations of the supervisory authorities.
7. The U.S. should further strengthen the existing mechanism of BSAAG by ensuring that there is adequate representation from all FI and DNFBP sectors and State financial regulators; to reflect its more valuable role in practice.
8. The coordinated approach for MSBs inspection should be expanded across the sector. More participation by Federal supervisors as appropriate may also be pursued. IRS-SBSE should continue its efforts in the area of unregistered money remitters.
9. Supervision needs to continue to focus on casinos to ensure that the peculiar risks of this industry are mitigated effectively.

346. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 and 35.

### ***Immediate Outcome 3 (Supervision)***

347. Although the AML/CFT supervision of FIs and DNFBPs in the U.S. is mostly conducted at the Federal level, the States are also involved in AML/CFT supervision of MSBs, life insurance companies and banks that are not members of the Federal Reserve System. For practical reasons, the assessors were not able to interview representatives of all 50 States' banking and life insurance supervisors. In cooperation with the U.S. authorities, discussions were held with representatives of the Iowa life insurance supervisor and the Department of Financial Supervision of the State of New York. Generally, the assessors understood from their discussions that these two States would be representative of the approaches taken by State supervisory authorities.

348. The U.S. supervisory framework for the banking sector is well developed and generally considerable supervisory resources are applied at the Federal level. This is commensurate with the

<sup>40</sup> Currently FinCEN has an ongoing rulemaking process to address this issue (see <https://www.gpo.gov/fdsys/pkg/FR-2016-08-25/pdf/2016-20219.pdf>).

size and significance of the sector. The securities sector is also very large and has the advantage of a dual supervision mechanism by the SEC and FINRA. The biggest supervisory gap here is the non-coverage of all IAs. Supervisory processes for MSBs are maturing and there is now a greater coordination among States in their supervision.

349. Life insurance companies are subject to lighter touch supervisory processes mostly reflecting the lower risk this sector represents, which is limited to the investment vehicles (“Covered Products”). Authorities base this assessment on the low numbers of SARs reported, lack of any significant supervisory findings for a number of years when the sector was being examined by IRS-SBSE and lack of ML typologies, and the assessors agree that this sector is lower risk. For these reasons FinCEN directed IRS-SBSE to refocus its limited examination resources to higher risk and/or more complex areas, such as casinos and MSBs, and therefore now FinCEN relies on the State authorities for insurance examinations. However, IRS-SBSE retains authority to conduct life insurance company AML/CFT exams, if requested by the States or directed by FinCEN.

350. In the DNFBP sectors, there has been an increased focus in recent years on the supervision of casinos, in line with the identified vulnerability of the sector. However, there is little AML/CFT supervision of DNFBPs other than casinos and dealers in precious metals and stones, most notably lawyers, accountants, real estate agents and CFAs. This has a significant impact on the effectiveness of the system given the roles of these sectors in relation to a number of high risk situations set out in the NMLRA involving real estate transactions, and advice on and the formation of large and complex structures. These deficiencies are significant enough to require major improvements in supervision.

351. The assessors based their conclusions on: extensive discussions with FinCEN, IRS-SBSE, all FFRs (FBAs, the SEC and the CFTC), SROs including FINRA and NFA, Iowa and New York State authorities and several industry associations and professional bodies; reviews of examination procedures, processes, manuals and priorities of these supervisory authorities, wherever made available; and exhaustive process narratives provided by the U.S. authorities. Input provided on the supervisory regime by the private sector representatives across the FI/DNFBP sectors during the on-site was also factored in, wherever appropriate.

#### *Licensing, registration & controls preventing criminals & associates from entering the market*

352. In general, the U.S. has a strong system of licensing and entry requirements for the **banking sector**. The sectoral regulators, whether at the Federal or State level, have the authority to charter and supervise all domestic and foreign banks operating in the U.S. and to insure deposits at domestic banks and a limited number of U.S. branches of foreign banks. The four FBAs apply similar (and sometimes coordinated) entry screening processes (although these frequently duplicate each other, the U.S. sees this as a strength of the system), supplemented by criminal background checks conducted by LEAs. The U.S. has demonstrated that the entry supervision/monitoring processes have prevented criminals from controlling banks. Applicants often withdraw their applications when they do not meet the licensing requirements. In at least one case, the application was rejected because of the existence of a SAR linked to two people associated with the application.

353. In the **securities sector**, there is a dual registration processes for broker-dealers involving the SEC and FINRA. FINRA conducts background checks, extensively reviews business models, and interviews key staff of broker dealers to focus on the adequacy of safeguards in place. Additionally, criminal background checks are conducted by LEAs. In the **derivatives sector**, CFTC has delegated the registration function to NFA, which registers applicants that comply with extensive disclosure obligations and are subject to a criminal background review.

354. Domestic **life insurance companies** are exclusively chartered by the States, which are also responsible for entry requirements applicable to foreign life insurance companies wishing to operate branches or subsidiaries in the U.S. For the large companies, which often have banking or wealth management subsidiaries, there is a process in place for State authorities and the applicable FBA to liaise with each other when addressing fit and proper requirements. The entry and licensing processes are generally similar to Federal processes in the banking sector.

355. There are generally good licensing, registration and other controls for **MSBs**, which take into account the fitness and propriety of individuals. Money transmitters are licensed in 47<sup>41</sup> of the 50 States (except Montana, New Mexico and South Carolina), as well as D.C, Puerto Rico and the U.S. Virgin Islands, and there seems to be a strong system for background and fitness and propriety checks of persons controlling them. In many States, vetting is done of everyone with an interest of 10% or more in the business, as well as officers, the board of directors, and any parent company. There is good coordination among the States through the mechanisms of the Money Transmitter Regulators Association (MTRA), the Nationwide Multi-State Licensing System (NMLS) and the Multi-State MSB Examination Taskforce (MMET). Apart from the State requirement to license, there is also a Federal requirement for money transmitters to register with FinCEN (which must be renewed every two years), and to update registration information in certain circumstances.

### *FinCEN's Unregistered MSB Initiatives*

356. FinCEN, collaborating with State authorities, has conducted outreach to identify potentially unregistered MSBs and has also focused on unregistered businesses. FinCEN has taken civil enforcement actions against MSBs, including for failing to register with it. IRS-SBSE has also continued to focus on unregistered MSBs. In 2015, for example, IRS completed 122 examinations of suspected unregistered MSB. IRS identified these MSBs for examination based upon referrals from FinCEN or an internal IRS review of SAR filings indicating potential unregistered activity. Sixty-four (48%) of the entities examined were cited for violations of the BSA.

<sup>41</sup> Since the date of on-site, authorities reported that MSBs in New Mexico and South Carolina are now covered under licensing regime as per the legislative amendments in these states.



## Box 26. Action against unregistered MSB

**Saifullah Anjum Ranjha (2008)** – Baltimore, MD: A Pakistani national residing in the U.S. operated a money remitter business, Hamza, Inc., licensed in the District of Columbia, but not in the State of Maryland. During 2003-07, LEAs, acting through a cooperative witness, transferred USD 2.2 million to Ranjha (mostly in Maryland) ostensibly for onward transfer to Al-Qaida and its affiliated organizations, through hawala. The witness represented that the funds were the proceeds of international drug trafficking and smuggling of counterfeit cigarettes and weapons. Ranjha facilitated funds transfers to designated accounts and individuals in Canada, England, Spain, Pakistan, Japan and Australia, after charging his commission. The funds were picked up by cooperative individuals and returned to the Government. Ranjha pleaded guilty to conspiring to ML, concealing TF and operating as an unlicensed money transmitter in Maryland and was sentenced to over 9 years in prison.

**Victor Kaganov (2010)** – Portland, Oregon: A naturalized citizen living in Oregon created shell corporations to hide illegal activities on behalf of his Russian clients. Using these corporations, he set up bank accounts and moved more than USD 172 million through the U.S. from July 2002 through March 2009. Most of the funds came from Russia, with the rest from more than 50 other countries, mainly in Asia and Europe. In March 2010, Kaganov pleaded guilty to operating an illegal money transmitting business and was sentenced to three years' probation and four months of house arrest. Kaganov was also found to be in violation of BSA registration, AML program and SAR requirements. In March 2011, FinCEN issued a USD 25 000 civil money penalty against Kaganov for operating an unregistered money transmitter and without a State licence.

357. The following table provides a snapshot of ML charges, convictions and the conviction rate for failure to register with FinCEN by MSBs:

Table 17. Number of ML charges, convictions and conviction rate (2010-2014)

Offense	Action	2010	2011	2012	2013	2014
<b>18 USC 1960</b> (Failure to comply with FinCEN registration requirement for MSBs)	Charged	53	40	24	22	47
	Convicted	21	29	16	20	39
	Conviction rate	40%	73%	67%	91%	83%

358. During the on-site, the assessors identified lack of licensing of MSBs in three states (Montana, New Mexico and South Carolina)<sup>42</sup>, with a potential to create vulnerabilities (particularly New Mexico, in relation to the south west border). State authorities also confirmed that this loophole might have been abused for illicit purposes. However, MSBs in these States only represent 2.3% of all MSBs registered with FinCEN and since on-site, the only State now left without a licensing regime is Montana.

<sup>42</sup> Ibid.

359. There is a strong licensing regime for casinos, owners and certain senior associated individuals. Lawyers and accountants have professional and continuing ethical requirements in order to be able to practise. For lawyers, this is administered through either the State Bar Associations or State courts. Real estate agents are licensed under State law but are not subject to any specific fit and proper criteria. The precious metal and stones industry also lacks any specific entry criteria.

360. Refusals to licence money transmitters, casinos and casino employees and revocations of licences are uncommon. However, the authorities indicated that applicants often withdraw their applications in cases where serious concerns are expressed by authorities. Licensees with problems such as financial distress will often sell or relinquish their licence instead of waiting for it to be revoked.

### *Supervisors' understanding and identification of ML/TF risks*

361. **FinCEN** is responsible for the AML/CFT supervision of the financial sector, working in cooperation with the sectoral supervisors to which it has delegated BSA examination authority. FinCEN seems to have a good understanding overall of the inherent nature of risks across the covered sectors, both between the sectors and in relation to various types of institutions within sectors and passes that understanding on to the delegated supervisors. It also supports the understanding of other supervisors through its own analysis and feedback.

362. In the **banking sector**, FBAs are required to conduct supervision of their supervised entities generally on a fixed cycle. In most cases this involves an on-site visit of varying duration, and for the largest banks, the FBA staff is embedded in the banks' premises, fostering immediate co-operation and dialogue on risk and controls. FBAs further maintain and update their understanding of ML/TF risks through on-going dialogue with law enforcement, participation in inter-agency forums such as the BSAAG and the FFIEC AML Working Group, industry meetings, and in regular and *ad hoc* meetings and discussions with FinCEN.

363. FBAs met during the on-site visit generally exhibited an advanced level of understanding of the ML/TF risks present in their respective sectors. FBAs' understanding of risks is also supported by their knowledge of FIs' products, services, customers and geographic locations. This information is also used in planning and scoping of such examinations, often in coordination with State banking regulators (most notably with FDIC and also with the Federal Reserve, which shares supervision of State-chartered banks that are Federal Reserve members on a bi-annual basis).

364. The OCC has developed its Money Laundering Risk (MLR) system to differentiate ML/TF risks among individual institutions and across groups of institutions and aid examiners in the process. It also facilitates a horizontal comparison among banks across multiple indicators. The OCC Lead Expert network also helps the OCC identify and analyse ML/TF risks across its portfolio and facilitates the early identification of significant risks and early communication of these risks to examiners for inclusion in supervisory strategies. The FDIC and the Federal Reserve have also established a number of controls to understand the ML/TF vulnerabilities and threats faced by the depository institutions subject to their respective supervision.

365. In the **securities sector**, SEC and FINRA have a good understanding of ML/TF risk. FINRA is the frontline examiner. The SEC oversees FINRA and conducts focused inspections based on SAR filings, among other risk factors. Supervisors seem well aware of risks in the sector and the same is reflected in their overall approach to supervision. This includes a substantial amount of coordination, and exchange of examination programs and referrals, geared towards a more coordinated approach to promote better understanding and identification of risks. This was particularly notable in the larger institutions, which often form part of financial conglomerates (banks, insurers, securities dealers, etc. supervised by more than one FFR). FINRA assigns cumulative risk-ratings to supervised entities and classifies them into appropriate risk buckets based on different parameters which further drive the supervisory processes.

366. In the **derivatives sector**, CFTC does not directly supervise FIs for AML/CFT. It has delegated this task to two SROs, the National Futures Association (NFA) and the Chicago Mercantile Exchange Group (CME Group). However, the CFTC has formed a BSA Review Team that conducts analysis of SAR filings in FinCEN's databases related to derivative trading activities. This is intended to detect emerging flags on frauds or other illegal activity, and to provide support to the investigative teams. Those searches can result in referrals to LEAs as well. On average, the BSA Review Team reviews more than 12 000 SARs annually and refers more than 100 of them to investigative teams in support of new or existing investigations. To date, the CFTC has brought 24 enforcement actions based on leads developed from SARs. While this SAR analysis is not disseminated to the SROs, regular meetings between the CFTC and the SROs facilitate exchange of trends.

367. States apply AML/CFT supervision as part of their broader prudential examinations of the **life insurance sector**. The AML/CFT component of supervision is specified in the NAIC examination manual. The overall scope of the supervision is commensurate with the lighter touch applied to insurance companies, but is high level compared to the FFIEC Manual, even allowing for the lower risks. For example, there is no mention of the assessment of ML/TF risk in the manual and there appears to be no expansion of ML/TF risk assessment outside of the Covered Products covered under BSA. Life insurance companies are not obligated to create written ML/TF risk assessments, so it is likely more difficult for supervisors to judge whether their programs are adequate. FinCEN guidance addresses risks related to Covered Products as these bear the most resemblance to comparable facilities, in other sectors but there is no obligation to assess addressing broader risks, such as loans or corporate investments for example (although this happens in practice in the larger companies). The State insurance supervisors in general displayed a limited understanding of ML/TF risk.

368. State supervisors in the **MSB** sector have a good understanding of the ML/TF risks for the sector (at least in those States which participate in the MTRA, NMLS and MMET). In relation to **casinos**, there is a good understanding of ML/TF risks in FinCEN and in the State casino regulators the assessors met during on-site. In respect of **other DNFBPs**, IRS-SBSE did not demonstrate that it is fully conversant with the risks across and between the different sectors with which it deals. Its examination priorities are mostly directed or influenced by FinCEN. The IRS Manual, chapter 4.26, does refer to risk analysis in the context of examinations (4.26.6.4.1.1.1) but only in relation to the risk of non-compliance. This lack of focus on ML/TF risk was confirmed by the assessors' meetings with the IRS-SBSE.

369. Generally, none of the relevant State regulatory agencies seem to pay particular attention to AML/CFT issues or to particularly understand risks emanating from DNFBPs, other than casinos. This is partly because FinCEN has prioritized the casino sector in recent times due to its vulnerability (with less attention to other DNFBPs), but primarily reflects the fact that none of the other sectors are covered under the comprehensive AML/CFT framework.

370. ABA has provided good voluntary guidance to lawyers and attorneys but as BSA obligations do not apply, there is no BSA supervisor for this sector. The ABA has a broad understanding of risks posed by the legal sector, but is not equipped to understand the risks posed by individual law firms. In particular, it considers strongly that any attempt to bring lawyers under BSA AML/CFT obligations will conflict with obligations around legal professional privilege and client confidentiality. Conversely, the assessors note that the lack of BSA coverage of lawyers contrasts with the very significant gatekeeper role being played by them particularly in the high-end real estate transactions and the company formation processes in the U.S.

### *Risk-based supervision of compliance with AML/CFT requirements*

371. **Lack of coverage of DNFBPs** is the most significant issue in the overall context of effectiveness of the supervisory process. Apart from casinos and dealers in precious metals and stones, DNFBPs are subject only to limited supervision related to cash transaction reporting, despite the authorities' understanding of the risks in these sectors, particularly in relation to advice on and formation of legal persons and arrangements, and the risks presented by high-end real estate. Although there is a strong focus on supervision of the casino sector, there is little focus on any other DNFBP sector, leaving them susceptible to abuse.

372. In the **banking sector**, the supervisory approach incorporates minimum standards with a risk-based approach to tailor examinations. FBAs and the State bank agencies are required to include reviews of BSA compliance programs in their examination of insured depository institutions. These reviews mostly include on-site examinations and are scheduled on a rules-based (12-18 month) cycle. Regardless of the individual FI risk profile, the supervisory program systematically covers all entities subject to the prudential supervision of the relevant regulator. The intensive approach to banking supervision reflects the importance and vulnerability associated with the U.S. financial system. The RBA is reflected, not in the frequency of examinations, but in the fact that the examinations are tailored based on the BSA/ML risk profile of the bank. This is done by selecting relevant supplemental examination procedures directed at what the FFIEC Manual describes as high risk activity (in addition to the core material that is covered in all cases and which constitutes a robust baseline for the implementation of AML/CFT supervision). This supervisory approach leads to close monitoring of the AML/CFT system put in place by the FI. A similar approach is generally followed by State bank regulators. The FFIEC Manual is a key strength of banking supervision in the U.S.

373. The FBA supervisory process encourages a dialogue between the bank and the examiner and leads to a clearer understanding of the measures needed to more effectively mitigate the bank's risks. There were, however, some concerns expressed to the assessors by representatives of the private sector that they have to discover the expectations of their regulators through the publication

of the formal enforcement actions against fellow participants. Bankers met by the assessors suggested that a more nuanced articulation of such regulatory expectations in advance would be more helpful than discovery through enforcement actions. The following tables indicate the numbers of institutions subject to BSA supervision by regulators:

Table 18. Number of depository institutions

FBA	No. of Regulated entities for BSA examinations					2015 Assets under supervision (USD trillion)
	2011	2012	2013	2014	2015	
BGFRS	1 047	1 063	1 064	1 065	1 058	5.8
FDIC	4 598	4 460	4 312	4 138	3 995	2.7
OCC	2 086	1 955	1 810	1 663	1 537	11.1
NCUA	7 179	6 888	6 620	6 350	6 021	1.2
No. of BSA examinations (BGFRS, FDIC, OCC, NCUA)						
This data was received and reviewed by assessors, but the U.S. requested it not to be published						

374. In the *securities sector*, the SEC and FINRA conduct risk-based examinations of broker dealers based on their examination priorities. AML is part of SEC's priorities and in 2015 the principal focus was on broker dealers filing incomplete or late SARs, allowing customers to deposit and withdraw cash, and allowing access to the U.S. market from higher risk jurisdictions. The BSA Review Group within SEC also reviews all the SARs filed by broker dealers along with SARs filed by other institutions that have a securities market connection. The results of such review are considered when determining follow up including targeted examinations.

375. FINRA conducts a risk-based examination program taking into account cumulative risk rating of broker dealers. The risk rating factors in parameters such as whether the firm has omnibus or intermediated account relationships, trading volume in penny stocks, percentage of business overseas or firms that target overseas clients, high impact firms having large numbers of client accounts, sales practices etc. Examination frequency and intensity is based on the sector risk categorization of the respective firms and not solely on ML/TF matters, although there is a regular topical focus on some ML/TF risks. Firms are grouped in examination cycles (1 year to 4 years) based on such parameters. Overall, the risk that is taken into account in deciding where to apply its examination resources appears to be the risk of non-compliance with the BSA obligations, rather than ML/TF risk.

Table 19. Number of examinations by SEC and FINRA

SEC	2012-13	2013-14	2014-15
Number of exams including AML review	94	105	104
Number of AML related deficiencies resulting into deficiencies letter requiring written response from firms	125	86	150

FINRA	2013	2014	2015
Number of exams including AML review	1 102	547	462
Number of AML cause exams	29	19	24
Number of exams that cited AML as a deficiency	410	238	207
Number of exams with AML citations that resulted in informal action (cautionary action letter)	327	207	177
Number of Enforcement actions that included an AML charge	35	31	34

6

376. In the **derivatives sector**, the NFA and the CME Group are the frontline examiners, although the CFTC retains jurisdiction to conduct examinations and can do targeted reviews. CFTC oversees the NFA and the CME Group and is not directly involved in examinations of FCMs and IBs on a routine or exception basis. CFTC also brings enforcement actions against institutions based on its own investigations and SAR reviews, and in some cases following identification by the NFA or CME group of KYC deficiencies or failures to investigate suspicious activities. NFA conducts most of the direct examination of its registered entities (non-clearing FCMs and IBs) and brings disciplinary actions against such entities for compliance deficiencies. AML/CFT compliance is part of the broader examination program. Factors generally considered during such examinations include business model, prior examination findings, number of SAR filings, business emanating from high risk countries etc.

Table 20. Number of examinations of FCMs and IBs

Agency		2012	2013	2014
CFTC	# of institutions regulated for AML	1 402	1 366	1 379
	# of failure to supervise actions, including failure to follow AML procedures	3	0	2
NFA	# of institutions regulated for AML	1 353	1 318	1 334
	# of AML examinations	122	74	82
	# of formal AML enforcement actions (including Civil Monetary Penalty (CMP))	7	5	4
	# of informal AML enforcement actions (including CMP)	66	50	44
CME	# of institutions regulated for AML	49	48	45
	# of AML examinations	7	5	11
	# of formal AML enforcement actions (including CMP)	0	0	1
	# of informal AML enforcement actions (including CMP)	0	0	2

377. In the **life insurance sector**, an AML/CFT examination component is included in the NAIC Handbook. The IRS-SBSE began Federal AML/CFT supervision of the sector in 2006 when the sector came under BSA obligations, but after several years with no enforcement actions (BSA violations), FinCEN determined IRS-SBSE's examination resources would be better used elsewhere. Examinations were turned over to the State authorities. Life insurance companies are required to assess risks with respect to Covered Products but there is no corresponding process for State



supervisors to assess the risk as is the case in the FBA sector. The AML/CFT component of the supervision process is less rigorous than for banks, which is consistent with the lower risk this sector represents. The overall quality of the process varies widely from State to State, mostly depending on each State's knowledge and understanding of ML/TF risk, which appears to vary materially. For example in Iowa, there appears to be little focus on risk and the process appears essentially to be a check for the presence of expected elements. On the other hand, DFS-NY appears to take a more sophisticated approach based on its knowledge of the banking sector.

378. In the **MSB sector**, the coordinated supervision effort by States participating in the MTRA/MMET is a strength. The MMET coordinates approximately 75 multi-State and State/Federal examinations per year. State supervisors appear to be focused on risk across States and come together to decide which money transmitters should be the subject of joint examinations. Supervisors select entities to examine based on risk and the BSA MSB Manual sets out a risk-based approach to individual examinations. Furthermore, IRS-SBSE also conducts MSB examinations. For example, during 2014-15, IRS-SBSE examined 517 MSBs, which included 171 principal MSBs and 346 of their respective branches and agents. IRS-SBSE also examined a further 7,341 MSBs operating as small independent MSBs, including any MSB services provided as an agent to a principal MSB.

379. In the **DNFBP sector**, the assignment of AML/CFT supervision of casinos to IRS-SBSE resulted in close attention to ML risk in the casino industry and by the State casino regulators. However while the IRS examination manual (chapter 4.26) refers to identifying non-bank FIs which are not regulated for BSA compliance by any other Federal regulator, and to risk analysis in relation to examinations, it appears that the risk IRS-SBSE takes into account in deciding where to apply its examination resources is, in fact, the risk of non-compliance with the BSA obligations, rather than ML/TF risk. IRS-SBSE did, however, examine 60 casinos and 30 dealers in precious metals and stones during 2014-15.

380. While there are ongoing ethical or code of conduct requirements in some DNFBP sectors (lawyers and accountants in particular), and professional supervision of these requirements, they are not focused on ML/TF risks and tend to be considered only in the context of a complaint. Only the OFAC requirements and the Form 8300 reporting requirements apply at a broader level across all the businesses and professions. OFAC does not supervise for its requirements, in these sectors. IRS-SBSE supervises compliance with the Form 8300 reporting requirements, noting that reporting of suspicions in this context is voluntary. This limited AML/CFT supervision of the majority of DNFBPs is a major gap in the supervisory framework.

### *Remedial actions and effective, proportionate, and dissuasive sanctions*

381. The supervisory process has resulted in identifying, remedying and sanctioning failures to comply with the AML/CFT requirements. In the **banking and securities sectors**, FinCEN has brought enforcement actions. Each FBA and other Federal regulators also pursue their own action in parallel with FinCEN (and State regulators), and this strategy extends to parallel criminal enforcement measures exercised by the DOJ. Authorities provided case studies indicating that referrals from FBAs and other Federal regulators to DOJ take place and are supported by clear processes. FBAs and other Federal regulators take a range of remedial actions, further discussed below.

382. Broadly, the type and range of enforcement sanctions applied appear to be satisfactory. Authorities provided a number of case examples demonstrating enforcement action imposed by FBAs, SEC and FINRA against FIs and responsible individuals for BSA/AML compliance failures.

383. Specifically in the banking sector, FBAs actively require FIs to implement corrective measures to address control weaknesses which do not merit a financial penalty (but failure to implement may result in an informal or formal action including CMP). These actions may include issuing supervisory findings in the form of Matters Requiring Attention (MRAs) and Matters Requiring Immediate Attention (MRIAs) that identify specific deficiencies or control weaknesses, and require the depository institution to take corrective actions in a time bound manner. MRAs/MRIAs are deemed corrected only after follow up and verification by FBAs. Authorities have indicated that these mechanisms are an important tool to correct deficiencies and it seems these are effective in preventing issues which, in the absence of these mechanisms, might otherwise worsen and require further formal or informal enforcement action. FDIC uses the mechanism of Matters Requiring Board Attention (MRBA) as a similar tool to highlight material issues and recommendations needing expeditious consideration by the directorate and between examination follow-up by regulators. MRBA does not preclude the FDIC from citing a violation of law related to the item that directors and management should address. State banking regulators use a similar approach to State-supervised banks. Similarly, in the securities sector, regulated entities are also required to implement corrective measures when deficiencies are identified.

384. In appropriate cases, where a specific commitment from the board of directors is needed, FBAs can and do use informal actions such as Bank Board Resolutions (BBRs) and MoUs. These contain more explicit commitments that the banks need to make to support the correction of the problems identified. NCUA's informal actions include a Document of Resolution (DOR) which outlines the highest priority issues that need to be corrected as per corrective action plan agreed by credit union.

385. Formal enforcement actions are always made public. These comprise written enforcement agreements, cease and desist (C&D) orders, CMPs, and removal and prohibition. In more egregious violations, this may also include termination of charter, deposit insurance and of U.S. banking activities. There is also a mandatory statutory requirement for the FBAs to issue a C&D Order against a bank for (i) failures of the bank's compliance program and for (ii) the failure to remediate a BSA "problem" that was previously brought to the attention of the bank. Case studies were provided by authorities where enforcement actions were taken, often in coordination with State regulators and DOJ, indicating a coordinated approach (See box below):

#### Box 27. Examples of coordinated enforcement action

**OCC and other agencies:** In December 2012, the OCC (coordinating with the DOJ, the BGFRS, FinCEN, OFAC and the New York County District Attorney's Office) imposed a USD 500 million CMP against a bank for BSA violation and its failure to fully comply with a C&D order issued in October 2010. The order required the bank to take comprehensive corrective actions to improve its BSA compliance program, while deferring the OCC's decision on assessing a penalty. The OCC also issued a separate C&D order to address deficiencies in the bank's enterprise-wide compliance program. Some of the key deficiencies assessed in the consent order for the assessment of CMP included:

- Deficiencies in BSA/AML monitoring of certain wire transfer transactions.
- Failure to perform BSA/AML monitoring of bulk cash transactions with group entities.
- Failure to collect or maintain CDD or EDD information for Group Entities.
- Failure to dispose alerts appropriately and to comply with SAR obligations.
- Failure to appropriately designate customers as “high-risk” for BSA/AML monitoring.

**FDIC:** In July 2015, FDIC and California Department of Business Oversight (CDBO) imposed CMP of USD 140 million and USD 40 million respectively against a bank for its failure to implement an effective BSA/AML compliance Program over an extended period of time. The institution failed to (a) retain a qualified and knowledgeable BSA officer and sufficient staff (b) maintain adequate internal controls reasonably designed to detect and report illicit financial transactions and other suspicious activities, (c) provide sufficient BSA training, and (d) conduct effective independent testing.

386. The following statistics relate to BSA formal enforcement action taken by FBAs. Assessors were also provided with data on MRA/MRIA and other informal enforcement action taken by the four FBAs, which the U.S. authorities cited as confidential and hence are not published in this chapter.

Table 21. **Formal enforcement action taken by FBA**

Agency		2013	2014	2015
<b>BGFRS</b>	Number of formal enforcement actions <sup>1</sup>	8	4	12
<b>FDIC</b>	Orders	22	20	19
	Civil Monetary Penalties (CMP)	0	0	2
	Removal Actions	0	1	0
	Suspensions and Prohibitions	0	1	0
<b>OCC</b>	Formal Enforcement Actions	16	16	8
<b>NCUA</b>	Cease and Desist Order	1	0	0

**Table note:**

1. Although formal enforcement actions are tailored to a specific institution, they are issued publicly.

387. In the **securities sector** when deficiencies are identified, SEC staff and FINRA issue a deficiency letter or cautionary letter respectively, requiring written responses from registrants on corrective steps to be taken by them. This is not considered an enforcement action. This may be followed up by examinations from FINRA or in limited cases by SEC itself to verify the position. Both SEC and FINRA have a range of sanctions available to them. Formal actions by FINRA can result in fines, disgorgement, restitution and expulsion of firms.

Table 22. **AML Deficiencies Cited in Examinations and Formal enforcement action taken by SEC and FINRA**

Agency		2013	2014	2015
SEC <sup>1</sup>	Number of AML deficiencies cited in SEC examinations	125	86	150
	Number of formal enforcement actions	1	0	2
FINRA <sup>2</sup>	Total number of exams that cited AML as a deficiency	410	238	207
	Total number of exams with AML citations that resulted in informal action (cautionary letter) requiring remedial measures	327	207	177
	Number of enforcement actions that included an AML charge	35	31	34

**Table notes:**

1. Data for SEC pertain to fiscal years 2012-13, 2013-14 and 2014-15.

2. After conclusion of each examination, an examination Report is issued to the firm, which includes deficiencies and recommendations. A formal written response that identifies the corrective action the firm has taken/plans to take is required. FINRA will then send a disposition letter that may be: No Further Action needed, Cautionary Action or Referral to Enforcement.

388. In the **derivative sector**, the bulk of supervision and enforcement actions are taken by NFA, with CFTC only exercising oversight on NFA.

Table 23. **Informal and formal enforcement action taken by NFA**

		2013	2014	2015
NFA	Number of Informal Actions	50	44	51
	Total number of AML deficiencies cited	78	75	82
	<b>Main areas of deficiencies (in %)</b>			
	Policies, procedures and internal control	50	45	32
	Annual independent testing	27	29	34
	Designation of compliance officer	0	1	1
	Training	23	24	33

389. During 2012-15, NFA filed 17 complaints before its Business Conduct Committee alleging violations, including AML deficiencies. Most resulted in CMPs ranging from USD 15 000 to USD 500 000 and in some cases, barring individuals from applying for membership of NFA in the future or acting as compliance officer. As indicated earlier, CFTC does not directly supervise FCMs and IBs.

390. In the **life insurance sector**, State supervisory authorities generally issue AML supervisory findings on an exception basis. The State regulators interviewed had no MRAs or MRIAs (equivalent to the banking sector) statistics and informed the assessors that AML non-compliance issues are handled informally and not in writing, and therefore, no information was provided to the assessors on the

results of State examinations. Prior to being directed to cease BSA examinations by FinCEN, IRS-SBSE had also not identified any compliance violations in the life insurance sector for referral to FinCEN for enforcement. The authorities attribute the lack of enforcement measures to the IRS not having found any violations warranting an enforcement action. The assessors were thus unable to determine whether the supervisory measures taken on AML/CFT obligations in the life sector are effective, although the weighting put on this sector is low.

391. **Money transmitters:** State supervisors report to FinCEN on MSB BSA compliance. In 2015, they reported conducting 2061 MSB examinations, uncovering a total of 767 BSA violations where FinCEN took enforcement measures. FinCEN can refer matters it is aware of to the State authorities for licensing action, and notify the relevant State whenever civil enforcement remedies under the BSA may be warranted. However, it is not clear what action the States may have taken as a result. Furthermore, IRS-SBSE provided some case examples of referrals being made by it to FinCEN after examinations. FinCEN has assessed 18 CMPs based on referrals from the IRS since the previous MER.

392. **Casinos** are subject to significant licensing and other sanctions and remedial actions. In relation to **DNFBPs other than casinos** (and to a limited extent dealers in precious metals and stones), there are limited AML/CFT obligations and hence very little supervision and, therefore, no sanctions. While the U.S. provided cases examples of criminal sanctions taken against lawyers and others for their complicity in ML, these do not relate to the enforcement of (minimal) AML/CFT obligations. While there is some good (non-enforceable) guidance in place in relation to lawyers, there was no indication as to the level of compliance with the guidance and, as it is voluntary, there would be no remedial action taken against lawyers for non-compliance. Similarly, company service providers are registered at the State level but are not specifically supervised or sanctioned for AML/CFT. As noted in other parts of this report, the risks relating to advice on and formation of legal persons and arrangements and to real estate are such that this gap significantly affects the effectiveness of the system.

### *Impact of supervisory actions/criminal proceedings on compliance*

393. FBAs report that the MRAs/MRIAs are having a positive effect on the level of compliance by **banks**. Statistics on these were provided to the assessors, but are not included in this report at the request of the authorities due to confidentiality reasons. The overall numbers of MRAs/MRIAs are considerably higher than the number of enforcement actions which tends to substantiate the view of the FBAs that remedial measures reduce the eventual number of enforcement measures needed. Authorities stated that public enforcement actions have a strong impact on the level of compliance across industry, a view supported by the private sector participants during the on-site visit. Furthermore while not a supervisory action, in respect of criminal prosecutions, DOJ also uses Deferred Prosecution Agreements (DPAs) under which the institution agrees to fulfil certain requirements to correct its failures, frequently with a monetary penalty. A monitor may also be appointed to assess compliance with the terms of the DPA. A DPA does not conclude until all the requirements are complied with and the monitor is satisfied that this is so. These DPAs are public, having an impact on the industry in terms of acceptable regulatory standards. However, no statistics were provided on the numbers of DPAs, or underlying violations.

394. In the **securities sector**, the SEC and FINRA have also brought actions against individuals for compliance and supervision failure, apart from actions against firms. This has resulted into fines, debarment and suspensions and also an articulation of supervisory expectations and industry standards.

Table 24. **Actions against Individuals taken by SEC and FINRA**

Agency		2013	2014	2015
SEC	Number of Individuals charged with an AML violation	2	0	0
FINRA	Number of Individuals charged with an AML violation	11	15	18

395. In the **life insurance sector**, only Covered Products are subject to AML/CFT measures including risk assessments. The large insurance conglomerates with banking or investment subsidiaries do in practice address group-wide risks. The State regulators do not conduct their own risk assessments in this sector, and the results of supervision often do not result in written findings. Although no statistics or more detailed information on supervisory remedial measures have been provided, there have been no enforcement actions which is consistent with the view that this sector is of lower risk than other FI sectors. The authorities note that most insurance industry SARs cite potential fraud against the insurer rather than a suspicion of ML/TF.

396. FinCEN has taken civil enforcement actions against **MSBs** for serious violations of their AML/CFT obligations, including failing to register with it. Since 2010, FinCEN has assessed penalties against eleven MSBs for failing to register, among other violations. The average penalty assessed for these violations was approximately USD 85 000. In addition, in two cases involving serious violations, in addition to failing to register, FinCEN entered consent orders in which the respective MSB owner/operator agreed to cease engaging in conduct and transactional activities related to money transmission, effectively barring them from operating as an MSB.<sup>43</sup>

397. For **casinos**, there is an increased focus on raising awareness and improving compliance. Coupled with an enforcement action taken by DOJ against a casino operator in 2015 resulting into payment of USD 47.5 million fine for failure to file SARs, this has led to significant increase in SAR reporting levels from the sector (see chapter 5). On-site discussion with authorities, State regulators and casino operators indicated that the sector has reacted positively to the emphasis being placed on this sector from compliance perspective.

#### *Promoting a clear understanding of AML/CFT obligations and ML/TF risks*

398. FinCEN and its domestic law enforcement and regulatory stakeholders conduct extensive outreach programs and provide well-regarded guidance, advisories and other information to engage the private sector and enhance the abilities of reporting entities. This includes: formal guidance provided to reporting entities by FinCEN, the FBAs, other FFRs, some State agencies, and law

<sup>43</sup> See e.g. “In the Matter of [Saleh H. Adam dba Adam Service](#)” and “In the Matter of [Aurora Sunmart Inc. and Jamal Awad](#)”.



enforcement partners. Numerous advisories (some public and others non-public distributed by FinCEN through its secured network) on a diverse range of threats ranging from mortgage fraud to financing terrorist organizations; enforcement actions published by regulators; and direct clarification and assistance provided by FinCEN and partners to reporting entities tend to promote an understanding.

399. The BSAAG is active and has a number of working groups that deal with issues of broad significance to reporting entities. Industry bodies work with FinCEN via the BSAAG and as a result assist in promoting an understanding within industry. There is a case for further strengthening its effectiveness by involving a wider range of FIs and State supervisors within BSAAG.

#### Box 28. Examples of awareness-raising programs of Federal Financial Regulators

The **OCC** organizes periodic workshops for Boards of Directors and CEOs of its supervised institutions (nine director workshops scheduled for 2015). It also organizes compliance officer roundtables for mid-size banks. These are intended to raise awareness among compliance officers, directors and senior managers of the ML/TF typologies and discuss regulatory requirements and supervisory expectations for identifying and mitigating associated ML/TF risks.

The **FDIC** offers a series of educational videos designed to provide useful information to bank directors, officers, and employees on areas of supervisory focus and regulatory changes. BSA/AML topics are included in some of these videos.

**SEC** and **FINRA** conduct regular meetings with industry groups to discuss AML issues, including risks, common exam findings, and supervisory expectations based on recent enforcement actions. SEC and FINRA each publish their respective examination priorities which include AML issues.

400. There is good guidance and outreach by authorities for the regulated sectors, and especially in the banking and securities sectors. Even so the assessors were told by those interviewed from these sectors that they continue to have a strong appetite for more directed and topical guidance given the complexities of BSA requirements and the manner in which the FBAs communicate enforcement findings. Guidance on the articulation between the immediate reporting requirement and the SAR obligations above thresholds would clarify the scope of these requirements and favour their efficient implementation. There is a significant gap in relation to DNFBPs other than casinos. In some sectors, there is voluntary [Good Practices Guidance](#), such as that issued by the ABA, which has also made efforts to publicize to State and local bar associations [Formal Opinion on ML](#) related issues. However it is unclear to what extent this has had any impact across the sector.

**401. The U.S. is rated as having a moderate level of effectiveness for IO.3.**



## CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

### *Key Findings and Recommended Actions*

#### *Key Findings*

1. The NMLRA highlights instances of complex structures, shell or shelf corporations, trusts, foundations and other forms of legal entities being used to obfuscate the source, ownership, and control of illegal proceeds. The vulnerability of legal persons to ML/TF is understood to different degrees by the competent authorities: the Treasury, LEAs and prosecutors have a higher level of understanding than State authorities who create and supervise them.
2. It is estimated that more than 30 million legal persons exist in the U.S. with about two million new legal persons created every year in the 56 incorporating jurisdictions. There is no information on how many legal arrangements subject to State law may be in place as these do not require State action to create. Information on how to create legal persons and arrangements in the U.S. is widely available publicly, and legal entity use is attractive as illustrated by the large number of incorporations each year. The relative ease with which U.S. corporations can be established, their opaqueness and their perceived global credibility makes them attractive to abuse for ML/TF, domestically as well as internationally.
3. Measures to prevent or deter the misuse of legal persons and legal arrangements are generally inadequate. The U.S. primarily relies on the investigatory powers of LEAs and certain regulators to compel the disclosure of ownership information. These powers are generally sound and widely used. However, the system is only as good as the information that is available to be acquired. The BO information available within the U.S. is often minimal or cannot be obtained in a timely manner for companies not offering securities to the public or not listing their securities on a U.S. stock exchange. There are no mechanisms in place to capture BO information on legal entities at the formation stage, and there are currently no measures in place to systematically collect BO information (as defined by the FATF) in all cases through CDD measures in the FI/DNFBP sectors. No mechanism is realistically available to authorities to collect BO information on legal arrangements from the trustee or other parties, other than through trust companies, and the extent to which these act for all trusts is unknown.
4. The ability of the U.S. to use the States' formation processes as a means of LEA timely access to accurate and adequate BO information is significantly impeded, because the States do not verify the information they collect on legal persons. The States consider their role in company formation to be administrative in nature without any control function. In keeping with the States' views on ML/TF risk generally, States do not consider that they have a significant AML/CFT role during the company formation/registration process. Federal legislative efforts to facilitate collection of adequate, accurate and current beneficial ownership (BO) information on legal persons have not been successful to date, through the company formation process, through requirements imposed on legal entities themselves or through CDD measures applied in the financial and casino sectors.
5. Trustees (except for trust companies) are not subject to comprehensive AML/CFT

obligations, but there are no obstacles to accessing BO information where held by trustees, provided that the LEAs know the status of trustee. LEAs demonstrated that they can and do access BO information but this involves substantial investigative resources which negatively impacts timeliness of access.

6. Some relevant information is collected as part of the requirement (where applicable) for legal entities in the U.S to obtain an Employer Identification Number (EIN) from the IRS. The authorities provided examples of LEAs' ability to obtain adequate and accurate information about the BO of legal persons created in the U.S. using the wide range of financial investigation tools at their disposal. However, because adequate and accurate BO information is not systematically collected and therefore readily available, it is not clear this was accomplished on a timely basis. The State authorities can only provide limited assistance since no State collects BO data at the time of incorporation or subsequently, nor do they impose this obligation on legal persons. There are no meaningful sanctions imposed on legal persons for non-compliance with the present informational requirements. For trusts, sanctions would involve bringing civil actions by the beneficiaries against the trustee.
7. The U.S. Federal authorities experience difficulties in collecting statistics from the State authorities on company formation: notably the lack of statistics on: the numbers and types of legal entities formed in each State; whether such formations were triggered through a person representing the new company or through a company formation agent; and requests to States by LEAs about specific entities.

### ***Recommended Actions***

1. Take steps to ensure that adequate, accurate and current BO information of U.S. legal persons is available to competent authorities in a timely manner, by requiring that such information is obtained at the Federal level, and in doing so, ensure that (a) BO information is collected from all legal persons including those formed to hold real property, and (b) BO information obtained is made available systemically to LEAs in a timely fashion.
2. To address the vulnerability of legal entities being used as shell companies or nominees, consider amending the BSA regulations to prohibit FIs from providing financial services (including correspondent banking services) to any U.S. legal person, where any U.S. person in the BO chain of ownership does not have an EIN issued by the IRS.
3. Build upon the 2016 rule making (BO measures applicable to the financial sectors) by ensuring that FIs can make BO information available to LEAs in a timely fashion.
4. Ensure that the appropriate Federal competent authority collects and compiles the following statistics for monitoring the exposure of U.S. legal entities to ML/TF:
  - The number and types of legal entities formed in each State;
  - Whether entities are created directly by the beneficial owner, or through intermediaries such as lawyers, CFAs or other TCSPs
  - The number of requests from law enforcement processed by States regarding specific entities.
5. Consider measures to limit or terminate the ability of shareholders and/or directors to act as

nominees. Alternatively create a specific obligation for them to disclose their nominee status and for FIs and DNFBPs to identify if they are nominees, wherever providing services to such persons.

6. Ensure that trustees are subject to an AML/CFT obligation to declare their status to FIs and DNFBPs, and an explicit obligation to obtain and hold adequate, accurate and current information on identity of all parties to trusts, including any other natural person exercising ultimate effective control over trusts.
7. Ensure that proportionate and dissuasive sanctions are applied for failure to comply with the measures set out in the foregoing.

402. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The recommendations relevant for the assessment of effectiveness under this section are R24 & 25.

### ***Immediate Outcome 5 (Legal Persons and Arrangements)***

#### *Public availability of information on the creation and types of legal persons and arrangements*

403. Information on types of legal persons that may be established in the U.S. and how to create them is available on the internet for each State, territory and the District of Columbia (collectively referred to in this Chapter as “States”). Each State creates and dissolves legal entities, and it is the State that has the power to verify the legal entities’ status. Consolidated links are freely available on the website of National Association of Secretaries of State (NASS) (see [link](#)) which makes the information easily accessible.

#### *Identification, assessment and understanding of ML/TF risks & vulnerabilities of legal entities*

404. The ML/TF vulnerabilities of legal persons and arrangements are well understood by law enforcement, prosecutors and Treasury, but less so by others, including representatives of Secretaries of States (the competent authority at the State level, responsible for the registration process). As noted in chapter 1, as an attractive and popular destination for company formation, the U.S. faces particularly significant vulnerabilities to ML/TF through legal persons and, to a lesser extent, legal arrangements, because of the lack of transparency that is built in to these vehicles. This vulnerability is not mitigated by existing BO measures and key sectors (lawyers, accountants, company formation agents and trustees (other than trust companies)) are not subject to comprehensive AML/CFT requirements. As in many countries, there is no requirement to use an intermediary in the U.S. and it is estimated that approximately half of the legal entities formed in the U.S are so formed. The vulnerabilities are further amplified by contextual factors (the enormous size of the company formation industry and the large number of companies formed in the U.S.).

405. The role of domestic legal entities in financial crime and ML was assessed in a sectoral assessment in 2006. The 2015 NMLRA also identifies several cases where legal entities (mostly corporations, limited liability corporations and in a few cases, trusts) have been misused for illicit purposes, including through complex structures involving front companies, shell companies and shelf companies. In many instances, these are used to disguise the intermingling of licit and illicit profits and incomes. To a much lesser extent

(as noted in the NMLRA), trusts have been identified in complex ML schemes, but there is no information on the numbers of trusts organized under U.S. States' laws.

406. The authorities agree that the absence of a physical presence can be a problem with the U.S. legal entities due to the difficulty of identifying the individuals (i.e. beneficial owners) who may use shell companies to conduct illicit activities. This remains a long standing vulnerability across a range of criminal predicates including healthcare fraud, sanctions evasions, ML and corruption.

407. FinCEN demonstrated its awareness of the vulnerability posed by legal entities being abused for hiding assets through the real estate, by issuing a GTO on 13 January 2016. The GTO required certain U.S. title insurance companies to identify the natural persons behind legal entities used to pay "all cash" for high-end residential real estate purchases in Manhattan, New York and Miami-Dade County, Florida, and to report the true BO behind the transaction. This is intended to address concerns that all-cash purchases may be conducted by individuals attempting to hide their assets and identity by converting funds to high-end residential properties using limited liability companies or other opaque structures<sup>44</sup> (see also paragraph 82 and 293).

#### *Mitigating measures to prevent the misuse of legal persons and arrangements*

408. Overall, measures to prevent the misuse of legal persons and legal arrangements are inadequate. The existing U.S. legal framework has serious gaps impeding effectiveness in this area regardless of the methods used to address systemic access to BO information (see R.24, R.25, R.10 and R.22). This is a priority issue that was flagged in the previous mutual evaluation of the U.S. Unfortunately; efforts to strengthen the legal framework in this area have been unsuccessful to date.

409. The formation process for legal persons varies across States, as does the information collected by States during the entity formation process and in annual/periodic reports<sup>45</sup>. During the formation process: only 23 States collect the principal office address from corporations, and 31 collect it from LLCs; 17 States collect the names and addresses of officers and/or directors (or persons with similar authority) from corporations; and 20 States collect the names of managers or members from LLCs. Formation documents in several States specify that this information is optional.

410. As part of annual/periodic reporting: 40 States collect the principal office address (or similar address) from corporations; 30 States collect the principal office address (or similar address) from LLCs; 46 States collect the names and addresses of officers and/or directors (or persons with similar authority); 33 States collect the names of LLC managers or members (or persons with similar authority); only 3 States collect some form of entity ownership or control information from LLCs, and only 4 States collect some form of entity ownership or control information in corporate periodic reports for companies.

<sup>44</sup> This is a temporary measure which will expire on 27 August 2016. This Order only came into effect on [1 March 2016](#) which is after the on-site visit. Consequently, this measure cannot be considered for the purpose of Core Issue 5.3 (how well the country has implemented measures to prevent the misuse of legal persons/arrangements, but its issuance before the on-site visit is taken into account in Core Issue 5.2 (how well the competent authorities understand the risks)).

<sup>45</sup> NASS Summary of Business Entity Information collected by States: <http://www.nass.org/nass-initiatives/nass-company-formation-task-force/>



411. States do not consider that they have a significant AML/CFT role during the company formation process. This is consistent with the Federal authorities' view that Federal authorities are responsible for the AML/CFT regime as a whole (as noted in Chapter 1). The Offices of the Secretaries of State review each application for incorporation to ensure that it meets the statutory requirements; however, the information contained in the application is generally not verified. Representatives of State authorities indicated to the assessors that States are in competition with one another to create companies, as part of strategies designed to improve their respective economic development.

412. As noted, States do not verify the information collected during the formation process which means that, in practice, the information held by them may not be accurate. Although false information provided during the corporation registration process may sometimes generate leads for LEAs, and help prosecutors to establish intent to evade applicable law in certain criminal prosecutions where such intent is a required element, the lack of verified basic information significantly weakens the impact that these measures have on preventing the misuse of legal persons.

413. A few states (Delaware, Wyoming and Nevada) have taken some preliminary steps to raise awareness about the misuse of legal persons. This includes publication of a Best Practices Paper in 2013 to highlight new developments in State company formation laws in these States and to set forth best practices of "company registries" in the U.S. The suggested "best practices" do not go far enough to meet the requirements of the FATF Standards and it is also unclear as to whether this non-enforceable guidance has led to any meaningful improvements in understanding, or the taking of any mitigating steps by any of the other States.

414. With respect to legal arrangements, there do not appear to be any obstacles preventing LEAs from accessing BO information that may be held by trustees. However there is no explicit obligation either in State common or statute law, or in the BSA, that obliges trustees to gather and retain BO information (as defined by the FATF) (although in practice the trustee may have access to this information in order to fulfil fiduciary obligations (if any) to the settlor or the beneficiaries of the trust). Further, unless LEAs know who the trustee is, it may be difficult to pursue enquiries through the financial or DNFBP sectors.

#### *Timely access to adequate, accurate & current basic/BO information on legal persons/arrangements*

415. Overall, basic information is available on legal persons provided the State of incorporation is known. Similar information may be available on trusts provided the trustee is known. However, BO information on legal persons is not generally accessible to the standards expected by the FATF in a timely manner due to the absence of: a) any requirement to collect BO information at the time of formation; and b) effective measures in place to collect BO information from legal persons or arrangements. LEAs use investigative techniques and procedures (e.g. surveillance operations (which can be lengthy), witness interviews, and searches for evidence) to obtain this information as needed.

416. Some limited measures are in place. U.S. law requires all entities formed in the U.S (with narrow exceptions) and any other entity that has a Federal or State tax filing requirement to obtain an Employer Identification Number (EIN) for tax administration purposes, if they have income, employees, or are otherwise required to file any documents with the IRS. EIN is also required under the BSA to open a bank account. In order to obtain an EIN, a legal entity must designate a “responsible party”. While the definition of a “responsible party”<sup>46</sup> might, in certain cases, help to identify the BO of a legal person, it is not synonymous with that term (as it is possible for someone other than the BO of a company, for example a principal officer to act as a responsible party) (see R.24 for a detailed analysis). In addition, not all legal entities are required to obtain an EIN and the responsible party information is accessible by LEAs for non-tax investigations only through a court order. Furthermore, private companies formed to hold land have no need to register with either the SEC or IRS. An EIN is also not required for a company that does not have a bank account with a U.S. FI or that does not have income, employees or is otherwise not required to file any documents with the IRS.

417. For legal entities with an EIN, any changes in “responsible party” need to be reported within 60 days. Entities are not subject to penalties for failure to make such a reporting. The only consequence of a failure to provide the IRS with the current identity of the “responsible party” is the potential non-receipt of a deficiency notice or tax demand notice from the IRS (and penalties and interest will continue to accrue on any tax deficiencies). Thus, apart from the discrepancies between the “responsible party” and the FATF BO definitions, the requirement to update EIN information is more a tax administration measure than a mandatory obligation to ensure accurate and up-to-date information about BO. This significantly reduces the adequacy, currency and accuracy of BO information that could be obtained by LEAs as part of their criminal investigations. Nevertheless, the EIN system is a potentially strong existing mechanism that could be appropriately levered by the authorities for the recording of BO information as contemplated by R.24.

418. FIs are only obliged to collect BO information (as defined by the U.S.) on corporations and legal arrangements in limited cases (see R.10 and Chapter 5).<sup>47</sup> However, in practice, many FIs do collect (although they do not verify) such information in certain circumstances based on joint regulatory guidance issued in March 2010. Depository institutions are required to have enhanced due diligence procedures for higher-risk customers and among the procedures suggested in such circumstances is collecting information on individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors. Regarding trusts, the authorities stated that FIs can identify the trustees and verify their identity, if the trustee is the person opening the account, despite the absence of a mandatory requirement for the trustee to self-identify. However, while these measures help to a limited extent, they are not adequate to ensure timely access to BO information in all high risk cases.

419. Although company formation agents (CFAs) are involved in forming companies on behalf of others and providing related services (e.g. serving as a registered agent), individuals and legal

<sup>46</sup> The “responsible party” is defined, for non-publicly traded companies, as “the person who has a level of control over, or entitlement to, the funds or assets in the entity that, as a practical matter, enables the individual, directly or indirectly, to control, manage, or direct the entity and the disposition of its funds or assets.”

<sup>47</sup> Since the on-site, the Final CDD Rule on BO was issued on 5 May 2016. The implementation period for the Rule is two years. (see <https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx>)

entities can perform these functions for themselves directly with State authorities. While some States do not define or recognise CFAs, others register them in the form of ‘registered agents’ or ‘commercial registered agents’ but their role is limited to accepting notices of service of process, other legal or tax notice or demands and to forward them on to the company<sup>48</sup>. CFAs are not subject to comprehensive BSA AML/CFT requirements. Consequently, even when a CFA is involved, there is no mechanism to collect or maintain BO information.

420. Although their involvement is not required, in practice, lawyers and accountants may also become involved in the company formation process, particularly for more complex corporate structures or for the purpose of preparing financial advice, statements and filings. As with CFAs, where lawyers and accountants are involved, they are not subject to comprehensive AML/CFT obligations, so there is no mechanism to ensure that they will have collected and maintained basic and BO information.

421. Authorities stated during the on-site visit that investigators will follow the money and conduct a criminal financial investigation whenever deemed necessary. The authorities provided case examples demonstrating that LEAs are able to obtain adequate and accurate information about the BO of some legal persons/arrangements created in the U.S., however there was no information available on the actual lengths of time it took the authorities to identify the BO where that was key to the success of the cases. LEAs advised the assessors that they must often resort to gathering this information through time-consuming, resource-intensive, and lengthy investigations, which may involve: detailed analysis of bank accounts and transaction records; physical around-the-clock surveillance; collection of emails; conducting searches; interviewing potential witnesses, etc. As a result, the competent authorities are not always able to access such information in a timely manner, and thus it cannot be said that there are no impediments to their collection of such information. The requirement to launch a full and costly investigation cannot be construed as an effective mechanism for timely access to adequate, accurate and current BO information. LEAs indicated that reforms that would give them easier access to IRS information on BO would be welcome from their perspective.

#### Box 29. Use of investigative powers to obtain beneficial ownership information

**Le-Nature Inc. (Greg Podlucky, et al) (2011-2012):** This case shut down a complex ML scheme involving fraud and tax evasion connected to a sophisticated Ponzi scheme. The proceeds were laundered through numerous legal persons and arrangements established to conceal the BO of these illicit assets. **Investigation:** Although authorities obtained legitimate business records from third parties via grand jury subpoena, conducted numerous third party interviews to determine the true ownership (as opposed to paper ownership) after following the source of payments for the acquisitions and tracing the flow of the funds through the myriad of bank accounts, no information was provided on the length of time this process took. **Outcome:** Podlucky pleaded guilty to one count of conspiracy to commit ML. In 2011, he was sentenced to 20 years imprisonment

**650 Fifth Avenue and Related Properties:** The DOJ obtained forfeiture of substantial assets controlled by the Government of Iran, including a 36-story office tower in Manhattan at 650 5<sup>th</sup>

<sup>48</sup> Such service providers must be registered in Nevada and Wyoming, and licensed and registered in Delaware.

Avenue with an appraised value of USD 525 million, other properties, and several million dollars in cash. Ownership of the office tower was split between Bank Melli (40% through shell companies Assa Corp. & Assa Ltd) and the Alavi Foundation (60%), which provided numerous services to the Iranian Government, including managing the office tower, running a charitable organization, and transferring funds from the office tower to Bank Melli. **Shell use:** U.S. authorities identified front companies used to conceal that certain U.S. assets were actually owned by Bank Melli, which had been previously designated for providing financial services to entities involved in Iran's nuclear and ballistic missile program, and was subject to a call for enhanced vigilance in UNSCR 1803. No information was provided on the length of time it took to determine the beneficial ownership of all these entities.

7

**Michael Staaf (March 2012):** In Pittsburgh, Pa., Staaf was sentenced to 120 months in prison and five years of supervised release on his conviction of conspiracy to commit bank fraud, mail fraud and wire fraud and ML conspiracy. Staaf operated Beaver Financial Services, a mortgage broker business, and several other companies that owned and managed real estate. He and several others engaged in a large-scale mortgage fraud and ML scheme involving tens of millions of dollars and dozens of mainly commercial properties. **Shell use:** One aspect of the scheme involved the purchase of properties owned by entities that Staaf controlled through an employee. Staaf would "sell" commercial property owned by an entity he controlled to another entity that he controlled at highly elevated prices. He used nominee accounts, shell corporations <sup>1</sup>, and other schemes to conceal his ownership of the proceeds of the fraud and to make the proceeds more difficult to track. No information was provided on the length of time it took to determine the beneficial ownership of all these entities.

**Note:**

1. New Bridgton Man Pleads Guilty in Large-Scale Mortgage Fraud Scheme, Press Release, United States Attorney's Office, Western District of Pennsylvania, November 21, 2011).

422. Some States seem cognizant of the fact that LEAs would like considerably more detailed information than the existing measures are designed to provide. Some States do provide assistance to LEAs by providing whatever information corporations are legally required to submit at the time of formation (however minimal). Corporate registries of States are publicly available (sometimes for a fee) and LEAs have access to them. However if law enforcement is unable to obtain BO information directly through investigation, there is little possibility that the office of the Secretary of States will be more helpful.<sup>49</sup>

423. As in the case of legal persons, timely access to adequate, accurate and current basic and BO information on legal arrangements by competent authorities faces serious impediments (as is common with many common law countries, there is no register of trusts) and there is no general obligation imposed on trustees under the BSA to declare their status as a trustee. The UTC and comparable State laws do impose obligations (which can be overridden) on trustees.<sup>50</sup> These laws do

<sup>49</sup> NASS Survey on Company Formation Process in the States available at the following [link](#).

<sup>50</sup> Section 810 (c) of the UTC states that "a trustee shall cause the trust property to be designated so that the interest of the trust, to the extent feasible, appears in records maintained by a party other than a trustee or

not specifically require BO information to be known to the trustees, though in practical terms, trustees may have access to such information in order to operate the trust. Lawyers are, in most cases, involved in setting up trusts. Lawyers are not subject to comprehensive AML/CFT requirements and it is not clear to what extent, BO information is available to them. Authorities indicated that compared to legal persons, use of legal arrangements for illegal purposes is less common as they generally require the use of lawyers to set up and these arrangements are, therefore, likely to be less attractive for criminal purposes. In any event, as in the case of legal persons, LEAs have to resort to resource-intensive and often lengthy investigations, which can be cumbersome, to access such information.

*Effectiveness, proportionality and dissuasiveness of sanctions*

424. The only sanctions against legal entities for not updating information on State company registries would be to dissolve the entity. So far as trusts are concerned, a beneficiary may bring a civil action against the trustees for breach of fiduciary duty. If the very purpose of the trust is to disguise the involvement of the parties and/or the illegal source of the trust assets, then it is highly unlikely that such an action would be commenced. If the trust is created for or subsequently used for an illicit purpose, this could invalidate the trust under State law, effectively making witting participants co-conspirators (See: UTC, Section 4).<sup>51</sup> Because the trustee is the owner of record of all assets within the trust, there is always a natural or legal person to whom law enforcement can serve subpoenas and search warrants, if they know such person is the owner. Failing to comply with such orders would be contempt of court. It is a criminal offense to provide false information to a FBI investigator.

**425. The U.S. is rated as having a low level of effectiveness for IO.5.**

---

beneficiary". However this could be accomplished without necessarily declaring to an FI the existence of the trust and the trustee's status as such and the obligation can be overridden by the terms of the trust.

<sup>51</sup> UTC Section 404 states "a trust may be created only to the extent its purposes are lawful, not contrary to public policy, and possible to achieve." The comment to this section states "a trust with a purpose that is unlawful or against public policy is invalid" but limits unlawful to situations where executing the trust requires the trustee to commit a tort or a criminal act, or to where the settlor's purpose in creating the trust was to defraud creditors or others, or the consideration of the trust was "illegal". It is not clear if this illegality addressed the proceeds of crime.





## CHAPTER 8. INTERNATIONAL COOPERATION

### *Key Findings and Recommended Actions*

#### *Key Findings*

1. The U.S. generally provides constructive and timely assistance when requested by other countries. This encompasses the range of international cooperation requests, including Mutual Legal Assistance (MLA), extradition, financial intelligence, supervisory, law enforcement and other forms of international cooperation. The U.S. also proactively seeks assistance in an appropriate and timely manner to pursue domestic predicate and TF cases which have transnational elements. The assistance requested includes requests for evidence and for the freezing, seizing and forfeiture of assets, besides financial intelligence, supervisory and other forms of international cooperation.
2. There may be barriers to obtaining beneficial ownership (BO) in a timely way, because the U.S. legal framework in this area is seriously deficient, and there are no other measures in place to ensure that BO is collected, maintained and easily accessible to the authorities. This can require resource-intensive investigations by LEAs, often impinging on timeliness and priority concerns.
3. Tax information is not generally available to foreign law enforcement for use in non-tax criminal investigations.

#### *Recommended Actions*

1. The U.S. should continue to allocate more resources to process the very large number of MLA and extradition requests, and updating the framework and systems for providing such assistance. This will facilitate timely response to cases which may not be receiving a high priority.
2. The U.S. should take urgent steps to ensure that adequate, accurate and current BO information of U.S. legal persons is available in a timely manner in order to facilitate their timely sharing, without having to resort to extensive investigation techniques and procedures in each case (see IO.5).

426. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

#### *Immediate Outcome 2 (International Cooperation)*

427. International cooperation plays a prominent and central role in U.S. efforts to combat ML and TF due to the country's particular risks (from transnational organized crime, the laundering of the proceeds from foreign predicate offenses, and international terrorism) and context (as playing a central role in the global financial system). In these circumstances, many large cases have transnational elements that require the U.S. to cooperate with other countries. At the highest level,

the President's National Security Strategy recognizes the centrality of international cooperation in criminal justice and counter-terrorism matters. Overall, the U.S. has implemented measures in this area that are broadly in line with its identified risks and context, and which achieve this Immediate Outcome to a large extent.

*Providing constructive and timely MLA and extradition*

428. Overall, the U.S. provides good quality constructive mutual legal assistance (MLA) and extradition across the range of international co-operation requests, including in relation to ML, TF, and asset forfeiture. This is demonstrated by feedback from 47 FATF and FSRB delegations on their experiences requesting international cooperation from the U.S. The vast majority of the feedback was positive and, on the basis of the responses received, there do not appear to be any systemic issues concerning the timeliness and quality of requests. This was also demonstrated through statistics and numerous illustrative case examples. As one of the largest economies and financial systems in the world, the U.S. is, understandably, the recipient of a very large number of requests for MLA in cases involving financial crime. As of July 2015, the U.S. was actively executing more than 5,200 incoming MLA requests for all criminal matters, of which 1,541 related to ML, TF, and asset forfeiture. Additionally, it was in the process of executing and pursuing more than 3,800 incoming extradition requests, of which 21 related to ML matters.

Table 25. **Incoming MLA and Extradition Requests (2009-2014)**

Incoming MLA Requests			
Total MLA requests received in criminal matters	5200±		
Total MLA requests received in matters involving money laundering, terrorist financing (providing material support or resources for terrorism), and asset forfeiture	1541		
Response to incoming MLA requests	ML	TF	Asset Forfeiture
Granted	568	53	501
Denied (grounds include lack of evidence, assistance not legally available, and other process reasons)	64	3	72
ML and asset forfeiture cases: Other reasons for not executing request (includes unable to locate evidence, withdrawn, and other non-process reasons)	150	N/A	102
TF cases: Other reasons for not executing request (includes no response from requestor, unable to locate evidence, and withdrawn)	N/A	14	N/A
Inexecutable under U.S. law	4	0	10
Total number of MLA requests related to ML, TF & asset forfeiture	786	70	685
Incoming Extradition Requests			
Total extradition requests received in criminal matters	3800		
Total extradition requests received in matters involving money laundering, terrorist financing (providing material support or resources for terrorism), and asset forfeiture	21		

Response to incoming extradition requests	ML	TF
Granted	10	0
Denied	3	0
Other (Includes cases withdrawn, fugitive not located, fugitive located in another country or fugitive arrested in requesting country)	6	0
Inexecutable under U.S. law	2	0
Total number of extradition requests related to ML & TF	21	0

429. The MLA requests reflected in the above table came from approximately 85 jurisdictions pursuant to bilateral treaties, agreements, and conventions, as well as requests sent as letters of request and letters rogatory (see R.37). Between 2009 and 2014, in ML and asset forfeiture matters, the U.S. received the most MLA requests from Switzerland, Mexico, U.K. and the Netherlands.

430. The DOJ Office of International Affairs (DOJ-OIA) executes or, depending on the nature of the assistance sought, oversees the execution of foreign requests for MLA. Its attorneys review each request, provide guidance, facilitate communication between the requesting and executing authorities, transmit evidence, and provide sample court documents for use by prosecutors and the law enforcement agents who may work with the prosecutors. For coercive measures such as restraining, seizing, and confiscating or forfeiting assets, the U.S. may provide assistance in two ways (not mutually exclusive): i) by taking actions *on behalf of* the foreign authority to advance the foreign asset confiscation proceedings (the U.S. currently has about 40 such cases ongoing); or ii) by *initiating its own forfeiture action* as part of a criminal case or a non-conviction based forfeiture (NCBF – *in rem* action) often based on evidence provided by the foreign jurisdiction.

431. Extradition requests are received through the State Department and are ordinarily referred to the DOJ-OIA for execution. The assessment team noted a potential barrier to provide assistance for requests made on the basis of extradition treaties that define extraditable offenses by felonies and where dual criminalization may be problematic (see. R.39), although the U.S. denied only one extradition request on that basis in 2012 in a case involving the laundering of proceeds from non-payment of taxes.

432. Managing such a large number of incoming requests in a timely manner presents significant challenges. The U.S. is however generally able to provide MLA in a timely manner. The DOJ-OIA maintains an electronic case management system and conducts file reviews of pending cases to prioritize requests, particularly when they involve serious offenses. Cases involving TF and ML are presumptively serious cases. The U.S. does not systematically collect statistics on how long the MLA/extradition process takes although it will benefit from a new I.T. system by the end of this year that will enable proper tracking of the time taken to respond to each MLA request. The U.S. was still able to provide estimates. The actual duration of the MLA process varies, depending on the clarity and completeness of the request received from the foreign jurisdiction, the complexity of the issues presented, whether it is possible to find the evidence sought or the person to be interviewed, and whether compulsory process is needed. The majority of feedback from FATF and FSRB delegations

noted that MLA was being provided in a timely manner. However, some delegations noted delays in specific cases, and the U.S. acknowledges that there is a backlog of pending MLA requests (presumably related to cases judged to be of lesser priority).

433. MLA requests seeking electronic subscriber information can generally be provided in three to four months, but may take up to one year if compulsory process is needed. To improve timeliness, the U.S. established the Cyber Unit in June 2014 which has submitted to court more than 800 applications for authorization to obtain electronic evidence. One delegation's feedback noted that U.S. response times for MLA requests relating to electronic data have subsequently reduced.

434. The duration of the extradition process depends on the complexity of the issues presented, the amount of time the hearing takes, number of hearing(s) required, and whether the fugitive files a *habeas corpus* petition after having been found extraditable. Extradition matters take approximately one to four months if a fugitive elects a "simplified extradition" procedure. Many fugitives waive extradition. The average contested extradition matter takes at least one year to resolve.

435. Overall, moderate improvements are needed to improve the system's effectiveness, and timeliness of responding to MLA requests in lower priority cases. Such improvements include (i) allocating more resources to process the very large number of MLA and extradition requests, and (ii) updating the framework and systems for providing such assistance. At the time of the on-site visit, the DOJ was leading implementation of a White House initiative which recognizes and addresses these issues: the Mutual Legal Assistance Treaties (MLAT) Modernization Plan. It aims at updating, improving, and accelerating the handling of requests from foreign governments for evidence. It has allowed DOJ-OIA to begin hiring more than 30 additional attorneys, 20 additional paralegals and support staff to improve the response times for foreign MLA requests, reduce the backlog of pending MLA requests (notably for electronic evidence), and train U.S. and foreign prosecutors on MLA. This is an important initiative which should continue as the DOJ-OIA's current staffing levels (approximately 60 attorneys, 30 paralegals and support staff) is not sufficient to handle the large volume of incoming MLA and extradition requests. In the interim, the Fiscal Year 2015 budget allowed the FBI to establish a dedicated group of FBI agents from its International Operations Division to assist DOJ-OIA with MLA and provided additional resources for the USAOs who also play a role in executing foreign MLA requests.

436. The U.S. provided numerous case examples which demonstrate that it provides a wide range of types of assistance in response to MLA and extradition requests and the time taken to respond to such requests (see Box 30 for a few examples). The U.S. is only able to provide intercept evidence in response to an overseas request for MLA if it opens a U.S. investigation and may find it difficult to provide BO information for legal persons or arrangements within a reasonable time (see IO.5). U.S. tax information is not generally available to foreign law enforcement for use in non-tax criminal investigations.

**Box 30. Examples of assistance provided and time taken to process requests**

**Information documenting the flow of funds (5 months):** In April 2010, DOJ-OIA received a request to provide information into the flow of funds into Liechtenstein, as they related to the investigation of a person suspected of laundering money from a fraudulent investment scheme that collected at least USD 6.7 million from investors. , DOJ-OIA provided Liechtenstein authorities with the records in September 2010. Liechtenstein authorities have record of USD 2.6 million of this flowing through their banks.

**Extradition (13 months):** In March 2014, a Colombian citizen was arrested in Haskell, Texas, on an emergency provisional arrest warrant coordinated by U.S. and Mexican authorities. The urgency stemmed from his imminent removal to Colombia. He was wanted for extradition to Mexico to stand trial on ML and organized crime charges relating to his role in a Colombia-based drug trafficking organization. In the U.S. case, he pleaded guilty to conspiracy to import cocaine. After completing his U.S. prison sentence, he was released into ICE's custody pending removal to Colombia. DOJ-OIA received the request in early March 2014, and the defendant was arrested within two weeks. Extradition proceedings following his arrest took approximately one year, and he was surrendered to Mexico in April 2015.

8

437. A particularly positive feature of the U.S. system is that DOJ-OIA assigns attorneys to cover specific countries and proactively assists foreign counterparts in preparing both MLA and extradition requests that comply with U.S. legal requirements. Regular case consultations (if necessary) are used to address any issues that may arise. There were 212 bilateral coordination meetings in 2012, 165 in 2013, and 114 in 2014. Such proactive engagement was highly praised in the feedback received from FATF and FSRB delegations, and helps to facilitate the swift execution of requests. The DOJ-OIA's public website also publishes basic information about making MLA/extradition requests, and contact links. As part of the MLAT Modernization Project, DOJ-OIA plans to provide more detailed information so that foreign authorities will be able to access information regarding the status of their respective requests.

438. International asset sharing is encouraged by U.S. authorities and often premised on freestanding international asset sharing agreements or asset sharing provisions within MLA agreements (see R.38). The U.S. can spontaneously share even when a country makes no direct request for a share of forfeited proceeds of crime that were forfeited due to assistance provided to the U.S. Since 1989, more than USD 257 million in forfeited assets has been transferred to 47 countries from DOJ's fund (DOJ-AFF, see IO.8). In the last three Fiscal Years, DOJ has shared USD 19 714 313.11 (FY2013: USD 2 124 066.45; FY2014: USD 13 588 369.68 and FY2015: USD 4 001 876.98) with 18 countries<sup>52</sup>. Since 1994, the TFF has transferred more than USD 37 million to 29 countries. To date, Antigua and Barbuda, the Bahamas, Canada, Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Singapore, Switzerland, and the United Kingdom have shared forfeited assets with the U.S.

<sup>52</sup> Antigua and Barbuda, Bahamas, Canada, Cayman Island, Czech Republic, Curacao, Dominican Republic, Greece, Israel, Italy, Korea, Luxembourg, Panama, Sweden, Switzerland, Turks and Caicos Islands, Uruguay, United Kingdom.

*Seeking timely legal assistance to pursue domestic cases with transnational elements*

439. The U.S. makes extensive use of MLA in an appropriate and timely manner to pursue domestic predicate and TF cases with transnational elements including making requests for evidence and for the freezing, seizing and forfeiture of assets. The **AFMLS Kleptocracy Initiative** (see IO.8) is an exemplar in this regard in the context of international grand corruption cases. Effectiveness in this area was demonstrated through statistics, numerous illustrative case examples provided by the U.S., and extensive discussions with the authorities. As of July 2015, the U.S. was actively seeking MLA in about 2 400 criminal matters, of which 1 542 related to ML, TF, and asset forfeiture. Additionally, it was seeking extradition in about 3 200 criminal matters, of which 457 outgoing extradition requests related to ML matters. Between 2009 and 2014, in ML and asset forfeiture matters, the U.S. sent the most MLA requests to Switzerland, U.K., Netherlands, and Canada. The U.S. provided numerous case examples which demonstrate that it seeks assistance in a wide range of cases (see example in Box below).

**Box 31. Examples of assistance requested**

**Asset sharing:** In 1999, U.S. LEAs provided information to the Criminal Police of Geneva about a suspected money launderer's activities and money transfers to accounts in Switzerland. Based on this information, the Swiss authorities opened a ML investigation against two individuals, resulting in the 2007 conviction of one individual on ML charges and the confiscation by Swiss authorities of two of his accounts at Credit Suisse, which contained a total of approximately USD 868 000. In November 2013, in recognition for the assistance provided by U.S. authorities on a ML case, the government of Switzerland shared 30% of the net forfeited proceeds, or USD 260 465, with the U.S. government.

**Extradition (ML and operating an unlicensed money transmitting business):** After fighting extradition for more than a year, in October 2014, the founder of Liberty Reserve (see Box 9), an online digital currency service extensively used by cyber-criminals with more than one million users worldwide, including over 200 000 users in the U.S. and involving transactions totaling over USD 6 billion, was extradited by Spain to stand trial in the Southern District of New York for ML and operating an unlicensed money transmitting business.

**Extradition (Terrorism):** In August 2014, Turkey extradited an individual to the U.S. to stand trial for terrorism offenses. Turkish authorities provisionally arrested him in May 2011, at the request of the U.S. He was wanted to stand trial in Arizona on one count of conspiracy to commit murder of a U.S. national and one count of providing material support to terrorists. Beginning in January 2005, he allegedly supplied component parts for improvised explosive devices to members and associates of the 1920 Revolution Brigades, an Iraqi insurgent group that has claimed responsibility for approximately 230 improvised explosive device attacks, 156 shelling attacks, and 82 sniper and small arms attacks targeting U.S. military personnel from 2005 to 2010.

440. In order to facilitate the preparation of timely and good quality requests for assistance, the DOJ-OIA has an internal non-public website through which most Federal LEAS and all Federal



prosecutors can access templates to prepare requests and an inventory of criminal assistance treaties, including multilateral treaties which the U.S. considers in force.

*Seeking other forms of international cooperation for AML/CFT purposes*

441. The U.S. authorities regularly seek other forms of international cooperation in an appropriate and timely manner for AML/CFT purposes. The U.S. maintains an extensive global network of liaison law enforcement attachés, DOJ attachés, and FinCEN attachés who seek international cooperation on behalf of the U.S. when needed. By placing attachés overseas, the U.S. is able to help and obtain help from foreign law enforcement counterparts in a more rapid, constructive, and effective manner.

**Box 32. The reach of the U.S. liaison network to facilitate international cooperation**

Federal Agency	Number countries covered
Drug Enforcement Agency (DEA)	86 offices in 67 countries
Department of Homeland Security/ICE/HSI	62 offices in 46 countries
Federal Bureau of Investigation (FBI)	60 offices covering over 200 countries
Internal Revenue Service – Criminal Investigations (IRS-CI)	Liaisons posted in 10 countries
DOJ currently stations nine Federal prosecutors as attachés in six countries covering 20 territories and the European Union.	

442. These liaisons focus on seeking assistance for the types of investigations and prosecutions that are consistent with the risk profile of the U.S. For example, DEA attachés focus their investigative efforts on DEA targets in support of domestic U.S. investigations and the IRS-CI attachés seek assistance from other countries to counteract tax schemes, ML, and the flow of narcotics and TF (see Chapter 1 for agencies' responsibilities).

443. One of the primary goals of the OCDETF Program is the development of multi-jurisdictional investigations that simultaneously target the geographically-dispersed components of major trafficking networks (see IO.7). OCDETF investigations are frequently international and involve TCOs. Currently, around 39% of OCDETF's investigations are being undertaken with active participation by, and coordination with, a foreign government. These investigations involve more than 100 different foreign LEAs.

**Box 33. Example of results achieved through other types of international cooperation**

The governments of the U.S. (through its DHS attachés' network) and Mexico (through its Secretaría de Hacienda y Crédito Público (SHCP) Unidad De Inteligencia Financiera (UIF)) prepared a bi-national study attempting to track the mechanisms used by criminals on both sides of the border to hide their ill-gotten gains, including, how money is transported, diverted into legitimate channels, or exchanged for goods and services. This study<sup>1</sup> has formed the basis for further investigations into these activities.

Note:

1. See *U.S.– Mexico Bi-National Criminal Proceeds Study*, 2010:

<https://www.dhs.gov/xlibrary/assets/cne-criminalproceedsstudy.pdf>

8

444. FinCEN plays a critical international collaboration role for the U.S., exchanging financial intelligence using the Egmont Group process and on the basis of bilateral and multilateral operational engagements, either on its own behalf or on behalf of its domestic partners. Since FY 2012, FinCEN has sent almost 500 requests per year (on average) to foreign FIUs from U.S. law enforcement and U.S. supervisory agencies. Starting in FY 2014, FinCEN began sending requests on its own. For FY 2015, FinCEN made 409 Egmont requests of its FIU partners on its own behalf or that of a U.S. law enforcement or regulatory agency and has made another 213 during the first half of FY 2016.

445. The following chart gives a breakdown of the outgoing requests by FinCEN in the past five years. Spontaneous disclosures sent by FinCEN dramatically increased last year (there were 45 in 2013, 17 in 2014, 779 in FY 2015, and 451 during the first half of FY 2016). This significant increase in spontaneous disclosures is due to the more proactive approach that FinCEN has been taking to operational and strategic analysis in the past couple of years (see IO.6), and which should be continued; and the significant increase in terrorist activity globally and the subsequent focus by the U.S. authorities on FTFs. For the same reasons, a greater proportion of the outgoing requests sent by FinCEN are being sent on its own behalf (rather than being sent on behalf of another LEA).

Table 26. **Egmont FIU Information Sharing Statistics – seeking/receiving information**

Description	2011	2012	2013	2014	2015
Outgoing requests sent by FinCEN	284	366	773	416	409

446. The U.S. National Central Bureau is the statutorily-designated representative to INTERPOL on behalf of the Attorney General. As such, it is the official U.S. point of contact in INTERPOL's world-wide, police to police communications and criminal intelligence network. INTERPOL Washington includes analysts and agents detailed from DOJ, DHS, Treasury, and many other agencies.

*Providing other forms international cooperation for AML/CFT purposes*

447. The U.S. can provide many forms of assistance before receiving a request for MLA through its network of attachés posted abroad (as described above). In the feedback from FATF and FSRB delegations, this network was generally praised for facilitating requests for assistance from foreign authorities, although it was noted that not all these agencies provide equal levels of service.

448. The U.S. can assist other countries in the investigation and prosecution of ML, TF and predicate offenses through a variety of means. Requests for ordinary investigative assistance and information sharing are usually made by foreign police authorities directly to the relevant liaison officers/attachés who pass the request for assistance to their appropriate regional office or headquarters in the U.S. for execution. The U.S. LEAs also play a proactive role sharing information spontaneously with their counterparts.

449. With respect to asset restraint, seizure, and forfeiture, DOJ-OIA works closely with AFMLS as well as its network of asset forfeiture experts in the USAOs located throughout the U.S., to provide a wide range of assistance. Assistance in tracing and identifying assets often unfolds via police-to-police communication, by or with the assistance of law enforcement and DOJ attachés (see previous section).

450. Outside these bilateral channels, the U.S. also exchanges certain law enforcement information through international and multilateral networks e.g. the Camden Inter-agency Asset Recovery Network (CARIN) network used for informal inquiries relating to the identification and tracing of the proceeds and instrumentalities of crime. On average, the U.S. successfully processes about 100 to 150 incoming CARIN requests for assistance per year.

451. Within the last three years, the DOJ used confiscated proceeds of crime to fund INTERPOL's Washington Asset Forfeiture Program (USNCB-AFP) which supports domestic confiscation investigations, and assists in the identification of assets within the U.S. pursuant to requests from foreign INTERPOL National Central Bureaus. In the last two years, inquiries for recoverable assets have resulted in locating 27 fugitives from U.S. justice as well as about 30 asset recovery leads.

452. As outlined above, FinCEN exchanges financial intelligence using the Egmont Group process and Egmont Secure Web (ESW) system and enters into bilateral and multilateral operational engagements. MOUs or exchange of letters are not required for FinCEN to engage in bilateral or multilateral information sharing with FIUs. Prior to 2012, FinCEN sought MOUs with FIUs as a matter of policy. Since then, FinCEN negotiates MOUs if the foreign FIU requires one to exchange information or if the FIU is not a member of the Egmont Group. FinCEN has either an MOU or an exchange of letters in place with the FIUs of a number of jurisdictions to facilitate the exchange of information and is negotiating others.

Table 27. **Egmont FIU Information Sharing Statistics**

Description	2011	2012	2013	2014	2015
Incoming requests received by FinCEN	728	772	765	845	1 021
Incoming spontaneous disclosures received by FinCEN	291	327	316	526	914
Outgoing spontaneous disclosures sent by FinCEN	58	57	45	17	779

453. FinCEN is the most requested FIU for information in the world, supporting requests from an average of 100 FIUs each year, or from approximately 75% of all FIUs with which it maintains a relationship. FinCEN shares the results of its analysis both spontaneously and upon request and, since 2012, has received an average of 871 requests from foreign FIUs for financial intelligence annually (see Table 27).

454. A special section within FinCEN's Liaison Division processes all incoming and outgoing case requests for assistance to FIUs and domestic law enforcement. FinCEN makes every attempt to meet partner FIU requesters' deadlines in providing responses, particularly those involving priority violations, but response times are often dictated by the type and amount of information found during research.

#### Box 34. Example of FinCEN Engagement to Facilitate Clearer FIU Requests

**FIU A:** FinCEN determined that FIU A had submitted several requests for information to assist enforcement in country B in half a dozen tactical cases. The requests lacked identifiers and had no clear U.S. nexus, making it difficult for FinCEN to process. Instead of rejecting the requests or delaying responses indefinitely, the FinCEN Egmont request processing team contacted the OGL for assistance. The OGL Specialist coordinated with FIU A, and FIU A involved the U.S. DOJ Resident Legal Advisor, who had been providing technical assistance related to a law enforcement case to FIU A. All relevant authorities collaborated to provide FinCEN the missing identifiers so the case requests could be processed. As a result, FIU A modified and re-submitted its requests to incorporate this feedback which then allowed FinCEN to process requests in a timely manner.

455. Below are illustrative examples of assistance FinCEN provides to foreign counterparts:

#### Box 35. Examples of Intelligence Provided to Case Requests

**FIU A:** FinCEN responded to a request from FIU B concerning an individual suspected of facilitating travel of non-U.S. citizens to the U.S. to open bank accounts to launder illicit funds. FIU B indicated that the suspect, who was associated with two travel companies, had been to the U.S. to open to accounts to potentially launder millions in funds. FinCEN reported that SARs were filed by U.S. banks over a two-year period concerning over USD 500 000 in fraudulent credit/debit card activity in the U.S. The fraud was identified with an individual using a known alias for the request suspect as well as a matching business name.

**FIU B:** FinCEN responded to a request from FIU C regarding two individuals, who are among 25 individuals under U.S. federal indictment as owners of a sports betting Internet website operating illegally in multiple U.S. states that profited more than USD 50 million during an 18-month period by accepting wagers on various sporting events—including horse-racing and professional and college football, basketball, hockey, and baseball. FIU C indicated the subjects of the request intended to liquidate some or all of their ownership in a European holding company. FinCEN reported that both suspects were cited in multiple SAR and SAR by Securities and Futures Industries (SAR-SF) filings involved millions in suspicious wire transfer and checking activity in 2014. Additionally, multiple

International Reports of the transportation of CMIRs, CTRs, CTR-filed by Casinos, and FBAR filings were found regarding the subject of the request within the past few years. International cooperation also takes place at the supervisory level. FinCEN signed its first MOU for AML/CFT supervisory purposes with a Mexican supervisory agency in 2013, and similar MOU with a Canadian AML/CFT supervisory agency in 2015. The MOUs provide for strict controls and safeguards to ensure that shared information is well protected and used in a confidential and authorized manner for AML/CFT supervision purposes only. The OCC, the FDIC, and the BGFERS have together entered into a significant number of information-sharing arrangements with foreign supervisors.

#### Box 36. International Supervisory Cooperation – Illustrative Data

- From 18 January 2014 through 10 August 2015, FinCEN has processed eight supervisory requests (five requests received and three requests sent).
- Since 2006, 24 MOUs or statements of cooperation have been entered by OCC/FDIC/FRS. This is in addition to making or responding to ad hoc requests for confidential information.
- SEC-OIA is handling an increased volume of requests in cross-border supervisory cooperation matters, cross-border examinations, asset verifications and registrations. During FY 2014, the SEC received 548 requests for international enforcement assistance<sup>1</sup>, 117 requests for supervisory assistance<sup>2</sup> from foreign authorities, and opened 30 investigations to assist the SEC's foreign counterparts.<sup>3</sup> Additionally, the SEC has benefited from "spontaneous referrals" made by foreign FIUs.
- The CFTC is handling an increased number of requests for cross-border cooperation and actively seeks cooperation from foreign authorities as well. In FY 2015, the CFTC received 38 requests for international enforcement assistance while sending 235 requests for enforcement assistance to foreign authorities.

#### Notes:

1. FY 2014 Agency Financial Report, at 26, available at [www.sec.gov/about/secpar/secafr2014.pdf](http://www.sec.gov/about/secpar/secafr2014.pdf)
2. FY 2014 Annual Performance Report; FY 2016 Annual Performance Plan, at p.30.
3. FY 2014 Agency Financial Report, at p.27.

456. The U.S. has also established a number of specific initiatives with strategically important partners such as with Mexico (strategically important because of the threat from drug trafficking through Mexico by transnational organized crime groups) and the U.K. (strategically important as a global financial center) to facilitate international cooperation on illicit finance matters:

- a) The ***Bilateral Illicit Finance Working Group (BIFWG)*** with Mexico to advance bilateral illicit finance cooperation by increasing coordination between agencies and identifying new trends and vulnerabilities being exploited by TCOs.

- b) The ***U.S.-Mexico Public Private Bilateral Banking Group*** that brings together policymakers, regulators and private sector representatives from both countries to identify illicit finance priorities and develop strategies to tackle the threat.
- c) The ***Recovery of Criminal Assets Taskforce (RoCAT)*** with the U.K. Crown Prosecution Service to coordinate confiscation and ML business. RoCAT holds quarterly video-conferences between the attorneys and investigators executing requests and the attorneys and investigators seeking the requested assistance, thereby expediting bilateral cooperation and resolving confiscation matters. International exchange of basic and beneficial ownership information of legal persons and arrangements.

457. As noted above, the U.S. is an attractive destination for company formation, and there are a very large number of legal persons incorporated in the country. In this context, it is not surprising that the U.S. receives a relatively large number of requests for legal and BO information about domestically incorporated companies. For example, most of the 100 to 150 CARIN requests executed by the U.S. each year involve requests to obtain BO information.

458. The U.S. has demonstrated some success in this area, though significant barriers exist (see IO.5). Some registries may also identify incorporators, officers, registered agents or other individuals who can provide investigative leads to the actual BO information. Requesting countries often search these online registries for their investigations. In case these registries do not provide necessary information, a foreign country can seek BO information from the U.S. on a police-to-police basis or through formal channels.

459. Lawyers often play a role in company formation where complex corporate structures are being established. In practice, lawyers may collect BO on their clients for their own business purposes which could, in theory, be accessed by the competent authorities through issuing a subpoena. However high-level approvals may be required from DOJ to issue a subpoena to lawyers when the U.S. is providing international assistance to another country. In the U.S., the attorney-client privilege protects from disclosure the confidential communications between attorney and client made for the purpose of furnishing or obtaining legal advice or assistance though this can be overcome i) where it can be shown that the attorney in question was actively participating in the criminal activities of his client; ii) where an attorney acts as a nominee shareholder, trustee, settlor, a company director, or under a power of attorney to represent a company, the disclosure of information resulting from, and in relation to, such activity, cannot be declined iii) where advice is sought from an attorney but it is not legal advice.

460. The IRS also collects some information in respect of both companies and trusts. However, this information cannot be shared through an MLA procedure if the request is based on a ML offense for which the predicate offense is tax evasion or tax fraud. Moreover, as a general rule, the U.S. cannot disclose to foreign government officials tax information obtained by officers or employees of a Federal agency pursuant to a court order (26 USC §6103(i)), except for tax administration purposes pursuant to a treaty, convention, or information exchange agreement( 26 USC §6103(k)(4)).

461. In this environment, the only recourse is for the LEAs to use time consuming and resource intensive investigative methods (see R.31 and IO.5). Some of these investigative means are very overt (e.g. witness statements) and would be impractical in covert cases. This has two implications



for international cooperation. First, the U.S. authorities are unlikely to undertake a resource-intensive investigation to uncover BO information on behalf of a foreign counterpart unless the case is of a significantly high priority (e.g. involving terrorism or a very large volume of proceeds). Second, even where the U.S. applies the resources, such information cannot always be provided in a timely way. The authorities acknowledged that, in fact, investigative processes can sometimes take many months.

462. In significant investigations, FinCEN has a range of tools available to it, including the ability to query the U.S. financial system (22 000 FIs) for accounts or transactions of specified individuals, entities, and organizations engaged in, or reasonably suspected of engaging in, terrorist acts or ML activity (see Section 314(a) of the Patriot Act process in R.29 and IO.6). FinCEN may resort to this on behalf of foreign law enforcement though it can be used in limited circumstances only (see R.29 & IO.6).

463. SEC staff assists foreign regulators to obtain information identifying persons who beneficially own or control legal persons organized in the United States. SEC staff provides such assistance through public records, including SEC reporting and filings by companies that register offerings or file periodic reports with the Commission, as well as registration applications and amended filings by SEC-registered entities such as broker-dealers and investment advisers,<sup>53</sup> through SEC nonpublic supervisory information,<sup>54</sup> and by obtaining the information through its authority to conduct an investigation on behalf of a foreign authority under Section 21(a)(2) of the Exchange Act.<sup>55</sup> The IOSCO MMOU and a number of bilateral information-sharing arrangements for enforcement cooperation specifically provide for assistance in obtaining information and records related to beneficial ownership.<sup>56</sup> Further, many of the SEC's supervisory MOUs provide broadly for the sharing of supervisory information, which would enable the SEC to share beneficial ownership information obtained through examinations of the financial institutions it regulates. The SEC shares information about BO in accordance with these arrangements with foreign authorities for information-sharing and confidentiality and pursuant to its authority under section 24(c)(1) of the *Exchange Act*. Further, many of the CFTC's supervisory MOUs provide broadly for the sharing of supervisory information, which would enable the CFTC to share beneficial ownership information obtained through examinations of the FIs it regulates. The CFTC shares information about BO, on a confidential basis, in accordance with both formal and informal arrangements with foreign authorities and pursuant to its authority under section 8(e) of the *Commodity Exchange Act*.

**464. The U.S. is rated as having achieved a substantial level of effectiveness for IO.2**

<sup>53</sup> See SEC Self-Assessment, at 237 (SEC sharing BO information), 163-164 (public sources), SEC Form ADVs filed by investment advisers, Schedules A and B (for control information).

<sup>54</sup> See SEC Self-Assessment, 221, 235 (SEC supervisory info).

<sup>55</sup> SEC Self-Assessment at 218 referencing power to obtain info identified in Question 13.3(a)-(g) (of which BO & control information is (e)).

<sup>56</sup> IOSCO MMOU, paragraph 7(b)(ii).

## TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2006 available at the following link.

### ***Recommendation 1 - Assessing Risks and applying a Risk-Based Approach***

This is a new Recommendation which was not assessed in the 3rd MER.

*Criterion 1.1* - The U.S. maintains a substantial number of complementary processes to identify and assess ML/TF risks which generate a wide variety of outputs. Risk assessments to support the President's national security strategies are prepared by relevant government agencies with participation from intelligence, law enforcement, and policy agencies involved in AML/CFT, including FinCEN which contributes ML/TF risks and trends identified from the reporting regime. To an extent, these risk assessments rely on non-public information and though not provided to the assessors, were extensively discussed during on-site. The Federal LEAs with principal investigative authority over financial crimes conduct their own identification and analysis of the ML/TF risks associated with the predicate crimes within their areas of responsibility. Most recently, in 2015, the U.S. published two consolidated national risk assessments (NMLRA and NTFRA) (see Chapter 1, *Country's risk assessment*).

*Criterion 1.2* - The risk assessments underlying the national security strategies are coordinated by the NSC staff and approved by the NSC. The *2015 National Security Strategy* identifies priority threats and policies including preventing the "global financial system from being abused by transnational criminal and terrorist organizations that engage in or launder the proceeds of illegal activity." The ONDCP has a predominantly AML focus related to the *National Drug Control Strategy* and related strategies. Separately, relevant government agencies prepare agency-specific reports and assessments that complement and support these strategies.

*Criterion 1.3* - The U.S. updates its risk assessments: annually or bi-annually for the national security strategies targeting narcotics trafficking<sup>57</sup> and the program to combat healthcare fraud; and as necessary for the other relevant national security strategies. Multi-agency NSC working groups assess national security strategy implementation and discuss emerging new threats and related ML/TF risks and their policy implications. The inputs for this process come from the U.S. intelligence, law enforcement and supervisory communities, drawing from ongoing investigations. There is no regular schedule planned for the updating of the NMLRA and the NTFRA, although in the broader context risk assessment is a continuous process.

<sup>57</sup> *National Drug Control Strategy, National Southwest Border Counter Narcotics Strategy and National Northern Border Counter Narcotics Strategy.*

*Criterion 1.4* - The NMLRA and NTFRA make the large volume of risk information generated by U.S. government agencies more easily accessible to the public and private sectors (see Chapter 1, *Country's risk assessment*). The U.S. confirms these are accurate “point in time” summaries of all underlying risk assessment work described above. The risk assessments underlying the President's national security strategies are classified and available to Federal government agencies engaged in protecting national security. The Director of National Intelligence and the Director of NCTC provide annual unclassified threat assessments to the U.S. Congress.

*Criterion 1.5* - Based on their understanding of the threats and vulnerabilities, and in keeping with their mandates, the authorities apply a risk-based approach (RBA) to allocating resources. Budget submissions and reports from key Federal agencies<sup>58</sup> indicate that funds are being allocated to support identified AML/CFT priorities, including the targeting of third party ML networks. The supervisory approach is broadly satisfactory for the financial sector with FinCEN, the FBAs, the SEC, other federal financial regulators, the IRS-SBSE and State authorities all playing their respective role in supervision. The collection of large cash transaction data from U.S. businesses and professions via the Form 8300 process is managed by FinCEN and IRS (which requires all nonfinancial trades and businesses, including DNFBPs (except casinos), to report cash received in one or more related transactions in amounts over USD 10 000). Certain financial institutions and casinos have a similar cash reporting requirement, referred to as a Currency Transaction Report. However, comprehensive AML/CFT preventive measures have not been directly applied to deter the abuse of investment advisers (only some are indirectly covered), lawyers, accountants, trustees, real estate agents and company formation agents (CFAs) (see the NMLRA, NTFRA, and published risk information from FinCEN).

*Criterion 1.6* - Aspects of the FATF Recommendations are not applied to certain transactions and/or accounts and most DNFBPs. The most notable of these are: (1) lack of measures addressing BO in BSA CDD obligations; and (2) investment advisers, lawyers, accountants, real estate agents, trustees and CFAs are not subject to comprehensive AML/CFT measures (they are only subject to the Form 8300 requirements and TFS obligations). The U.S. attributes the low (residual) risk in the minimally covered sectors to complementary regulatory safeguards and/or market-based practices that reduce the ML/TF risk in normal transactions and customer relationships. In some limited instances these can tend to limit vulnerability (e.g. some investment advisers are indirectly covered, if they are part of a financial group or are subsidiaries of banks/bank holding companies or are acting for a financial institution in the framework of an outsourcing arrangement). The U.S. also asserts that ML/TF activity through the minimally covered sectors is generally due to deficient compliance with existing safeguards or criminal complicity on the part of the service provider, rather than the customer taking advantage of inadequate regulations. However, these factors do not prove low ML/TF risk as the lack of preventive measures means that negligent/unwitting facilitation of ML/TF through these sectors is less likely to be detected. The assessors attribute compliance costs and burden on the private sector as the more heavily weighted factors influencing these exemptions and thresholds (notably the SAR reporting thresholds and the exemption of real estate agents from BSA obligations), rather than a proven low risk of ML/TF, as required by the *FATF Recommendations*. For example the

<sup>58</sup> 2015 DEA budget, 2015 FBI budget, 2015 DHS Budget for ICE and USSS, 2015 IRS Budget, *DHS Congressional Budget Justification FY 2015*, and the *TEOAF Forfeiture Fund Accountability Report for fiscal year 2013*.

U.S. confirmed in its technical compliance (TC) response that SAR reporting thresholds were intended to “reduce the burden of reporting and to confirm the treatment of ML and related transactions to that of other situations in which reporting is required by the Supervisory Agencies”.<sup>59</sup>

*Criterion 1.7* - The U.S. has enacted legislation directed at FIs and some DNFBPs to address some threats categorized in the NMLRA as higher risks. Public corruption is partially addressed by the requirements aimed at foreign PEPs (although this only applies in the Covered FI sector). The misuse of banking products and services is partially addressed through systemic measures directed at private banking and correspondent banking. The widespread use of cash is addressed more broadly by the IRS Form 8300 reporting requirements. However, some other key vulnerabilities in the NMLRA<sup>60</sup> are either not addressed or are only addressed by indirect measures. For example, the NMLRA identifies cash transaction structuring as a vulnerability, notwithstanding that attempts to structure are seen as useful flags for LEAs.

*Criterion 1.8* - The U.S. does not explicitly allow for simplified measures. For CDD and account monitoring, the regulations set baseline customer identification requirements with which Covered FIs and DNFBPs must comply regardless of the risks presented by their customers, products, services, etc. The baseline requirement must always be met, and cannot be simplified.

*Criterion 1.9* - Covered FIs/DNFBPs are supervised for compliance with the requirements of criteria 1.10 to 1.12, as described in R.26 and R.28. However, all investment advisers, lawyers, accountants, real estate agents, trustees and CFAs are not subject to obligations under R.1.

*Criterion 1.10* - Covered FIs/DNFBPs are required to develop a BSA/AML risk assessment. However, some FIs, all investment advisers, lawyers, accountants, real estate agents, trustees and CFAs are not covered. The FFIEC Manual which applies to the banking sector expects that the risk assessment must take into consideration all relevant factors (e.g. products, services, customers, geographic locations and correspondent relationships):<sup>61</sup>

- a) According to the FFIEC Manual, it is “a sound practice that the risk assessment be reduced to writing” (p.18). Other sectors (except the life insurance sector) are required to have written risk assessments.
- b) FinCEN and other competent authorities provide information on relevant risk factors that FIs should take into account when determining the level of risk (see criteria 1.4 above).

<sup>59</sup> 61 Fed. Reg. 4326, 4328 (Feb. 5, 1996).

<sup>60</sup> Structuring resulting from thresholds, disguise (hidden actors using fronts), compliance deficiencies, complicit violators in FIs, and complicit merchants and financial services providers.

<sup>61</sup> **Banks and credit unions:** 31 CFR §1020.210 (FinCEN), 12 CFR §21.21 (OCC), 12 CFR §208.63 (Federal Reserve), 12 CFR §326.8 (FDIC), 21 CFR §748.2 (NCUA). **Brokers or dealers in securities:** 31 CFR §1023.210 (FinCEN), Rule 3310 (FINRA). **Casinos and card clubs:** 31 CFR §1021.210. **Dealers in precious metals and stones:** 31 CFR §1027.210. **FCMs and IBs:** 31 CFR §1026.210 (FinCEN), Rule 2-9 (National Futures Association). **Insurance companies:** 31 CFR §1025.210. **MSBs:** 31 CFR §1022.210. **Mutual funds:** 31 CFR §1024.210. **Operators of credit card systems:** 31 CFR §1028.210. **RMLOs:** 31 CFR §1029.210.

- c) Covered FIs and DNFBPs are required to keep their risk assessments up to date, but other sectors are not subject to such a requirement.
- d) All covered FIs/DNFBPs sectors are required to make their risk assessments available to supervisors and various other competent authorities.

*Criterion 1.11* - Covered FIs/DNFBPs are required to have policies, controls and procedures that are approved by senior management and which enable them to manage and mitigate the ML/TF risks identified by their risk assessment. Some specific higher risks are identified by the U.S. in legislation or enforceable means: c.1.7. Covered FIs/DNFBPs are required to conduct an independent audit to test their program and have an ongoing employee training program. Reporting entities are required to implement internal controls, policies and procedures which are adequate to mitigate their ML/TF risks<sup>62</sup>. Not all investment advisers are covered. For DNFBPs (other than casinos and dealers in precious metals and stones), no comprehensive AML/CFT obligations apply.

*Criterion 1.12* - The U.S. does not explicitly allow for simplified measures: c.1.8.

### *Weighting and Conclusion:*

The U.S. has a strong risk assessment process involving well-coordinated LEAs and multiple competent authorities. However, the authorities' collective good understanding of the threats faced by the U.S. is not being sufficiently translated into effective mitigation measures against vulnerabilities of the high-end real estate agents, lawyers, accountants, trustees and CFAs (often cited as vulnerable to abuse by criminal elements and shown to be so by the NMLRA) as these are not covered for AML/CFT obligations, other than limited Form 8300 and targeted financial sanctions obligations.

***Recommendation 1 is rated partially compliant.***

### ***Recommendation 2 - National Cooperation and Coordination***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The deficiency related to effectiveness which is not assessed as part of technical compliance under the 2013 Methodology.

*Criterion 2.1* - The U.S. has a range of national AML/CFT policies that are informed by the risks identified, and regularly reviewed and updated as described in c.1.4 including: the President's *National Security Strategy*, *National Drug Control Strategy*, *Strategy to Combat Transnational Organized Crime*; *National Strategy for Counterterrorism*; *DOJ Strategic Plan* which sets out Federal law enforcement strategies for pursuing priorities including ML/TF; and *FinCEN's 2014-2018 Strategic Plan* which addresses FinCEN's role as both the FIU and the primary AML regulator.

*Criterion 2.2* - The NSC coordinates the development of national security strategies which include AML/CFT initiatives. The Office of TFFC chairs the AML Task Force which is an ongoing inter-agency group convened in November 2012 to review the U.S. AML framework, identify priority AML/CFT regulatory and enforcement issues, consider where improvements are needed, and implement the necessary legal and operational changes. The DOJ coordinates the application of LEAs in pursuing

<sup>62</sup> 31 USC §5318(h), regulations listed in footnote 61.

priority criminal threats, including ML/TF threats. The ONDCP, like the NSC staff, is part of the Executive Office of the President. The ONDCP is responsible for developing the *National Drug Control Strategy*, the consolidated National Drug Control Budget, and the annual drug control strategy specific to the U.S. southwest and northern borders: *ONDCP Reauthorization Act of 2006*.

*Criterion 2.3* - The U.S. has numerous mechanisms in place, at both the policy and operational levels, to enable policy makers, the FIU, LEAs, supervisors and other relevant competent authorities to cooperate and, where appropriate, coordinate domestically on the development and implementation of AML/CFT policies and activities. Inter-agency groups and task forces facilitate such cooperation and coordination, and are described in detail under Chapter 1 (*Legal and institutional Framework*) and Chapter 2 (*National coordination and cooperation*).

*Criterion 2.4* - The U.S. has a number of inter-agency forums to coordinate policy making and operational efforts to combat the financing of proliferation of weapons of mass destruction (WMD). A description and role of these agencies and task forces is provided under Chapter 1 (*Legal and institutional Framework*) and Chapter 2 (*National coordination and cooperation*).

#### *Weighing and Conclusion:*

All four criteria are met.

***Recommendation 2 is rated compliant.***

#### ***Recommendation 3 - Money laundering offense***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies were: the list of domestic predicate and foreign ML offenses did not fully cover the designated categories of offenses; mere possession and concealment of proceeds did not constitute ML; and the definition of *property* for the cross border ML offense only included monetary instruments or funds.

*Criterion 3.1* - The U.S. has four Federal offenses which criminalise ML broadly in line with the Vienna and Palermo Conventions:

- a) **“Basic offense”**: conducting or attempting to conduct a financial transaction with property knowing that it is the proceeds of a felony under State, Federal or foreign law, and which in fact involves the proceeds of “Specified Unlawful Activity” (SUA), with the intent to: i) promote carrying out an SUA; ii) commit tax evasion; or knowing the transaction is designed in whole or in part to iii) conceal/disguise the nature, location, source, ownership or control of the proceeds; or iv) avoid a transaction reporting requirement: 18USC§1956(a)(1).
- b) **“International offense”**: transporting, transmitting or transferring monetary instruments or funds out of/into the U.S.: i) with the intent to promote carrying out an SUA regardless of whether or not the monetary instruments/funds constitute criminal proceeds; or ii) knowingly transporting, transmitting, or transferring a monetary instrument/funds constituting the proceeds of some form of unlawful activity with the specific intent to conceal/disguise aspects of the proceeds of an SUA or avoid a transaction reporting requirement under State/Federal law: 18 USC §1956 (a)(2)(A) & (B).



- c) “Undercover sting offense”: conducting a financial transaction with property represented to be the proceeds of an SUA by an undercover law enforcement official or someone acting under his/her direction and with a similar intent as those set out in §1956(a)(1): §1956(a)(3).
- d) “Transactional offense”: knowingly engaging or attempting to engage in a “monetary transaction” (transaction through a FI) in criminally derived property of over USD 10 000: §1957.

The Federal ML offenses apply if: 1) there is even a *de minimis* connection<sup>63</sup> to “inter-state commerce” (a requirement necessary to establish Federal jurisdiction); and 2) the activity constitutes a *financial transaction*<sup>64</sup> (18 USC 1956 offenses) or *monetary transaction* (18 USC 1957 offense). Mere possession is not criminalised because the ML act is not distinct from the predicate crime. ML is not charged in relation to mere acquisition of proceeds of crime through commission of the predicate offense although mere receipt by a third party, with requisite knowledge, may be sufficient to attract liability for ML: U.S. v. Gotti, 459 F.3d 296, 335 (2d Cir. 2006).

*Criterion 3.2* - All but one of the 21 designated categories of predicate offenses are covered. Predicate offenses are defined in a statutory list of SUA covering approximately 250 serious offenses: §1956(c)(7)(A)-(F). Tax crimes are not SUAs although the laundering of proceeds of another predicate offense with the intent to evade taxes is considered a crime: §1956(a)(1)(A)(ii) and *United States v. Zanghi*, 189 F.3d 71, 81 (1st Cir. 1999) and the U.S. relies on mail and wire fraud to capture instances of tax fraud - when appropriate.

*Criterion 3.3* - The U.S. does not apply a threshold approach domestically.

*Criterion 3.4* - The basic and undercover sting offenses cover any type of property, regardless of value, that directly or indirectly represents the proceeds of a SUA: 18 USC §§1956(a)(1), (2), and (3). The international offense covers these aspects but only in relation to “funds” or “monetary instruments” § 1956(a)(2). The transactional offense only applies where the value of the laundered property exceeds USD 10 000: §1957. Gaps under the transactional and international offenses are deemed minor since the basic offense will apply when the transmission or transfer of proceeds qualifies as a *transaction*.

*Criterion 3.5* - When proving that property is the proceeds of crime, it is not necessary that a person be convicted of a predicate offense: 18 USC §§1956 & 1957.

<sup>63</sup> The “inter-state commerce” requirement has been broadly interpreted by the courts to include cases involving: use of interstate transportation (e.g. highways), telephones or the mail; any drug offence; theft from companies purchasing goods interstate in the normal course of their business; ML involving goods partially manufactured interstate (e.g. jewelry, diamonds), etc.

<sup>64</sup> The term “financial transaction” covers a very broad range of conduct and is defined in §1956(c)(4) as “(A) a transaction which in any way or degree affects interstate or foreign commerce involving (i) the movement of funds by wire or other means or (ii) one or more monetary instruments, or (iii) the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree.” A *transaction* is understood to include the sale, purchase, lease, pledge, gift, transfer, or other disposition (deposit, withdrawal, transfer between account, exchange of currency, loan, extension of credit, using a safe deposit box or purchasing/selling monetary instruments). Any disposition of the receipt of proceeds, any handing over in the care of, including mere receipt by a third party, with requisite knowledge, may be sufficient to attract liability for ML.

*Criterion 3.6* - Twelve designated categories are specifically included as foreign predicate offenses: §1956(c)(7)(B)(i)-(vii). The remaining 9 categories are not listed individually in this sub-section: 1) participating in an organized criminal group and racketeering; 2) illicit trafficking in stolen and other goods; 3) fraud (when it is not by/against a foreign bank); 4) counterfeiting currency; 5) counterfeiting and piracy of products; 6) environmental crime; 7) forgery; 8) insider trading and market manipulation; and 9) tax crimes. The gap is largely mitigated as: (i) the definition of SUA includes crimes arising under foreign law<sup>65</sup>; (ii) section 1956(c)(7)(B)(vi) can capture any foreign predicate, so long as the crime abroad is transnational in nature and involves an organized criminal group (three or more persons) set up to commit a serious offense, as defined by the Palermo Convention;<sup>66</sup> and (iii) in circumstances where the non-listed foreign predicates are not captured by §1956(c)(7)(B)(vi), the U.S. is able to use certain domestic predicates for ML which apply extraterritorially. The U.S. provided assessors with case law in which domestic predicates served to capture foreign conduct, thus permitting a money laundering charge in the U.S. for the nine non-listed offenses. This means any one of the approximately 250 violations encompassed in §1956(c)(7) might be domestic predicate offenses for ML in some circumstances, and have been interpreted by Federal courts to apply extraterritorially in some instances.<sup>67</sup>

*Criterion 3.7* - Self-laundering is criminalised: 18 USC §§1956 & 1957.

*Criterion 3.8* - For the three ML offenses under 18 USC §1956, proof of knowledge and the intention can be inferred from direct, indirect or objective factual evidences. All elements of the ML offense must be proved beyond reasonable doubt. For the transactional offense, proof of criminal intent is not necessary. The only proof needed is that the defendant knowingly engaged in the monetary transaction and knew the property involved in that transaction was criminally derived from activity constituting a felony under State, Federal or foreign law.

*Criterion 3.9* - Proportionate and dissuasive criminal sanctions apply to natural persons convicted of ML. A criminal fine of up to USD 500 000 or twice the value of the property involved in the transaction (whichever is greater), or imprisonment for up to 20 years, or both apply for the basic, international,

<sup>65</sup> Additionally, the money laundering statutes, by virtue of 18 USC §1956(f), apply extraterritorially, provided that “the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and the transaction or series of related transactions involves funds or monetary instruments of a value exceeding USD 10 000.” Thus, a U.S. citizen can be charged with ML that occurs exclusively abroad. Further, § 1956 applies to “foreign persons” who commit offenses involving transactions, property, or institutions with certain specified connections to the U.S. *Id.* §1956(b)(2), (f). Additionally, §1957 imposes criminal liability on “United States person[s]” who engage in prohibited transactions “outside of the United States.” *Id.* §1957(d)(2).

<sup>66</sup> § 1956(c)(7)(B)(vi)’s reference to “an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States,” has been interpreted by case law, to capture any foreign predicate, so long as the crime abroad is considered serious, transnational, and organized in nature, as defined by the Palermo Convention. *United States v. Real Property Located at 9144 Burnett Road, SE, Yelm, Washington*, 104 F. Supp. 3d 1187 (W.D. Wash. 2015). Section 1956(c)(7)(B)(vi) includes participating in an organized criminal group and tax evasion, per case law, but could also include any of the other 7 foreign predicates not listed individually in §1956(c)(7)(B)(i)-(vii). The judicial precedent that permits the U.S. this flexibility is new since its 2006 MER, and U.S. authorities can seek to rely on it in all judicial districts as needed, but it is not binding.

<sup>67</sup> This is in addition to the offenses against foreign nations specifically listed in 18 USC §1956(c)(7)(B)(i)-(vii).

undercover sting, and conspiracy offenses: 18 USC §1956(a)(1)-(3). A criminal fine of up to USD 250 000 (for a natural person) or USD 500 000 (for a legal person), or twice the amount of the criminally derived property involved in the transaction (whichever is greater), or imprisonment for up to 10 years, or both apply for the transactional offense: 18 USC §1957. Higher fines may be applied in cases of egregious conduct. All ML offenses are also punishable by civil fines of up to USD 10 000 or the value of the property involved in the transaction (whichever is greater): § 1956(b). Any officer, director or employee of a FI found guilty of a ML offense should also be the subject of a written notice to the relevant regulatory agency: §1956(g). Natural persons may be sanctioned as *principals* to the offense or *accessories after the fact*: 18 USC §§2 & 3.

*Criterion 3.10* - Criminal liability and proportionate, dissuasive sanctions for ML apply to legal persons, and are without prejudice to the criminal liability of natural persons: 1 USC § 1. Legal persons are punishable by the same criminal and civil fines described in c. 3.9. Any FI found guilty of a ML offense should be the subject of a written notice to the relevant regulatory agency and may subsequently face the revocation of its licence: USC §1956(g).

*Criterion 3.11* - There are ancillary offenses to all of the ML offenses: §1956(h), §1956(a)(1)-(3) and 1957(a), including conspiracy and attempt. Anyone found aiding and abetting, counselling, commanding, inducing, procuring, or wilfully causing a ML offense can be prosecuted and punished as a principal: 18 USC §2.

### *Weighting and Conclusion:*

Criterion 3.1 shortcomings are minor as the Federal ML offenses cover all but an extremely limited number of circumstances. That gap is also narrowed to some extent by the 36 States which have enacted State-level ML offenses (all of which apply regardless of any connection to “inter-state commerce”). Shortcomings under c.3.2 and c. 3.6 are also considered minor: while tax crimes are not specifically listed as predicate, other predicates in effect criminalise a range of tax fraud and even though 9 designated categories of predicate are not specifically listed as foreign SUAs, a broad range of foreign conduct is captured by other means including domestic SUAs applying extra-territorially.

***Recommendation 3 is rated largely compliant.***

### ***Recommendation 4 - Confiscation and provisional measures***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies were: the inability to seize/restraint property of equivalent value which may be subject to **confiscation**; and proceeds derived from offenses which are not required predicate offenses cannot be frozen/seized/confiscated based on a ML offense.

*Criterion 4.1* - The U.S. has three mechanisms enabling confiscation: i) criminal (in personam) confiscation applies to, among other things, any property held by a defendant convicted of an ML offense which was involved in the ML offense or traceable to it<sup>68</sup>; ii) civil judicial non-conviction-based forfeiture (NCBF) (i.e., civil forfeiture) (in rem) procedures may be used to forfeit any

<sup>68</sup> 18 USC §982(a)(1) and §981(a)(1)(G) apply to all assets of terrorists, including those convicted of TF.

property linked to a crime which is held by the defendant or a third party (§981); and iii) administrative forfeiture (in rem) permits a Federal seizing agency to forfeit property held by the defendant or a third party, as long as such seizure is not contested<sup>69</sup>. Property is also subject to criminal confiscation in all cases where civil forfeiture is available: 28 USC §2461(c). Over 220 separate Federal offenses give rise to confiscation in the context of predicates and non-predicate crimes. For ML offenses and crimes constituting ML predicate offenses, the following types of property (including that which is “clean”, commingled, appreciated in value, income or earned interest) may be confiscated:

- a) any property involved in a transaction or attempted transaction in violation of a ML offense (even if the offense was not completed): 18 USC §982(a)(1) (criminal confiscation), 18 USC §981(a)(1)(A) (NCBF)
- b) property other than SUA proceeds, which is also part of the *corpus* of the ML offense
- c) proceeds of predicate offenses, including income/other benefits derived from such proceeds: 18 USC §981(a)(1)(C)-(F) and 18 USC §982(a)(2)-(8) [(a)(1)(A) of the former and (a)(1) of the latter are broader than proceeds but could technically include proceeds]
- d) instrumentalities (i.e., any property *involved* in the ML offense or used to commit the SUA offense): 18 USC §982(a)(1); 18 USC §981(a)(1)(A). It can be deduced from the very broad notion of *involved in* that instrumentalities used or intended for use in the commission of a ML offense are also subject to confiscation. Separately, many predicate offenses, in the statutes in which they are criminalized, contain provisions permitting the forfeiture of instrumentalities (e.g. for drug offenses, 21 USC §881, 21 USC §853(a)(2); for firearms offense, 18 USC §924(d), 26 USC §5372; for smuggling offenses, 19 USC §1595a).

NCBF is permitted for the proceeds of ML and predicate offenses, and in respect of the instrumentalities of a ML offense and some of the predicate offenses: 18 USC (a)(1)(C). Instrumentalities (some forfeitable in the U.S. under statutes authorizing forfeiture of *facilitating property* or property used to commit an offense) are forfeitable pursuant to some of the main forfeiture statutes and the statutes criminalizing certain offenses<sup>70</sup>. Specifically, 18 USC §981(a)(1)(G) provides for the forfeiture of “all assets, foreign or domestic (...) of any individual, entity or organization engaged in planning or perpetrating any *Federal crime of terrorism*.” *Federal crime of terrorism* is defined in 18 USC §2332b(g)(5) to include the primary TF offenses, namely 18 USC §2339A (providing material support to terrorists), 18 USC §2339B (providing material support to terrorist organizations), and 18 USC §2339C (financing of terrorist acts).<sup>71</sup>

Equivalent value forfeiture is possible in criminal cases when the tainted property subject to confiscation under a particular statute has become unavailable. In such cases, the *substitute assets*

<sup>69</sup> 18 USC §983(a)(1)-(2), 19 USC 1602 & 1607, and other statutes.

<sup>70</sup> E.g. 18 USC §982(a)(6)-(8); 8 USC. §1324(b), 18 USC §981(a)(1)(B) (facilitating property for certain foreign crimes, including drug trafficking, crimes of violence, public corruption); 18 USC §§2253 and 2254; 17 USC §§506(b) and 509; 16 USC §407; 16 USC §1540(e)(4); 16 USC §3637(d); 18 USC §1037(c)(1)(B); 18 USC §2319A(b); 22 USC §401(a); 21 USC §881(a); 18 USC §1028(b)(5); 18 USC §1029(c)(1)(C); 18 USC §1955(d); 18 USC §986(a)(6); etc.

<sup>71</sup> 18 USC §981(a)(1)(G), 18 USC §2332(b)(g)(5), 18 USC §2339A, 18 USC §2339B, 18 USC §2339C.

are forfeitable value-based confiscation order made upon the criminal conviction of the defendant: Rule 32.2(e) of the *Federal Rules of Criminal Procedure* and replicated in many separate Federal offenses that give rise to confiscation<sup>72</sup>. For ML offenses, equivalent value forfeiture is not applied where the defendant acted merely as an intermediary who handled but did not retain the property in the course of the ML offense, unless the defendant conducted three or more separate transactions involving a total of USD 100 000 or more in any 12 month period: 18 USC §982(b)(2).

*Criterion 4.2* - The U.S. has measures that enable their competent authorities to:

- a) Identify, trace and evaluate property subject to confiscation by using grand jury and administrative subpoenas, search warrants and writs of entry: 18 USC §985, 18 USC §3322.
- b) Carry out provisional measures (e.g. seizure or restraint), or other measures to preserve property prior to trial, and prevent any transfer/disposal of property subject to confiscation<sup>73</sup>. There is no general power to freeze/seize non-tainted assets prior to a conviction or value-based confiscation order, although this is possible on one Federal judicial circuit.
- c) Take steps (in both civil and criminal proceedings) to prevent or void actions prejudicing the country's ability to freeze/seize/recover property subject to confiscation: 18 USC §981(f), 18 USC §982(b)(1), 21 USC §853(c). It is an offense to take any action to destroy/remove property to prevent seizure or to knowingly impair the jurisdiction of a U.S. court over property subject to confiscation: 18 USC §2232 (a) & (b). Violations of restraining orders issued in advance of forfeiture can be deemed contempt of court, the punishment for which can include imprisonment.
- d) Take any appropriate investigative measures through the broad investigative powers described in R.29 and R.31.

*Criterion 4.3* - The rights of bona fide third parties are protected by law<sup>74</sup>.

*Criterion 4.4* - The U.S. has various mechanisms for managing and, when necessary, disposing of property frozen, seized, and confiscated. All forfeited cash, proceeds from the sale of forfeited property, interest from the investment of the DOJ – AFF balances, and interest from the Seized Asset Deposit Fund (i.e. currency not yet confiscated) are to be deposited with JAFF. Proceeds of all confiscations enforced/administered by a Treasury or DHS LEA occurring are deposited into the TFF. Both funds may be used for asset management expenses, qualified third party interests, equitable asset sharing payments, or investigative expenses.

<sup>72</sup> 21 USC §853(p); 18 USC §982(b)(2); 18 USC §1963(m), 31 USC §5332(b)(4); 31 USC §5317(c)(1)(B), 18 USC §2253(b).

<sup>73</sup> E.g. 18 USC §982(b)(1)-(3), 18 USC §981(b)(4) (restraint of assets pursuant to foreign arrest or charge) 21 USC §853(e)&(f), 18 USC §983(j), 18 USC §981(b)(2); 18 USC §981(k) (seizure of funds subject to forfeiture in correspondent accounts); 19 USC §§1594-95, 1602-03.

<sup>74</sup> *Federal Rules of Criminal Procedure* 32.2(c); 18 USC §982(b)(1); 21 USC §853(c) & (n); 21 USC §853(n)(6)-(7); 18 USC §1963(l)(6)-(7) (RICO); 18 USC §983(d) (innocent owner defense); Rule G of the Federal Rule of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Action.



*Weighting and Conclusion:*

Although the confiscation of instrumentalities is not covered for all predicate offenses, this is a minor deficiency as the key predicate offenses (from a risk perspective) do yield this power, including the drug and RICO offenses. There is no general power to freeze/seize non-tainted assets prior to a conviction to preserve them in order to satisfy a value-based confiscation order; however, this is permitted on one Federal judicial circuit.

**Recommendation 4 is rated largely compliant.**

**Recommendation 5 - Terrorist financing offense <sup>75</sup>**

In the previous mutual evaluation, the U.S. was rated as compliant with these requirements.

**Criterion 5.1.** - The U.S. criminalises TF in line with the *United Nations Convention for the Suppression of Terrorist Financing* (TF Convention). There are five Federal TF offenses:

- a) ***Wilful provision or collection of funds*** with the intention that such funds be used, or with the knowledge that such funds<sup>76</sup> are to be used, in full or in part, in order to carry out: i) an offense set out in the treaties listed in the Annex of the *TF Convention*<sup>77</sup>; or ii) any other acts intended to cause death or serious bodily injury to a civilian or any other person not taking an active part in the hostilities in a situation or armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act: 18 USC §2339C(a).
- b) ***Knowing concealment or disguise of the nature, location, source, ownership or control of any material support or resources, or any funds or proceeds of funds***, with the knowledge or intent that the concealed material support or funds were or would be: i) provided to a designated foreign terrorist organization in violation of 18 USC. §2339B; or ii) provided or collected in violation of 18 USC. §2339C(a): 18 USC §§2339C(c)(2)(A) and (B).
- c) ***Knowing provision of material support or resources, or concealing or disguising the nature, location, source, or ownership of material support or resources, with the intent or knowledge that such material support or resources are to be used for preparing for or carrying out certain enumerated predicate offenses related to terrorism***, including but not limited to those involving: aircraft and airports; arson; chemical, biological, and nuclear weapons; explosives; hostage taking; damage to U.S. property, communications lines and systems or energy facilities; or any other offense separately listed as a *Federal crime of terrorism*, meaning certain acts calculated to influence or affect the conduct or retaliate against the conduct of the U.S. government: 18 USC§ 2339A, 18 USC §2332b(g)(5)(B).

<sup>75</sup> R.5 and its interpretative note were revised by the FATF in February 2016, i.e. after the on-site visit. The revised version will be taken into account during the follow-up process.

<sup>76</sup> *Funds* is defined in line with Article 1.1 of the *TF Convention*.

<sup>77</sup> All of these treaties have been entered into force in the United States.



- d) **Knowing provision of material support or resources to Foreign Terrorist Organizations (FTO)**, as designated by the Secretary of State under section 219 of the *Immigration and Nationality Act*, codified as amended at 8 USC §1189, knowing that the organization is a designated FTO, or knowing that the organization engages or has engaged in terrorist activity or terrorism: 18 USC. §2339B. *Terrorist activity* covers a broad range of violent criminal behaviour: 8 USC §§1182(a)(3)(B)(iii) and (iv). *Terrorism* is defined as “premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents”: 22 USC §2656f(d)(2).
- e) **Wilfully undertaking financial transactions (including making/receiving contributions of funds, goods or services) with a Specially Designated Global Terrorist (SDGT)**, as designated by the Secretaries of State or Treasury under Executive Order (E.O.) 13224 (2001). U.S. persons and persons within the United States are prohibited from engaging in financial transactions with any SDGT (which can include both individuals and entities, foreign and domestic) unless they have first obtained a license from OFAC, nor may they engage in a transaction to circumvent E.O. 13224, or make or receive any contribution of funds, goods, or services to or for the benefit of an SDGT. E.O. 13224, 50 USC. §1705(c).

*Criterion 5.2* - Together these five TF offenses extend to any person who wilfully provides or collect funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used to carry out a terrorist act (18 USC §§2339A, 2339C(a), and 2339C(c)(2)(B)), or be used by a terrorist organization or by an individual terrorist in the absence of a terrorist act (18 USC §§2339C(c)(2)(A), 2339B, 50 USC §1705(c)).

*Criterion 5.3* - The TF offenses extend to any funds and/or other types of material support or resources whether from legitimate or illegitimate source: 18 USC §2339A(b)(1), 18 USC §2339C(e).

*Criterion 5.4* - Neither the offense of providing material support or resources to FTOs nor wilfully undertaking financial transactions with designated persons and organizations requires the funds to have been used to carry out or attempt a terrorist act or be linked to a terrorist act: 18 USC §2339B and 50 USC §1705(c). For the wilful provision or collection of funds offenses, it is not necessary that funds were actually used or intended to be used to carry out a terrorist act as defined in the treaties listed in the Annex of the *TF Convention*: 18 USC §2339C(a)(3). The material support offense of §2339A is linked to the commission of a terrorist act or attempt to commit such act (defined as a wide range of predicate offenses covering activities carried out with terrorist purposes).

*Criterion 5.5* - Intent and knowledge may be inferred from objective factual circumstances: *Federal Rules of Evidence*.

*Criterion 5.6* - Sanctions are proportionate and dissuasive: up to 20 years imprisonment for each violation and/or a fine (§2339C(a)); up to 20 years imprisonment for each violation or indefinitely where the act resulted in death, and/or a fine (§2339B); up to 15 years imprisonment or indefinitely where the act resulted in death, and/or a fine (§2339A); and up to 10 years imprisonment and/or a fine for each violation (§2339C(c)). The maximum fine applicable for all these offenses is USD 250 000 for a natural person and may be many times this in respect of an organization when a multiplier is applied to calculate the amount of the fine: §§2339A, 2339B, 2339C. Civil penalties of at

least USD 10 000 apply to legal entities breaching §2339C(a), and of USD 50 000 or at least twice the amount of which the FI was required to retain possession of for breaches of §2339B(a)(2): §2339C(f), §2339B(b). Wilfully undertaking financial transactions with SDGTs is punishable by imprisonment for up to 20 years and criminal fines of up to USD 1 000 000, or both: 50 USC §1705(c). Civil penalties up to USD 250 000 or an amount that is twice the amount of the transaction that is the basis of the violation (whichever is greater) can also be imposed: 50 USC §1705(b).

*Criterion 5.7* - Both natural and legal persons can be prosecuted for the TF offenses: §§2339A, 2339B and 2339C; 50 USC §1705, s.3 E.O. 13224. In addition to any other criminal, civil, or administrative liability, specific civil penalty provisions apply to legal entities situated in the U.S. or organized pursuant to U.S. law if a person responsible for the management or control of that legal person has, in that capacity, committed the offense of providing/collection funds, or attempting or conspiring to do so: USC §2339C(f).

*Criterion 5.8* - Attempting or conspiring to commit the TF offenses is criminalised: 18 USC §§2339A(a), 2339B(a)(1), 2339C(a)(2), and 50 USC §1705(a). Anyone found aiding and abetting, counselling, commanding, inducing, or procuring the commission of a crime can be prosecuted and punished as a principal: 18 USC §2.

*Criterion 5.9* - Sections 2339A, 2339B, and 2339C are predicates for ML: 18 USC §1956(c)(7)(D). Violations of 50 USC §1705 are not, but this would be an issue only in limited circumstances.

*Criterion 5.10* - The TF offenses apply, regardless of whether the person alleged to have committed the offense is in the same or different country from the one in which the terrorist(s)/terrorist organization(s) is located or the terrorist act(s) occurred/will occur: §2339A (unlimited jurisdiction to prosecute), §2339B (applicable to anyone within the U.S. or subject to its jurisdiction), §§2339B(a)(1) & (d) (extra-territorial Federal jurisdiction allows U.S. offenders, non-U.S. offenders and persons who have never been in the U.S. to be prosecuted for crimes committed). The 2339C(a) offense applies extra-territorially and includes “found-in” jurisdiction, extending the jurisdictional reach to anyone later brought into the U.S. to face charges, regardless of where the initial crime took place: 2339C(b)(2)(B). Any U.S. person or any person within the U.S. may be liable under E.O. 13224: 50 USC §1705.

### *Weighting and Conclusion:*

All of the 10 criteria are met.

***Recommendation 5 is rated compliant.***

### ***Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing***

In its 3rd MER, the U.S. was rated largely compliant as targeted financial sanctions (TFS) were not implemented against all persons/entities designated pursuant to United Nations Security Council Resolution (UNSCR) 1267(1999). The framework has not substantively changed since then.

*Criterion 6.1* - For designations under UNSCRs 1267/1989 and 1988:

- a) The Department of State is the competent authority responsible for proposing designations to the UN via the U.S. Mission to the UN.
- b) Potential targets for designation are identified using a range of classified and open sources. The lead agency (Treasury or State), in consultation with the non-lead agency and DOJ, compiles an administrative record of classified and unclassified information supporting the designation, based on the criteria in the relevant UNSCRs.
- c) The evidentiary standard of proof applied to a designation proposal is a “reason to believe” and legal review of the designation process is under the “arbitrary and capricious” standard of the: *Administrative Procedure Act*. The decision is not conditional on the existence of a criminal proceeding.
- d) Submissions are made using the UN standard forms and procedures for listing filled out in coordination with the agency that developed the domestic designation evidentiary information.
- e) Submissions include the basis for the designation, with supporting unclassified information, and as much identification information on the target as possible. The U.S. usually allows its status as a designating state to be made known.

*Criterion 6.2 - For designations under UNSCR 1373:*

- a) The Secretaries of the Treasury (Sec/Treasury), State (Sec/State), Homeland Security and the Attorney General consult on all designations. The Sec/Treasury is the lead for designating foreign/domestic persons owned, controlled by, acting on behalf of, associated with, assisting or supporting terrorist acts or designated persons: SDGTs: 31 CFR 594.316 & E.O. 13224; 31 CFR 594.310.. The Sec/State is the lead for designating: foreign persons who have committed (or pose a significant risk of committing) terrorist acts threatening U.S. security, its nationals, foreign policy or economy; and FTOs<sup>78</sup>.
- b) The U.S. has clear State or Treasury-led mechanisms and dedicated resources for identifying targets for designation.
- c) When a third country requests the U.S. to take freezing action, Treasury (or State) prepares an administrative record (*evidentiary*) to support a U.S. designation under E.O. 13224.
- d) The same standard of proof applies as is described in c.6.1(c) (“reason to believe basis”).
- e) When requesting another country to give effect to freezing mechanisms, the U.S. provides an unclassified statement of the case, including the basis for the designation and identifiers associated with the target itself and additional information when possible.

*Criterion 6.3 - The President is authorized to collect identifying information on individuals and entities meeting the designation criteria: IEEPA, National Emergencies Act. These powers are delegated to the Sec/Treasury and Sec/State for the designation of specially designated terrorists (SDTs) and SDGTs. The Sec/State is also authorized to collect information to designate organizations*

<sup>78</sup> *Immigration and Nationality Act*, s.201, codified as amended at 8 USC §1189. All current FTOs have also been designated as SDGTs pursuant to E.O. 13224.

as FTOs: 8 USC §1189(a). Ex parte action may be taken if the applicable law/regulation does not explicitly state that a person/entity must be present and no prior notice of a designation is needed:<sup>1</sup> E.O. 13224, s.10.

*Criterion 6.4* - Domestic designations pursuant to UNSCR 1373 implement TFS without delay by taking immediate legal effect: E.O. 13224. UN designations pursuant to 1267/1989 and 1988 are generally implemented without delay from the moment of UN designation, even though the domestic designation process may take a number of months. This is because of a unique feature of the U.S. context: as a P5 member of the Security Council, the U.S. always receives pre-notification of proposed UN designations and almost always completes its designation process prior to UN listing. The U.S. has not implemented TFS against all persons/entities designated by the UN and on a few occasions has not implemented designations without delay (see analysis under IO.10). The USG reports however that since 2010, 88% of its domestic designations of UN-designated entities have been made without delay within a matter of hours of UN designation).

*Criterion 6.5* - OFAC administers three sanctions programs for terrorists and terrorist organizations: (i) the *Terrorism Sanctions Regulations* (31 CFR Part 595 implements E.O. 12947 on foreign terrorist disruptions of the Middle East peace process); (ii) the *Global Terrorism Sanctions Regulations* (31 CFR Part 594 implements E.O. 13224 on grave acts/threats of terrorism by foreign terrorists); and (iii) the *Foreign Terrorist Organizations Sanctions Regulations* (31 CFR Part 597).

- a) All U.S. persons (natural and legal), including citizens and lawful permanent residents in the U.S, all U.S. companies and their branches worldwide, and foreign entities and individuals with respect to their activities in the U.S. are required to freeze without delay or prior notice the funds or other assets of designated persons/entities.
- b) Freezing<sup>79</sup> actions pursuant to E.O. 13224 extend to all property and “interests in property”<sup>80</sup> in line with the criteria set out under c.6.5(b).
- c) All U.S. persons<sup>81</sup> are prohibited from dealing with, and providing services to/by/for the benefit of, persons (natural and legal) and entities designated pursuant E.O. 13224 and E.O. 12947 unless first authorized by OFAC<sup>82</sup>.
- d) OFAC has mechanisms in place to communicate designations (and any changes to the lists) to FIs and DNFBPs including publication of the Specially Designated Nationals (SDN) and Blocked Persons List and in the Federal Register via a bulletin to the Clearing House Interbank Payment System (CHIPS) member banks and multiple e-mail notification lists. The Federal Reserve Bank of New York resends an electronic bulletin of all designations to the more than 10 000 institutions connected to its Fedwire system.

<sup>79</sup> “Blocking” is the term for the freezing of assets used in Executive Orders and OFAC regulations.

<sup>80</sup> Meaning an interest of any nature whatsoever, direct or indirect, in whole or in part: 31 CFR 594.306. Under OFAC’s “50 Percent Rule,” any entity owned 50% or more in the aggregate by one or more blocked individuals or entities is also considered blocked, regardless of whether that entity is listed on OFAC’s SDN List.

<sup>81</sup> Including permanent resident aliens or any person in the U.S: 31 CFR 594.315.

<sup>82</sup> 31CFR Part 594 implements E.O. 13224, 31 CFR Part 595 implements E.O. 12947.

- e) Anyone freezing/rejecting a funds transfer must report to OFAC within 10 business days: 31 CFR 501.603. Upon receipt, these reports are examined to ensure that appropriate action was taken.
- f) The rights of innocent third parties are protected: see c.4.3 above.

*Criterion 6.6* - There are mechanisms for de-listing and unfreezing the funds/other assets of persons/entities which do not, or no longer, meet the designation criteria:

- a) For 1267/1989 or 1988, persons submitting a de-listing request are directed to the relevant UN Sanctions Committee website for information on the de-listing procedure. The U.S. will notify the relevant Committee and provide supporting material if it believes that a person/entity no longer meets the UN designation criteria.
- b) For 1373, procedures for de-listing and unfreezing the funds/other assets of persons/entities no longer meeting the designation criteria are publicly outlined in 31 CFR 501.807.
- c) For 1373, the U.S. has public procedures to allow, upon request, review of the designation decision before a court: 31 CFR 501.807, Administrative Procedure Act, and U.S. Constitution.
- d) For 1988, if OFAC or the State Department determines that a person/entity will be de-listed domestically (based on the procedures above), the U.S. will contact the relevant UN authority to facilitate a review of the UN designation pursuant to the procedures set out in UNSCR 1730.
- e) For 1267/1989, if OFAC or the State Department determines that a person/entity will be de-listed domestically, it will contact the relevant UN authority and Ombudsperson Committee to facilitate a review of the UN designation pursuant to the procedures in UNSCRs 1904, 1989 and 2083. If the U.S. believes the person/entity should remain designated, it will share with the Ombudsperson information regarding the designated person/entity.
- f) There are procedures to request the unfreezing of funds believed to have been frozen in error due to mistaken identity: 31 CFR 501.806.
- g) The mechanisms in c.6.5(d) are used to communicate de-listing/un-freezing actions.

*Criterion 6.7* - OFAC can license or authorize access to frozen property/accounts to the extent necessary for basic or extraordinary expenses (humanitarian grounds) or to transfer non-frozen assets into the U.S. which prevents them from being frozen upon receipt by a U.S. person.

### *Weighting and Conclusion:*

The U.S. has applied TFS to most but not all persons pursuant to UNSCRs 1267/1988/1989, and on a few occasions has not implemented TFS without delay (c.6.4). This is a minor deficiency because: the U.S. has implemented TFS without delay against 88% of the persons/entities designated by the UN since 2010. TFS have been applied to all UN Taliban designations since 2006, and the Taliban was designated as an entity which, in principle, captures anyone associated with it.

***Recommendation 6 is rated largely compliant.***

### ***Recommendation 7 – Targeted financial sanctions related to Proliferation***

This is a new Recommendation which was not assessed in the 3<sup>rd</sup> MER report.

*Criterion 7.1* - OFAC implements proliferation-related TFS programs without delay in the same way as described in c.6.4, under Executive Orders on combating the proliferation WMD. The U.S., as a P5 member of the Security Council, always receives pre-notification of proposed UN designations and, therefore, is able to postpone the UN process if necessary until its own domestic designation is in place<sup>83</sup>. The only deficiency is that the U.S. has not implemented TFS against all of the persons/entities designated by the UN pursuant to UNSCRs 1718 and 1737 (see IO.11).

*Criterion 7.2* - OFAC is responsible for implementing and enforcing TFS as follows:

- a) TFS apply to: all U.S. natural/legal persons and permanent resident aliens regardless of where they are located, all persons/entities within the U.S., and all U.S. incorporated entities and their foreign branches. Certain programs also require foreign subsidiaries owned or controlled by U.S. persons and foreign persons in possession of U.S.-origin goods to comply.
- b) Freezing<sup>84</sup> actions pursuant to E.O. 13382 and E.O. 13551 extend to all property and “interests in property” (meaning an interest of any nature whatsoever, direct or indirect, in whole or in part) that come (or thereafter come) within the U.S., or within the possession or control of U.S. persons, which includes most products/services provided by FIs located in the U.S. or organized under its laws, including their overseas branches: 31 CFR 544.305; 31 CFR 544.308; 31 CFR 510.307. A person/entity’s property and interests in property are also frozen if they are owned, directly or indirectly, 50% or more by one or more designated persons/entities, regardless of whether the entity itself is on OFAC’s SDN List.
- c) Payments, transfers, exportations, withdrawals, or other dealings may not be made or effected with respect to frozen property or frozen accounts except pursuant to an authorization or license from OFAC expressly authorizing such action: 31 CFR 544.201. For DPRK, with certain exceptions, U.S. persons are prohibited from transferring, paying, exporting, withdrawing, or otherwise dealing in the property and interests in property of an person/entity named in the Annex to E.O. 13551 or designated pursuant to the North Korea Sanctions Regulations: 31 CFR 510.
- d) The process for communicating designations described in c.6.5(d) is used.
- e) Anyone holding frozen funds or property is required to report to OFAC within 10 business days, and submit an Annual Report of Blocked Property detailing the aggregate value of the property being held under each sanctions program: 31 CFR 501.603. FIs that reject a funds transfer where the funds are not blocked under the provisions of this chapter, but where processing the transfer would nonetheless violate, or facilitate an underlying transaction that is prohibited under other sanctions programs must report the rejected transaction to OFAC within 10 business days

<sup>83</sup> Executive Order 13382 (E.O. 13382); 31 CFR Part 544; 31 CFR 510; Executive Order 13551 (E.O. 13551).

<sup>84</sup> “Blocking” is the term for the freezing of assets used in Executive Orders and OFAC regulations.



- f) The rights of bona fide third parties are protected: see c.6.6(f) & 6.6(b).

*Criterion 7.3* - OFAC administers and enforces compliance with TFS and issues guidelines for their enforcement: Appendix A to 31 CFR 501. The State and Federal financial regulatory agencies monitor the FIs/DNFBPs under their supervision for compliance with proliferation-related TFS: see R.26 and R.28. Civil, administrative and criminal sanctions apply for failing to comply with sanctions programs<sup>85</sup>. Penalties range from USD 250 000 fine for natural persons to USD 1 million for legal persons. Imprisonment ranges from 5 to 20 yrs. Penalties are considered proportionate and dissuasive.

*Criterion 7.4* - The U.S. has publicly known procedures to submit de-listing requests to OFAC for domestically designated persons/entities that, in the U.S. view, no longer meet the designation criteria (31 CFR 501.807). Such procedures mirror those for c.6.6, in line with the UN obligations. If OFAC determines that a person/entity will be de-listed domestically, it will contact the Focal Point. If the U.S. believes the person/entity should remain listed by the UN, the U.S. may share with the Focal Point information (possibly even classified information) to support the continued designation.

- a) Persons/entities not (or no longer) meeting the designation criteria may be de-listed and their funds/other assets unfrozen: 31 CFR 501.807. The OFAC website has links that allow de-listing petitioners to directly contact the staff responsible for reviewing petitions.
- b) Publicly known procedures exist to unfreeze funds/assets of persons with the same/similar name as designated persons/entities or those inadvertently affected by a freezing mechanism: see sub-criteria 7.2(f) & 6.6(f).
- c) OFAC has authority to license certain transactions that otherwise would be prohibited due to sanctions, when doing so would "further U.S. foreign policy: 31 CFR 501.801. These procedures are publicly available and in line with the procedures set out in UNSCRs 1718 and 1737.
- d) De-listings and unfreezings are communicated through the same channels used to communicate the initial sanctions obligations: see c.7.2(d) & 6.5(d).

*Criterion 7.5* - The U.S. has mechanisms to handle contracts, agreements or obligations that arose prior to the date on which accounts became subject to TFS: a) any U.S. person holding such funds shall hold or place them in a *blocked interest-bearing account*<sup>86</sup> located in the U.S.; and b) OFAC may authorize release of certain frozen funds or economic resources in accordance with criterion 7.5 and relevant UNSCRs under the licensing procedures described c.7.4(c).

<sup>85</sup> *OFAC Reporting, Procedures and Penalties Regulations* 31 CFR 501.701, *WMD Trade Control Regulations* 31 CFR 539.701, and *WMD Proliferators Sanctions Regulations* 31 CFR 544.701.

<sup>86</sup> Meaning an account blocked: i) in a federally insured U.S. bank, thrift institution, or credit union, provided the funds are earning interest at rates that are commercially reasonable; or ii) with a broker or dealer registered with the SEC under the *Securities Exchange Act of 1934*, provided the funds are invested in a money market fund or in U.S. Treasury bills: 15 USC 78a et seq.: 31 CFR 544.203.

*Weighting and Conclusion:*

The U.S. has applied TFS without delay to most but not all persons designated by the UN pursuant to UNSCRs 1718 and 1737. This is a minor deficiency as the U.S. has implemented 90% (138 of the 154) of the UN DPRK-related and Iran-related listings without delay (within a matter of hours).

***Recommendation 7 is rated largely compliant.***

***Recommendation 8 – Non-profit organizations (NPOs)*** <sup>87</sup>

In its 3<sup>rd</sup> MER, the U.S. was rated compliant. The FATF had not yet adopted the detailed requirements of the Interpretive Note to this Recommendation.

*Criterion 8.1* - The U.S. has conducted several internal reviews of its domestic charitable sector to assess its risk of misuse for TF: one in June 2010 as part of TFS information published by Treasury, and another in 2012/13 to support the 2015 *National Terrorist Financing Risk Assessment*. While there has been no separate, comprehensive review of the adequacy of laws and regulations relating to NPOs since 2003, the authorities indicated that the laws are subject to ongoing review (e.g. by the civil components of IRS) and any deficiencies are brought to the notice of policy-makers. One important example of this process was the enhancements made to the Form 990 (the annual returns required from tax-exempt NPOs) in 2008.

*Criterion 8.2* - Treasury conducts multifaceted outreach to NPOs to raise awareness of TF threats and deter their misuse. It maintains resources for charities on risks of terrorist abuse on its [website](#), issues periodic general and thematic guidance, and holds regular meetings with NPOs to discuss guidance, CFT policies, practices and challenges such as maintaining access to the regulated financial system.

*Criterion 8.3* - The U.S. pursues a policy of promoting transparency, integrity and public confidence in the administration and management of all NPOs through its outreach. Transparency is also facilitated by Federal tax laws which provide that most information reported by tax-exempt NPOs to the IRS Tax Exempt and Government Entities Division (IRS-TEGE) is publicly available.

*Criterion 8.4* - Approximately 1.4 million tax-exempt organizations (including public charities and private foundations) and 300 000 houses of worship or smaller public charities account for a significant portion of the financial resources under control of the NPO sector, and a substantial share of the sector's international activities. Both Federal and (varying) State requirements apply to those entities falling under the FATF definition of *non-profit organization* to ensure that they:

- a) Document administrative and policy controls over their operations; meet an organizational and operational test to qualify for tax exemptions; and file with the IRS forms<sup>88</sup> and relevant associated documents, including detailed identifier and organizational information, when applying for tax exemptions: IRC Section 501(c)(3).

<sup>87</sup> R.8 and its interpretative note were revised by the FATF in June 2016, i.e. after the on-site visit. The revised version will be taken into account during the follow-up process.

<sup>88</sup> Form 1023 for charities, and Form 1023-EZ for smaller charities.

- b) File annual statements to the IRS providing information on their income, expenses, assets, liabilities, programs (Form 990). Smaller charities with annual gross receipts under USD 50 000 file an annual Form 990-N keeping their identifying information up to date. Some states also require charities to file periodic financial results with the State if they hold assets subject to a charitable trust.
- c) Maintain financial records and other information reported on Form 990 and other IRS forms.
- d) Apply to the IRS for recognition of their tax-exemption status. Houses of worships are exempt from these requirements, but this gap is partly mitigated as many choose to apply for tax-exempt recognition since it may result in exemptions from State/local income and property taxes and enable donors to obtain charitable deductions for their contributions. Thirty nine states require any charity to register before soliciting funds within the State, no matter where the charity is domiciled.
- e) Keep detailed records and case histories to demonstrate that grants to individuals serve their charitable purposes.<sup>89</sup>
- f) Retain records for Federal tax purposes until the statute of limitations expires for the charity amending its return and the IRS assessing additional tax (usually 3 years after the return is due or filed, whichever is later). Longer retention period may be required for State or local taxes, but the required 5 years retention period is not met in all circumstances.

*Criterion 8.5* - At the Federal level, IRS-TEGE monitors compliance with U.S. tax laws, and IRS-CI conducts criminal investigations as necessary. Although houses of worship are not required to file a Form 990 series return, the IRS can examine them if there is a reasonable belief that they are engaging in activities not consistent with their tax-exempt status. Penalties apply for violating these requirements which appear to be proportionate and dissuasive (see R.35). The States and District of Columbia oversee the fund-raising practices of charities domiciled or operating in their jurisdictions. Charities operating in the U.S. are also subject to self-regulation managed by umbrella and watchdog organizations.

*Criterion 8.6* - Authorities are able to investigate NPOs and gather relevant information:

- a) To enhance domestic coordination and information sharing on TF issues, IRS-TEGE personnel are detailed to FBI-TFOS, and IRC-CI special agents are assigned to the Joint Terrorism Task Forces (JTTFs) and Treasury's OIA. Other Federal LEAs may partner with IRS-CI to obtain access to non-public tax information for their investigations of terrorist activity under certain conditions specified by law. Within IRS, the civil examiners in IRS-TEGE work with IRS-CI which enhances its ability to investigate terrorist abuse of NPOs.
- b) All relevant authorities can access relevant programmatic and financial information if needed.
- c) There are multiple mechanisms to promptly share information regarding suspicion of terrorist abuse including: Federal LEAs directly accessing FinCEN's database (see R.29 and IO.6); the JTTF task force environment which brings together multiple agencies to investigate TF activity; and coordination with OFAC when NPOs are designated pursuant to R.6. TEGE has

<sup>89</sup> Compliance Guide for 501(C)(3) Public Charities, Schedule I of Form 990 and instructions.

its own financial investigative capabilities and can process leads from all relevant Federal, State and local sources.

*Criterion 8.7* - The Department of State, Bureau of Economic and Business Affairs, is the initial point of contact for international requests for information on NPOs suspected of TF abuse. Inquiries are then forwarded to the appropriate agency, such as the IRS for information related to Federal tax returns.

*Weighting and Conclusion:*

Sub-criterion 8.4(f) has one deficiency which the assessment team considers to be minor as the time limits for record retention are not insubstantial and, in some instances may meet and exceed the 5-year minimum required by R.8. There also remains a gap in the system in relation to houses of worship which are not captured by or do not voluntarily choose to submit to federal or state requirements (see sub-criterion 8.4(d)).

***Recommendation 8 is rated largely compliant.***

***Recommendation 9 – Financial institution secrecy laws***

In its 3rd MER, the U.S. was rated compliant with these requirements. The detailed analysis set out at paragraphs 557 – 567 of the 3<sup>rd</sup> round 2006 MER continues to apply.

*Criterion 9.1* - FI secrecy laws do not inhibit the implementation of AML/CFT measures. The *Right to Financial Privacy Act* (RFPA) (12 USC 3401-22.) governs how U.S. Federal agencies obtain information from FIs<sup>90</sup>, and under what circumstances they may disclose it:

- a) Access to information by competent authorities: The RFPA contains numerous exceptions to allow disclosure by an FI to competent authorities for regulatory/supervisory, law enforcement and intelligence matters. Accounts of individuals held by FIs not subject to the RFPA are protected from disclosure to the Federal Government by the Gramm-Leach-Bliley Act (GLBA), 15 USC 6801 et seq., and its implementing regulations. The GLBA allows FIs to provide non-public personal information about their customers to law enforcement when served with a court order, and also allows sharing for required institutional risk control purposes and to protect against fraud. The GLBA also grants FIs safe harbor, including for disclosures to law enforcement, on matters related to public safety, institutional risk control and fraud prevention. GLBA does not restrict a federal regulator's ability to get information from its regulated entities.
- b) Sharing of information between competent authorities: The RFPA also governs the transfer of covered financial records by the Federal agencies holding those records, and permits the sharing of information for a wide range of purposes: 12 USC 3412 and 3413.

<sup>90</sup> The RFPA defines "financial institution" to include any of the following entities located in any state or territory of the U.S.: any office of a bank; savings bank; card issuer [as defined in 15 USC 1602(n)]; industrial loan company; trust company; savings association; building and loan or homestead association (including cooperative banks); credit union; and consumer finance institution".

- c) Sharing of information between FIs: FIs are able to share information with one another, under a safe harbor that offers protections from liability, to better identify and report potential ML or terrorist activities: s.314(b), USA PATRIOT Act: 31 CFR. 1010.520. Participation in information sharing pursuant to section 314(b) of the USA PATRIOT Act is available to those FIs located in the U.S. and required to have AML compliance programs pursuant to Section 352 of the USA PATRIOT Act.

### *Weighting and Conclusion:*

The criterion is met.

**Recommendation 9 is rated compliant.**

### **Recommendation 10 – Customer due diligence**

In its 3rd MER, the U.S. was rated partially compliant. The technical deficiencies related to: insufficient requirements to identify BOs and conduct ongoing due diligence; timing of customer identity verification and the obligation to terminate the business relationship; customer identification for occasional transactions not involving cash; and scope issues (IAs, commodity trading advisors, and life insurers were not adequately covered).

*Criterion 10.1* - Keeping anonymous accounts or accounts in obviously fictitious names is not expressly prohibited. However, the CIP provisions have been in place for many years and prevent opening anonymous accounts or accounts in fictional names. **Covered FIs**<sup>91</sup> are required to implement a written CIP that must include risk-based procedures for verifying the identity of each customer to enable a FI to form a reasonable belief that it knows the customer's true identity. At a minimum, persons opening accounts must provide the following information which the FI must verify: name, date of birth (for natural persons), address and/or place of business, and an identification number (for U.S. persons, a tax payer identification number (TIN)<sup>92</sup> and for non-U.S. persons, at least one of the following: a TIN, passport number (and country of issuance), alien identification card number, or number and issuing country of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard). The foregoing measures apply regardless of risk, and thus appear to prevent FIs from opening anonymous accounts or accounts in fictitious names: 31 CFR §1020.220. There are no equivalent explicit obligations for **life insurance companies, loan or finance companies and government sponsored housing enterprises**, other than a general requirement to obtain all relevant customer related information necessary for an effective AML program, which in the life insurance sector, only applies to permanent life insurance policies, other than group life insurance policies; annuity contracts, other than group annuity contracts; and any other insurance product with features of cash value or investment: CFR §1025.210, CFR. §1029.210 and CFR §1030.210 respectively. **MSBs** are

<sup>91</sup> This includes insured banks, commercial banks, agencies or branches of a foreign bank in the U.S., credit unions, savings associations, corporations acting under section 25A of the *Federal Reserve Act* 12 USC 611, trust companies, securities broker-dealers, futures commission merchants (FCMs), introducing brokers in commodities (IBs), and mutual funds.

<sup>92</sup> The CIP program rules permit covered FIs to rely on evidence that a TIN has been applied for before the account is opened, if it has not yet been received.

subject to a general requirement to develop, implement and maintain effective AML programs, reasonably designed to prevent them from being used to facilitate ML/TF. The program must incorporate policies, procedures and internal controls reasonably designed to assure compliance with CFR §1022.200 including, *inter alia*, requirements for verifying customer identification: CFR §1022.210.

**Criterion 10.2 - Covered FIs** are required to undertake CDD measures when:

- a) Establishing business relations: Covered FIs are required to establish a written CIP that must contain account opening procedures. At a minimum, prior to opening an account<sup>93</sup>, they must obtain and verify certain identity information from their customers: see c.10.1. The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. Life insurance companies are required to integrate agents and brokers into their AML programs and obtain all relevant customer-related information necessary for an effective AML program (regulatory expectations do not specify when this needs to be obtained). MSBs do not typically maintain customer account relationships, but do have CDD obligations in those limited circumstances: currency dealers or exchangers (31 CFR §1022.410 and providers of prepaid access (31 CFR §1022.210(d)(1)(iv)).
- b) Carrying out occasional transactions: Certain FIs (including banks, securities broker-dealers, FCMs, IBs, MSBs, and mutual funds) are required to record and report transactions in currency above USD 10 000 (CTRs) to FinCEN after verifying the customer's identity. This obligation requires reporting related transactions that together exceed USD 10 000 and are made during the same day if the FI has knowledge that each transaction was made by or on behalf of the same person. Other FIs (e.g. life insurance companies) must record and report on Form 8300 receipts of currency that (alone or when combined with monetary instruments) exceed USD 10 000 whether in one transaction, or in two or more related transactions occurring over a 12 month period.
- c) Undertaking occasional transactions that are wire transfers: Banks and non-bank FIs are required to maintain records for wire-transfers of USD 3 000 or more: e.g. CFR §1020.410(a), CFR §1010.410 (e). This includes obtaining, verifying and retaining customer-related identification information.
- d) There is suspicion of ML/TF regardless of any exemption or thresholds: There are no CDD requirements specifically addressing additional or other CDD measures to be taken where there is suspicion of ML or TF beyond those addressed below.
- e) Doubts about veracity and adequacy of previously obtained customer identification data: CIP obligations for Covered FIs must include procedures for responding to situations in which they cannot form a reasonable belief that they know the customer's true identity. These procedures should describe: a) when the account should not be opened; b) the terms under which a customer may use an account while its identity is being verified; c) when the account should be closed after attempts to verify a customer's identity have failed; and d) when SARs

<sup>93</sup> The definition of *account* encompasses the concept of business relations: 31 CFR §1020.100(a)(1).



should be filed. In principle, this covers situations where covered FIs have doubts about the veracity and adequacy of previously obtained information. Covered FIs are also required to maintain effective internal controls under the BSA/AML compliance program rule, requiring them to maintain current customer information for meeting monitoring obligations. Other FIs are subject to less explicit, more general program requirements that do not address the element of doubt.

*Criterion 10.3* - The CIP must include risk-based procedures for identifying and verifying each customer's identity to the extent reasonable and practicable, subject to the minimum standards noted under c.10.1. The procedures must enable the **Covered FI** to form a reasonable belief that it knows the true identity of each customer, and be based on its risk assessment, including the type of account, method of account opening, identification information available to the Covered FI, and its size, location and customer base: e.g. 31 CFR §1020.220. Covered FIs subject to the CIP rule must implement a written program appropriate for their size and type of business, including procedures for customer identification and record-keeping. The CIP must also provide for risk-based verification, either through documents or non-documentary methods (e.g. comparing information from the customer with that from a consumer reporting agency, public database or similar source), or a combination of the two. For natural persons, documentary verification may be through a government-issued photo-identification document evidencing nationality or residence. For legal persons, a document evidencing the entity's existence (e.g. certified articles of incorporation, a partnership agreement or trust instrument) may be relied upon. There is an exemption from CIP for any account that a Covered FI acquires through an acquisition, merger, asset purchase or assumption of liabilities: e.g. §1020.100 (definition of *account*). **For MSBs**, requirements are not as detailed as for other Covered FIs and form part of the general program or record-keeping requirements. Foreign exchange dealers, as part of their record-keeping requirements, must verify customer identification at account opening (31 CFR §1022.410), maintain a record of each currency exchange over USD 1 000 regardless of amount, including the customer's name, address, passport/TIN/, date and amount of the transaction, currency name and country, and total amount of each foreign currency. **Life insurance companies** are required to have policies and procedures for obtaining all relevant customer-related information necessary for an effective AML program, integrate their agents and brokers into their AML program, and implement policies and procedures reasonably designed to detect suspicious activity from all relevant sources including from their insurance agents and insurance brokers: 31 CFR §§1025.210(b)(1) and 1025.320(a)(3)(i). However, neither insurers nor their agents or brokers are subject to a specific obligation under the BSA to verify the customer's identity using reliable independent source documents

*Criterion 10.4 - FIs (other than securities broker-dealers, FCMs and IBs)* are not explicitly required to verify that any person purporting to act on behalf of the customer is so authorized, or identify and verify the identity of that person. Whenever a CTR must be filed to report a cash transaction of more than USD 10 000, the FI is required to verify and record the name and address of the natural person presenting the transaction, and the identity, account number, and social security/TIN (if any) of any person/entity on whose behalf the transaction is undertaken: 31 CFR §1010.312. In addition, these FIs are expected (albeit not required) to identify and verify the identity of any person purporting to act on behalf of the customer, and verify the person is so authorized in accordance with sound

business practices. **Securities broker-dealers** are required to make a memorandum of each brokerage order, and any other instruction given or received for the purchase/sale of securities, including the identity of any other person who entered or accepted the order on behalf of the customer: 17 CFR §240.17a-3(a)(6). Every FINRA member is required to use reasonable diligence for opening and maintaining accounts, to know and retain the essential facts concerning every customer and concerning the authority of each person acting on the customer's behalf: FINRA Rule 2090. In the **derivatives sector**, **FCMs and IBs** are required to keep a record showing the true name and address of any person guaranteeing or exercising any trading control with respect to account: 17 CFR §1.37(a).

**Criterion 10.5 - Covered FIs** are required to obtain BO information only in limited specific circumstances: i) correspondent accounts that are payable-through accounts; and ii) private banking accounts for non-U.S. clients above USD 1 million in value<sup>94</sup>: 31 CFR §1010.610(b)(1)(iii) & 31 CFR §1010.620(b). *Beneficial owner* is defined as “an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, however, without any corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a BO”: §1010.605. The term excludes an individual who may have a financial interest in the account, but no corresponding ability to “control, manage or direct” it. **Securities broker-dealers** are required to make and keep current a record of each cash and margin account indicating, *inter alia*, the name and address of the account's BO: 17 CFR §240.17a-3(a)(9). However, where the account is held by a corporation, such records are required only in respect of the person(s) authorized to transact business for such accounts. In these circumstances, BO is defined as “the person who has or shares pursuant to an instrument, agreement or otherwise power to vote or direct the voting of a security” which is not in line with the FATF definition: 17 CFR §240.14b-2. The **life insurance sector** is not subject to requirements to identify and verify BOs.

**Criterion 10.6 - Covered FIs** are subject to the FFIEC Manual provision requiring them to obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. In addition, the Manual requires the CDD processes to include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g. change in employment or business operations). Similar obligations exist for **securities broker-dealers**: NASD Notice to Members 02-21, FINRA Rule 2090). There are no similar obligations in other financial sectors.

**Criterion 10.7 - Ongoing monitoring** to ensure compliance with the BSA reporting requirements, including monitoring for suspicious activity, is required by the AML program and SAR reporting rules.

- a) **Scrutinizing transactions: Covered FIs** are expected to have in place internal controls to “provide sufficient controls and monitoring systems for timely detection and reporting of

<sup>94</sup> Since the on-site, the Final CDD Rule that includes a BO requirement was published on 11 May 2016. The implementation period for the Rule is two years. (see <https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx>)

suspicious activity”: FFIEC Manual: pp. 33-34. Taken together, the AML programs and SAR requirements (including the expected risk assessment) require a general transaction monitoring and ongoing due diligence mechanism by covered FIs as well as MSBs.

- b) Keeping CDD data up-to-date: Covered FIs: The FFIEC Manual, CDD/Customer Risk section sets out the FBAs’ expectations for ongoing customer due diligence which appears to be broad enough, when considering “accounts”, to cover business relationships. The provisions address measures to monitor consistency of account use with expectations, and keeping information up to date. Under the BSA and the implementing regulations, each MSB must develop an effective AML program that is tailored to the risks inherent in its business depending on its customer base, location and market served, and types of services offered. It must be reasonably designed to ensure proper record-keeping and reporting, and prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities: 31 CFR. §1022.210. Its due diligence should be commensurate with the level of risk of its business. If an MSB's risk assessment indicates potential for a heightened risk of ML/TF, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk. Securities broker-dealers are required to maintain an account record for each account with a natural person as a customer or owner where the broker-dealer has been required to make a suitability determination. Broker-dealers are required to attempt to update these account records every 36 months: 17 CFR §240.17a-3(a)(17). Life Insurance Companies, other FIs: No explicit CDD provisions other than the general requirement to have an effective AML program.

*Criterion 10.8* - There is no specific obligation for **any category of FIs** to understand ownership and control structure of customers which are legal persons or legal arrangements.

*Criterion 10.9* - For customers which are legal persons/arrangements, **Covered FIs** are required to identify and verify the customer’s identity through the following information: name; principal place of business, local office or other location; and TIN. Verification procedures (which must be contained in CIP) may include documents showing the existence of the entity or arrangement (e.g. certified articles of incorporation, a government issued business license, a partnership agreement or trust instrument). Verification procedures need to be applied only to the extent reasonable and practicable and not in all cases: e.g. 31 CFR §1020.220(a)(2). AML program for MSBs should have verification procedures: 31 CFR §1022.210 (d)(1)(i)(A). Other sectors are not specifically covered.

*Criterion 10.10* - **Covered FIs** are required to implement measures, reasonably designed to identify and verify the identity of BOs of an account, as appropriate, based on the covered FI’s evaluation of the account’s risk: FinCEN, FBA and SEC guidance issued in 2010. In the context of this guidance and the corresponding provision in the FFIEC Manual, the definition of *beneficial owner* does not conform to the FATF standards. These measures are risk based and initially apply only in the circumstances determined by the Covered FIs. No elements cover situations where: there is doubt; or where no natural person exercises control through ownership or other means; or requiring the Covered FI to ascertain the identity of the most senior managing official. Covered FIs are also subject to a more limited obligation to identify and take reasonable measures to verify the identity of BOs of private banking accounts as described under c.10.5 above. Although covered FIs are under a separate and

more general obligation to take additional steps to verify the customer's identity by seeking information about individuals with authority or control over the account, including signatories, this requirement only applies when FIs cannot verify the identity of customers (and not the identities of their BOs) through documents or non-documentary methods: e.g. 31 CFR §1020.220(a)(2)(ii)(C). **MSBs and other FIs** conducting occasional transactions in amounts over USD 10 000 are required to collect and verify information identifying the natural person conducting the transaction (even if the transaction is initiated in the name of a legal entity) and the natural person on whose behalf the transaction is conducted. However, the "person conducting the transaction" is not necessarily the same as the BO as defined by the FATF. For **other FIs including life insurance companies**, no provisions apply other than the general requirement to have an effective AML program.

**Criterion 10.11 - Covered FIs** are not required to verify the identity of BOs (noting that in the U.S. as in other common law jurisdictions, legal arrangements are not entities). Covered FIs are required to obtain a document showing the legal arrangement's existence (e.g. the trust instrument): 31 CFR §1020.220(a)(2)(ii)(A)(2). Trust instruments usually show the names of the settlor, the trustee(s) and can also show named beneficiaries. The trustee, under U.S. trust law, holds title to the assets in a trust, but may share control with the settlor, depending on whether the trust is revocable or irrevocable. However, there are no explicit obligations to verify the identity of settlors, trustees, protectors (if any), the beneficiaries or classes of beneficiaries and any other natural persons exercising control over the trust property. The guidance referred to in c.10.10 states that "CDD procedures **may** include the following: (emphasis added): *Where the customer is a trustee, obtaining information about the trust structure to allow the institution to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.* In summary, this does not conform to the standard, and there are no explicit obligations to verify the identity of any parties to legal arrangements.

**Criterion 10.12** - State insurance law requirements provide as follows:

- a) Life insurance companies and insurance policies are regulated under State law. All States have governing legislation requiring life insurance companies to record the name of the beneficiary (where one is designated) of life insurance policies whether or not the policy has an investment component.
- b) The States have governing legislative requirements which require life insurance companies to be satisfied that they will be able to establish the identity of the beneficiary, if any, at the time the proceeds of the insurance policy become payable.
- c) In the U.S. a beneficiary of the proceeds of a life insurance policy cannot receive the proceeds until the insured person has died – the beneficiary has no other vested rights. Therefore this typology seems impracticable for ML, has not been observed in the U.S., and the assessors believe it represents a proven low risk. Accordingly this element of c.10.12 is not applicable in the U.S. context.

**Criterion 10.13 - FIs** are not required to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

*Criterion 10.14 - FIs* are not required to verify the identity of the customer and BO (as defined by the U.S.) before or during the course of establishing business relations or conducting transactions for occasional customers. Instead, FIs are required to verify the identity of their customers within a reasonable time after the account is opened: 31 CFR §1020.220 (depository institutions); 31 CFR §1023.220 (securities broker-dealers); 31 CFR §1024.220 (mutual funds), 31 CFR §1026.220 (FCMs and IBs) and CFR §1022.410 (dealers in foreign exchange). The flexibility to conduct verification procedures after establishing the relationship is not predicated upon the essential requirement of not interrupting the normal course of business. **MSBs** are required to collect, verify and retain customer/originator information for funds transfers of USD 3 000 and more prior to transactions: 31 CFR §1010.410. **Life insurance companies** are outside the purview of these requirements, but compensating contractual measures make the life sector a lower risk.

*Criterion 10.15 - A Covered FI's* CIP must include risk-based procedures for responding to circumstances in which it cannot form a reasonable belief that it knows the true identity of a customer including: i) when the FI should not open an account; ii) the terms under which a customer may use an account while verification of the customer's identity is being carried out; iii) when the FI should close an account after attempts to verify a customer's identity have failed; and iv) when a SAR should be filed in accordance with applicable law or regulation (e.g. 31 CFR 1020.220(a)(2)(iii)). Life insurance policies are usually activated when the insurer has collected enough data on the life insured. For **MSBs**, for transactions above USD 3 000, CDD is mandatory before a transaction takes place. There are no equivalent obligations in other financial sectors.

*Criterion 10.16 - Covered FIs* are required to apply CDD requirements to existing customers on the basis of materiality and risk. For CIP purposes, a customer is defined to specifically exclude a person who has an existing account with the covered FI provided that the institution has a reasonable belief that it knows the person's true identity: e.g. 31 CFR §1020.100(c)(2)(iii) for banks. Such FIs are required to have risk based procedures based on their assessment of the relevant risks, including those presented by the various types of accounts maintained, the various types of identifying information available, and their size, location and customer base: e.g. 31 CFR §1020.220(a)(2) for banks. In addition to the CIP requirements, **securities broker-dealers** are subject to additional record-keeping obligations pursuant to Exchange Act Rule 17a-3 and SRO customer protection and suitability rules that contain customer diligence requirements, which are not limited to new customers. For example, Exchange Act Rule 17a-3(a)(17) requires broker-dealers to maintain an account record including certain information for each account with a natural person as a customer or owner for which the broker-dealer is, or within 36 months has been, required to make a suitability determination: FINRA Rules 2090, 2111, 4512. In the **derivatives sector**, FCM members of NFA are required to contact their active customers (natural persons), at least annually, to verify that this information continues to be materially accurate, and provide the customer with an opportunity to correct and complete the information: NFA rule 2-30(b). No equivalent measures apply to the **life insurance sector**, although the general program rules apply to all customers of covered products, including existing customers.

*Criterion 10.17 -* The regulations addressing enhanced due diligence (EDD) differ in some respects across sectors, however, FIs are required in prescribed circumstances (USA PATRIOT Act Section 312 requirements applicable to certain correspondent accounts and private banking accounts) to perform EDD. Otherwise, **Covered FIs** are required to perform EDD where they assess the ML/TF



risks as high. The adequacy of their risk assessment and their EDD procedures are challenged by their supervisors. The FFIEC Manual contains extensive regulatory guidance on what could be considered high risk (with examples of EDD for high risk customers), and gives supervisors authority to impose a higher-risk rating where they do not agree that the FI has rated the risk correctly. The special measures required for correspondent banking arrangements address prescribed categories of higher-risk countries (see c.13.2). **Life insurance companies** are required to have policies, procedures and internal controls, based on their assessment of ML/TF risks associated with covered products, including the ability to obtain all relevant customer-related information necessary for an effective AML program: 31 CFR §1025.210. **MSBs** are required to have an AML program in place which is reasonably designed to prevent the MSB from being used to facilitate ML/TF, and commensurate with the risk posed.

*Criterion 10.18 - Not applicable.* The U.S. does not explicitly allow for simplified measures. For CDD and account monitoring, the regulations set baseline requirements with which FIs and DNFBPs must comply and which are based on the risks presented by their customers, products, services, etc. The baseline requirement must always be met, and cannot be simplified.

*Criterion 10.19 - FIs* are not explicitly required to terminate the business relationship if unable to comply with relevant CDD measures. However, the CDD expectations set out in the FFIEC Manual state that **covered FIs** should continue to review suspicious activity to determine whether other actions may be appropriate (e.g. management determining that it is necessary to terminate a relationship with the customer/ employee who is the subject of the filing). The CIP for Covered FIs must include procedures for responding to circumstances in which they cannot form a reasonable belief that they know the customer's true identity. These procedures should describe, *inter alia*, when the account should be closed after attempts to verify a customer's identity have failed, and when a SAR should be filed in accordance with applicable law and regulation: 31 CFR §1020.220(a)(2)(iii) (**depository institutions**), 31 CFR §1023.220(a)(2)(iii) (**securities broker-dealers**); 31 CFR §1024.220(a)(2)(iii) (**mutual funds**), 31 CFR §1026.220(a)(2)(iii) (**futures commission merchants & introducing brokers in commodities**). In the **life insurance sector**, insurance contracts may limit the ability of insurance companies to terminate policies or business relationships. With few exceptions, **MSBs** only offer occasional transaction services and have no flexibility under the relevant record-keeping, reporting, and AML program rules to allow a customer to commence business relations or perform a transaction if the required customer identification and transaction information cannot be collected.

*Criterion 10.20 -* As discussed in R.20, Federal law requires **FIs** to file a SAR when suspicious activity is detected, and prohibits them from disclosing to any person involved in the suspicious transaction that a SAR has been filed. Although there is no specific provision in the law, this prohibition has been interpreted broadly enough to cover situations in which an FI does not pursue the CDD process and instead files a SAR when it forms a suspicion of ML/TF and reasonably believes that performing the CDD process will tip-off the customer.



*Weighting and Conclusion:*

Lack of CDD requirements to ascertain and verify the identity of BO (except in very limited cases) is a significant shortcoming. IAs are not directly covered by BSA obligations. Some IAs, however, are indirectly covered through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements. Other important gaps are that FIs (other than in the securities and derivatives sectors) are not explicitly required to identify and verify the identity of persons authorized to act on behalf of customers, and some FIs are not explicitly required to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship. FIs are not required to understand the ownership and control structure of customers that are legal persons/arrangements.

**Recommendation 10 is rated partially compliant.**

**Recommendation 11 – Record-keeping**

In its 3rd MER, the U.S. was rated largely compliant with these requirements. The main technical deficiency was that life insurers of covered products were only required to keep limited records of SARs, Form 8300, their AML program and related documents.

**Criterion 11.1 - FIs** are required to maintain records on transactions for at least five years following completion of the transactions. The *Bank Secrecy Act* contains a number of statutory record-keeping requirements: e.g. 12 USC §1829b (for **banks and money transmitters**), 31 USC §5311 (all **financial institutions**), 31 USC §5318(l) (for customer identification programs), 31 USC §5325 (for purchases of monetary instruments) and 31 USC §5326 (for GTOs). Additionally, sector specific record-keeping requirements have been prescribed in numerous implementing regulations as well as the in the respective parent Act, wherever applicable: e.g. 31 CFR §1010.410. See e.g. 31 CFR §1020.410(a) & (c) (for **banks**), 31 CFR §1023.410 & Rule 17a-3 under the *Securities Exchange Act of 1934* (for **securities broker-dealers**); 31 CFR §1022.410 (for **foreign exchange dealers**); 31 CFR §1022.210 & 1022.420 (for **providers and sellers of prepaid access**). Record-keeping requirements for **FCMs and IBs** are also elaborate and seem to cover the requirements. **GSEs and RMLOs** are subject to AML program and separate record-keeping requirements: 31 CFR §1030.320(c) for housing GSEs; and 31 CFR §1029.320(c) for RMLOs. **Life insurance companies** are subject to SAR obligations which include a record-keeping component: 31 CFR §1025.320(d). These provisions are comprehensive and also at times duplicative and complex. In some cases, a threshold triggers the record-keeping requirement (e.g. transmittal of funds by non-bank FI for USD 3 000 or more and sale of bank checks/drafts, cashier checks, among others by FIs for more than USD 3 000). Persons who file a Form 8300 must retain a copy of each filed Form for five years from the date of filing. Generally records need to be made available upon request to FinCEN and any designated authority/other sectoral regulators.

**Criterion 11.2 - FIs** are required to obtain CIP and related client identifying information and supporting documents. At a minimum, these include all identifying information about a customer (e.g. name, date of birth, address, and TIN) and documents relied upon to verify the identity (e.g. driver's license/passport for individuals; articles of association, business license, corporate charter,

partnership agreement etc. for legal persons, and trust instrument for legal arrangements). The record retention period for customer identifying information (e.g. name, date of birth, address etc.) is five years after closing the account, or in the case of credit card accounts at banks, after the account becomes closed or dormant. Transaction records for occasional transactions are required to be maintained for five years after the date of the transaction record is made. There is a limited five-year retention requirement for account files, business correspondence and results of any analysis conducted by FIs related to SAR filings, noted below. The foregoing applies to FIs with a CIP obligation: **banks, securities broker dealers, mutual funds, and FCMs and IBs** 31 CFR §1020.220; 31 CFR §1023.220; 31 CFR §1024.220; 31 CFR §1026.220. To the extent that certain account files, business correspondence and results of analysis are supporting documentation for a SAR, **banks, broker-dealers, FCMs and IBs, housing government-sponsored enterprises, insurance companies, loan or finance companies, money services businesses, and mutual funds**, are required to retain these records for five years following the date of the filing of the SAR. See **Banks**: 31 CFR §1020.320(d); **Futures commission merchants and introducing brokers in commodities**: 31 CFR §1026.320(d); **Housing government-sponsored enterprises**: 31 CFR §1030.320(c); **Insurance companies**: 31 CFR §1025.320(d); **Loan or Finance Companies**: 31 CFR §1029.320(c); **Money services businesses**: 31 CFR §1022.320(c); **Mutual funds**: 31 CFR §1024.320(c); **Securities broker-dealers**: 31 CFR §1023.320(d). Additionally, Exchange Act Rule 17a-4 requires a broker-dealer to maintain all communications received and copies of all communications sent, as well as all written agreements (or copies thereof), that relate to the broker-dealer's "business as such" for three years (the first two years in an easily accessible place): 17a-4(b)(4) and (b)(7). Also, all account record information required pursuant to §240.17a-3(a)(17) must be maintained until at least six years after the earlier of the date the account was closed or the date on which the information was replaced or updated: 17a-4(e)(5). **MSBs** must collect the customer's name, address, and date of birth, occupation, and TIN for each reportable currency transaction: 31 CFR §1010.410.

*Criterion 11.3* - Transaction records are quite comprehensive and detailed and seem sufficient to allow reconstruction of individual transactions for evidentiary purposes: 31 CFR Chapter X. However, the gaps noted under R.10 could inhibit some reconstruction of individual transactions activity.

*Criterion 11.4* - **FIs** must make records available upon request to FinCEN and any agency exercising delegated authority. Records must be filed or stored in such a way as to be accessible within a *reasonable* period of time, taking into consideration, the nature of the record and the amount of time expired since the record was made: 31 CFR §1010.430(d). In discussions with competent authorities, the question of timeliness of compliance with information requests was not an issue. **Broker-dealers** are required to furnish copies of their records promptly to a representative of the SEC and FINRA upon request: *Exchange Act*, Rule 17a-4(j) and FINRA Rule 8210. All books and records that must be kept by the *Commodity Exchange Act* or its implementing regulations must be made available for inspection by any representative of the CFTC or the DOJ: 17 CFR §1.31(a)(1)-(2). **IAs** are required to furnish copies of their records promptly to a representative of the SEC upon request: *Advisers Act*, Rule 204-2(g). In addition, and as a condition to regulatory relief provided by SEC staff (in consultation with FinCEN staff), **IAs** that have entered into certain CIP reliance relationships with broker-dealers, must agree to, among other things, promptly provide its books and records relating

to its performance of the CIP to the Commission, to a SRO that has jurisdiction over the broker-dealer, or to authorized law enforcement agencies, either directly or through the broker-dealer, at the request of (i) the broker-dealer, (ii) the Commission, (iii) a SRO that has jurisdiction over the broker-dealer (FINRA), or (iv) an authorized law enforcement agency.

### *Weighting and Conclusion:*

There are minor gaps including; no specific record retention requirement for account files, business correspondence and results of any analysis conducted by FIs in general, and existence of thresholds for triggering the record-keeping requirement.

**Recommendation 11 is rated largely compliant.**

### **Recommendation 12 – Politically exposed persons**

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements as PEPs measures did not explicit apply to MSBs, life insurance sector, investment advisers and commodity trading advisers. The 2012 Recommendations have been extended to domestic PEPs and international organizations.

**Criterion 12.1 - Covered FIs** are subject to special standards of due diligence when dealing with senior foreign political figures in the context of *private banking accounts*<sup>95</sup>: s.312 USA PATRIOT Act, §1010.620. Covered FIs are required to take reasonable measures to ascertain the identity of all the nominal and beneficial owners (BO) of such accounts, and ascertain whether any of them is a *senior foreign political figure*. However, although “senior foreign political figure” is defined broadly in line with the FATF definition of *foreign PEP*, the U.S. definition of BO does not meet FATF standards as noted under R.10. If the direct owner or BO is a foreign PEP, Covered FIs must: ascertain the source of funds deposited into the account and the account’s purpose and expected use; and conduct enhanced scrutiny of the account. The FFIEC Manual expands regulatory expectations beyond the parameters set in the BSA and requires Covered FIs to take risk-based measures to determine if PEPs open accounts at Covered FIs. The Manual also generally requires developing PEP-related policies which include involving bank management in decisions to accept or retain PEPs accounts, and evaluations of the risks and appropriate steps to be taken, if it becomes known subsequently that the customer is a PEP: p.290-295. No specific PEPs requirements apply to **MSBs and the life insurance sector**, other than the broader due diligence requirements set out in the AML program requirements.

**Criterion 12.2** - Domestic and international organization PEPs are not explicitly covered.

**Criterion 12.3** - The requirements of c.12.1 apply to family members and close associates of foreign PEPs but not those of domestic or international organization PEPs: 31 CFR §1010.605(p).

**Criterion 12.4 - Life insurance companies** are not subject to specific PEPs requirements.

<sup>95</sup> A *private banking account* is defined as an account (or combinations of accounts) at FIs requiring a minimum aggregate deposit of funds/other assets of USD 1 million which are for the benefit of one or more non-U.S. persons who are the direct or beneficial owners of the account and are administered by a person at the FI who acts as a liaison between the FI and the direct or beneficial owner(s).

*Weighting and Conclusion:*

All investment advisers, MSBs and life insurance companies are not covered. Other significant shortcomings are that domestic and international organizations PEPs are not covered.

***Recommendation 12 is rated partially compliant.***

***Recommendation 13 – Correspondent banking***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiency was not requiring senior management approval when opening individual correspondent accounts.

**Criterion 13.1 - Each FI** establishing, maintaining, administering, or managing a correspondent account in the U.S. for a foreign FI is required to establish appropriate, specific, and (where necessary) EDD policies, procedures, and controls that are reasonably designed to detect and report instances of ML through those accounts: s.312, USA PATRIOT Act which amended BSA through insertion of sub-section (i) to 31 USC §5318. FinCEN published a final regulation implementing the due diligence provisions applicable to covered FIs: 31 CFR §1010.610. As per the implementing regulation, policies, procedures and controls shall include: (a) the nature of the foreign FI's business and the markets it serves; (b) the type, purpose, and anticipated activity of such correspondent account; (c) the nature and duration of the covered FI's relationship with the foreign FI and any of its affiliates; (d) the AML and supervisory regime of the home jurisdiction and (to the extent that information regarding such jurisdiction is reasonably available) of the jurisdiction in which any company owning the foreign FI is incorporated or chartered; and (e) information known or reasonably available to the covered FI about the foreign FI's AML record. The regulation also requires EDD in certain cases (e.g. foreign banks holding off-shore banking licenses, or licenses issued by non-cooperative jurisdictions, or jurisdictions otherwise designated as warranting special measures). Supervisory guidelines and expectations on correspondence banking are set out in the FFIEC Manual: pp.177-180. The FFIEC Manual further describes record-keeping, reporting and due diligence examination procedures: pp.111-124. However there is no specific requirement to obtain senior management approval before opening a new correspondent account, or to determine the foreign bank's reputation or quality of its AML controls and supervision. As part of their AML program, however, banks must have senior management-approved account opening policies and procedures, including for correspondent accounts: FFIEC Manual p. 178.

**Criterion 13.2 -** Certain foreign banks must be subject to EDD, including obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (PTA), and the sources and beneficial owner (BO) of funds/other assets in the PTA: Implementing Regulation 31 CFR §1010.610(b)(1)(iii)(A). The FFIEC Manual further provides that U.S. banks offering PTA services should develop and maintain adequate policies, procedures, and processes to guard against possible illicit use of these accounts: p.195. At a minimum, policies, procedures, and processes should enable each U.S. bank to identify the ultimate users of its foreign FI's PTAs and should include the bank's obtaining (or having the ability to obtain through a trusted third-party arrangement) substantially the same information on the ultimate PTA users as it obtains on its direct customers.

*Criterion 13.3* - Covered FIs are prohibited from establishing, maintaining, administering or managing correspondent accounts in the U.S. for, or on behalf of, foreign shell banks and are required to take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed in the U.S. for a foreign bank is not being used by that foreign bank to indirectly provide banking services to a foreign shell bank: s.313 USA PATRIOT Act 31 USC 5318(j), 31 CFR §1010.630(a). Separately, the FFIEC Manual outlines procedures for assessing banks' compliance with statutory and regulatory requirements prohibiting correspondent accounts for foreign shell banks: p.111.

#### *Weighting and Conclusion:*

There is no specific requirement to obtain senior management approval before opening a new correspondent account, or to make a determination of a correspondent's reputation or quality of its AML controls and supervision.

***Recommendation 13 is rated largely compliant.***

#### ***Recommendation 14 – Money or value transfer services***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. Compliance in this area was reduced by technical deficiencies in other areas (CDD measures, new technologies and non-face-to-face-business, and suspicious transaction reporting).

*Criterion 14.1* - MVTS providers, both formal and informal and are subject to BSA requirements as MSBs, including registration with FinCEN: 31 USC§5330, 31 CFR §1022.380. Regulations provide for biennial renewal and re-registration processes (in certain limited cases like change in ownership or control, or more than 50% increase in agents). Additionally, 47 of the 50 States (except Montana, New Mexico and South Carolina)<sup>96</sup>, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands have separate MSB licensing requirements.

*Criterion 14.2* - Any person failing to comply with the registration requirements may be liable for a civil penalty of up to USD 5 000 for each violation. Each day a violation continues constitutes a separate violation. The Secretary of the Treasury may also bring a civil action to enjoin the violation: 31 USC §5330(e), 31 CFR §1022.380(e). It is unlawful to do business without complying with the registration requirements. A criminal fine and/or imprisonment for up to five years may be imposed. Failure to comply with State requirements or FinCEN registration is criminalized: 18 USC §1960(b)(1)A/B. To address unregistered money transmitters, the IRS Stakeholder Liaison Group conducted unregistered MSB outreach from 2006 to 2010, when the effort was taken up by FinCEN as one of its priorities. FinCEN has also taken civil enforcement actions against MSBs engaged in serious violations of their AML/CFT obligations, including failing to register with it.

*Criterion 14.3* - MVTS are regulated as MSBs and subject to monitoring for AML/CFT compliance.

<sup>96</sup> Since the date of on-site, authorities reported that MSBs in New Mexico and South Carolina are now covered under licensing regime as per the legislative amendments in these states.



*Criterion 14.4* - MVTs are required to prepare and maintain a list of their foreign and domestic agents, which must be revised each January 1 for the preceding 12-month period: 31 CFR1022.380 (d). A copy of the initial agent list and each revised list must be retained for five years. The list generally includes details such as agent's name, contact details, type of services offered, gross transaction amount, details of the depository institution where the agent maintains transaction accounts, branches and sub-agents if any. It must be made available to FinCEN and other LEAs upon request.

*Criterion 14.5* - MVTs are required to develop, implement, and maintain an effective AML program reasonably designed to prevent their operations from being used to facilitate ML/TF: 31 CFR§1022.210(a). MSBs must require their agents to implement appropriate systems and controls. While there is no formal requirement to monitor agent compliance, the regulatory expectation is that such monitoring will occur: MSB Examination Manual p.15-16 & 50-51. For MSBs using foreign agents or counterparties, the AML program must include risk-based policies, procedures, and controls designed to identify and minimize ML risks associated with foreign agents/counter parties that facilitate the flow of funds into and out of the U.S.: FinCEN Interpretive Release 2004-1 at Appendix H of the MSB Manual. FinCEN, the IRS and most States have examination authority over MSB agents. FinCEN has direct enforcement authority over agents.

#### *Weighting and Conclusion:*

There are no formal agent monitoring requirements for MSBs.

***Recommendation 14 is rated largely compliant.***

#### ***Recommendation 15 – New technologies***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant. The main technical deficiency was that there was no explicit provision requiring life insurers, MSBs or investment advisers and commodity trading advisors to have policies and procedures for non-face-to-face-business relationships or transactions.

*Criterion 15.1* - In the NMLRA the potential misuse of digital currency, domestic and foreign prepaid products, remote deposit capture of checks, and third party payment processors are reviewed with case examples and studies illustrating vulnerabilities and typologies. The laws governing the establishment of AML programs in the financial sector, and the FFIEC Manual generally require FIs to take into account all relevant factors into consideration, including the associated risks presented by products and services, new delivery mechanisms and the risks presented by new technology.

*Criterion 15.2 - Covered FIs and MSBs*, when developing and implementing an AML program, are required to incorporate policies, procedures, and internal controls based the institution's assessment of the ML/TF risks associated with its unique combination of products, services, customers, and geographic locations. The MSB and FFIEC Examination Manuals provide an extensive set of expectations governing the risk assessment process, including detailed expectations on the risks associated with products and services. The model AML Program template FINRA developed for use by small firms stipulates that the firm should identify its ML/TF risks based on "*the type of customers it serves, where its customers are located, and the types of products and services it*



offers.”(See [link](#)). **Life Insurance companies**, when developing and implementing an AML program, are required to incorporate policies, procedures, and internal controls based upon their assessment of the ML/TF risks associated with covered products: 31 CFR §1025.210. Furthermore, enforcement actions illustrate the obligation in the AML Program rule and supporting guidance that FIs include risks associated with new products, practices, and services in their AML risk assessments and AML policies and procedures, and the use of new or developing technologies for new and pre-existing products.

### *Weighting and Conclusion:*

Not all investment advisers are covered. There are no explicit requirements for FIs to address the risks presented by new technologies. However, the NMLRA does address risk related to new technology, and some measures in place in the FFIEC Manual relating to new products and services are frequently interpreted by FIs and supervisors to address the risk of new technologies, and some enforcement measures reflect this.

**Recommendation 15 is rated largely compliant.**

### **Recommendation 16 – Wire transfers**

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The main technical deficiencies were a threshold of USD 3 000 (instead of USD 1 000 as required by the FATF standards) and no obligation to include all required originator information on batch transfers. The FATF standards in this area have since been expanded to include requirements relating to beneficiary information.

**Criterion 16.1** - Ordering and intermediary FIs located within the U.S. are required to include the originator’s name, account number and address in any transmittal order above USD 3 000: 31 CFR §1010.410(f). There is no explicit obligation to include a unique transaction reference number in the absence of account. Ordering FIs are required to verify the identity of the originator, and include the following beneficiary information with transmission order: (a) the identity of the beneficiary’s FI and as many of the following items as are received with the payment order: (i) the beneficiary’s name and address; (ii) account number; and (iii) any other specific identifiers of the beneficiary: 31 CFR §1010.410(f). This does not meet c.16.1 which requires both the name of the beneficiary, and either the account number or a unique transaction reference number. The USD 3 000 threshold applies to all the above requirements.

**Criterion 16.2** - The National Automated Clearing House Association (NACHA) develops the interbank electronic batch transfer payment system operating rules. These rules require that all international ACH transactions comply with its new International ACH Transaction (IAT) format. Each IAT entry includes the originator’s name and physical address (including street address, city, State/province, country and postal code), originator identification information (which may include the originator’s account number), and the originating bank name, routing number and branch country code. The same information is required for the beneficiary and beneficiary bank. The rules also require the identification of the ultimate foreign beneficiary of the funds transfer for inbound IAT debits and the foreign party funding when that party is not the originator for inbound IAT credits. The Reserve

Banks, in their operation of an ACH service, largely incorporate NACHA's rules in their Operating Circular 4 (and EPN, the private sector ACH operator, does the same in its operating rules). As a result, the incorporated NACHA rules become a contract between the operators (the Reserve Banks and EPN) and their customers (which includes all banks that originate or receive ACH payments). To the extent a bank does not comply with NACHA rules as incorporated in Operating Circular 4 or EPN's operating rules, the respective operator has a contractual claim against the bank and may take actions as allowed under Operating Circular 4 or EPN's operating rules.

*Criterion 16.3* - Record-keeping and information transmittal requirements for wire transfers by banks and non-bank FIs are subject to a USD 3 000 threshold: 31 CFR §1020.410 (for banks), 31 CFR §1010.410 (for non-bank FIs), below which there are no requirements.

*Criterion 16.4* - While FIs (including MSBs) are always required to verify customer identification when facilitating a funds transfer of USD 3 000 or more, there is no requirement to verify identity where a suspicious transaction below the relevant threshold occurs.

*Criterion 16.5* - For domestic wire transfers above the USD 3 000 threshold, all of the requirements described in c.16.1 apply, albeit with the same deficiencies. No requirements apply to wire transfers below that threshold.

*Criterion 16.6* - Subject to the applicable threshold, domestic transfers above the USD 3 000 threshold are subject to the same requirements as for international transfers.

*Criterion 16.7* - Subject to the USD 3 000 threshold, FIs are required to obtain and retain: the originator's name and address; the amount and execution date of the transmittal order; any payment instructions received from the originator with the transmittal order; the identity of the beneficiary's (recipient's) FI; any form relating to the transmittal of funds completed or signed by the person placing the transmittal order; and as many of the following items as are received with the transmittal order—the beneficiary's name, address, and account number, and any other specific identifier of the beneficiary: 31 CFR §§1020.410(a), 1010.410 (e). These records must be kept for five years: 31 CFR §1010.430(d). No thresholds apply to securities brokers who are required to make and preserve records of all receipts and disbursements of cash and all other debits/credits: 17 CFR §240.17a-3 and 240.17a-4.

*Criterion 16.8* - Subject to the applicable threshold and the deficiencies noted in c.16.1, before executing a wire transfer, ordering FIs are required to collect, retain, and transfer information as specified above at criteria 16.1-16.7. But the prohibition on executing the wire transfer if these requirements are not met is not explicit.

*Criterion 16.9* - Intermediary FIs are required to record and to transmit the same information as ordering FIs: 31 CFR §1010.410(f).

*Criterion 16.10* - Before sending a transmittal order to the Federal Reserve Bank or otherwise converting to the expanded Fedwire message format, an intermediary FI is deemed in compliance if it includes in the transmittal order certain information, and retains and provides the remaining required information upon request of another intermediary FI or the beneficiary FI. The intermediary FI is required to keep such information for five years: CFR §1010.410(f)(3).

*Criterion 16.11* - Intermediary FIs are only required to take reasonable measures to identify cross-border wire transfers lacking required information or containing information that may indicate the wire violates U.S. targeted financial sanctions. Non-enforceable guidance issued jointly by the U.S. FBAs in 2009 on the potential misuse of cover payments advised that: “banks should have as part of their monitoring processes, a risk-based method to identify incomplete fields or fields with meaningless data U.S. banks engaged in processing cover payments should have policies to address such circumstances in connection with risk management for correspondent banking services, and should within reasonable timeframes develop and implement plans for adapting automated monitoring systems”: p.3.

*Criterion 16.12* - Intermediary FIs are not explicitly required to determine when to reject or suspend an incoming wire transfer for lack of information, but would be expected to file a SAR. An outgoing wire would be subject to the travel/record-keeping rules and would have to have the required information. The BSA requires covered FIs to establish AML compliance programs which are reasonably designed to comply with the record-keeping and reporting requirements of the BSA and its implementing regulations. These require FIs to implement systems of internal controls to ensure ongoing compliance.

*Criterion 16.13* - FIs are required to have appropriate controls and systems in place to identify and monitor suspicious activity and ensure necessary compliance. Appropriate controls include measures to assure and monitor compliance with record-keeping and reporting requirements including internal control systems to identify and monitor for suspicious activity. Such controls may include post- or real time monitoring of funds transfers to identify cross-border wire transfers or international ACH transactions lacking required originator or beneficiary information that may indicate suspicious activity.

*Criterion 16.14* - When paying out wire transfers over the USD 3 000 threshold in person to the beneficiary, its representative or agent, beneficiary FIs are required to verify the identity of the person receiving the payment, and obtain and retain a record of the person’s name, address, type of identification reviewed, and TIN (or, if none, alien identification number, or passport number and issuing country, or make a notation in the record about the lack thereof). If the beneficiary FI has knowledge that the person receiving the proceeds is not the beneficiary, the beneficiary FI must obtain and retain a record of the beneficiary’s name, address, and TIN (or, if none, alien identification number, or passport number and issuing country if known by the person receiving the proceeds, or make a notation in the record about the lack thereof). If the payment is delivered other than in person, the beneficiary FI shall retain a copy of the check/other instrument used to effect payment, or the information contained thereon, and the name and address of the person to which it was sent.

*Criterion 16.15* - An FI’s risk assessment (generally based on type or identity of customer, type of service/product, and applicable geographies served) must determine whether, as part of the mitigation procedures specified in its AML program, the FI should reject or delay transmittal order/payment order lacking complete information, or implement additional follow up procedures. However there are no explicit obligations pertaining to executing, rejecting or suspending wire transfers or taking follow-up action that are not subject to OFAC sanctions.

*Criterion 16.16* - Record-keeping and wire transfer obligations in 31 CFR 1010.410 (subject to USD 3 000 threshold) apply to MVTs providers, located within the U.S., whether operating directly or through their agents.

*Criterion 16.17* - MSBs are required to develop, implement, and maintain effective AML programs reasonably designed to prevent them from being used to facilitate ML/TF activities: 31 CFR §1022.210(a). The program must incorporate policies, procedures, and controls reasonably designed to assure compliance with the BSA and implementing regulations. However, they are not required to: take into account all the information from both the ordering and beneficiary sides in order to determine whether an SAR has to be filed; or file an SAR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the FIU.

*Criterion 16.18* - It is a criminal offense for U.S. persons to provide material support or assistance to foreign terrorist organizations (FTOs), and FIs are required to block all funds in which FTOs or their agents have an interest. The U.S. implements and enforces its obligations under the relevant UNSCRs, including UNSCRs 1267 and 1373, through E.O. 13224, as described in R.6.

#### *Weighting and Conclusion:*

Requirements apply subject to a USD 3 000 threshold for both domestic and international wire transfers and not below the threshold. Other shortcomings: there are no explicit requirements to include all the originator and beneficiary information in the transmittal order; to verify originator and beneficiary information below the threshold in case of suspicion of ML/TF; for MSBs to consider information from both the ordering and beneficiary sides for SAR determination; and for intermediary or beneficiary FIs on executing, rejecting or suspending transactions due to lack of required information.

***Recommendation 16 is rated partially compliant.***

#### ***Recommendation 17 – Reliance on third parties***

In its 3<sup>rd</sup> round MER, the U.S. was rated largely compliant with these requirements. Deficiencies noted were: no explicit obligation on relying institution to obtain core information from introducer and no measures applied to investment advisers, commodity trading advisors or the life insurance sector. There have since been some changes to the FATF standards in this area.

*Criterion 17.1 - FIs* with a CIP requirement may rely on another FI (including an affiliate) to perform any procedures of the CIP under specific conditions notably that: (i) such reliance is reasonable under the circumstances; (ii) the other FI is required to establish and maintain an AML program and is regulated by a Federal functional regulator; and (iii) the other FI enters into a contract requiring it to certify annually to the relying institution that it has implemented its AML program, and will perform the specified requirements of the relying institution's CIP: 31 CFR§1020.220(a) (6) (***banks***), 31 CFR§1023.220(a)(6) (***securities broker-dealers***), 31 CFR §1024.220(a)(6) (***mutual funds***), 31 CFR§1026.220(a)(6) (***futures commission merchants and introducing brokers in commodities***). While there are no specific obligations on relying FIs to immediately obtain core CDD information from the FI they are relying upon as required under standards, the relying FIs remain responsible for

providing that information at any moment. Third party reliance by MSBs is not applicable as they do not provide account based services. **Life insurance companies** are required to establish and implement policies and procedures reasonably designed to obtain customer related information from insurance agents and insurance brokers for meeting their SAR obligations: 31 CFR§ 1025.320(a)(3).

*Criterion 17.2* - The law does not allow reliance on FIs not regulated by a U.S. regulator, including foreign branches of U.S. banks which are regarded as foreign banks for BSA purposes.

*Criterion 17.3* - There are no separate and special reliance procedures for third parties that are part of the same group. Hence, the conditions applicable in other cases (as described under c.17.1) apply in such circumstances as well.

### *Weighting and Conclusion:*

Not all investment advisers are covered. There is one minor shortcoming: no specific obligations on relying FIs to immediately obtain core CDD information from the relied upon FI.

**Recommendation 17 is rated largely compliant.**

### **Recommendation 18 – Internal controls and foreign branches and subsidiaries**

In its 3<sup>rd</sup> round MER, the U.S. was rated largely compliant with these requirements. Technical deficiencies were: AML program requirements did not apply to certain non-federally regulated banks, investment advisers and commodity trading advisors; there was no obligation under the BSA for FIs to implement employee screening procedures; and the BSA requirements did not apply to the foreign branches and offices of domestic life insurers issuing and underwriting covered life insurance products.

*Criterion 18.1* - Covered FIs are required to establish AML programs, including, at a minimum: a) developing internal policies, procedures and controls; b) designating a compliance officer sufficiently senior to assure compliance with all obligations under the BSA; c) have an ongoing employee training program; and d) have an independent compliance function to test programs: s.352, USA PATRIOT Act. **Each of the FBAs** has regulations prescribing that the compliance programs should, at a minimum, cover the following elements: a) a system of internal controls to assure ongoing compliance with the BSA; b) independent testing for compliance; c) a designated individual(s) responsible for coordinating and monitoring BSA/AML compliance; and d) training for appropriate personnel. Similar requirements apply in the **securities and derivatives** sector: 31 CFR §1024.210 for **mutual funds**, 31 CFR§1023.210 for **broker-dealers** (which are also subject to applicable SRO rules), and 31 CFR §1026.210 for **FCMs, and IBs** in derivative sector. Generally, these provisions require FIs to address risks as part of these programs. **Covered FIs that have deposit insurance** are prohibited from hiring any person who has been convicted of (or agreed to enter into a pre-trial diversion or similar program in connection with a prosecution for) a criminal offense involving dishonesty, breach of trust or ML: 12 USC §1829. In the **securities sector**, broker-dealers must have specific employees fingerprinted and submit the fingerprints to the U.S. Attorney General or its designee for identification and appropriate processing: 17 CFR §240.17f-2. Moreover, federal



law and SRO rules subject persons associated with broker-dealers to disqualification from the industry upon the occurrence of enumerated events, such as certain criminal convictions, or a finding that the individual has willfully violated the federal securities laws: Section 3(a)(39) and Rule 19h-1 of the Securities Exchange Act of 1934. **MSBs** are required to have an effective and commensurate AML program reasonably designed to prevent ML/TF which covers designating a compliance officer, training and independent review: 31 CFR §1022.210. **Life insurance companies** (which are required to integrate insurance brokers and agents in their AML program) are subject to the four broad elements as stated above in detail: 31 CFR §1025.210.

*Criterion 18.2* - For banks, the FFIEC Manual sets out enforceable expectations on consolidated BSA/AML programs addressing both domestic and foreign subsidiaries. **For MSBs**, there are provisions for agreements between agents and principals relating to their AML programs.

*Criterion 18.3* - **Foreign branches and offices of U.S. banks** are required to: have policies, procedures, and processes in place to protect against ML/TF risks; be guided by the U.S. bank's BSA/AML policies, procedures, and processes; and meet all local AML-related laws, rules and regulations: FFIEC Manual p.164-167. Their BSA compliance programs should ensure that all affiliates (including those operating within foreign jurisdictions) meet the applicable regulatory requirements. The **life insurance sector** is similarly bound by BSA/AML obligations, and would also be expected to have policies, procedures, and processes to address ML/TF risks as per their AML program rule obligations. While there is no explicit obligations to inform the home supervisors if host country does not permit proper implementation of AML/CFT measures, banks are required to take appropriate measures and provide supervisors with any information deemed necessary to assess compliance with U.S. banking laws. In higher risk situations, supervisors can also direct banks to take additional measures, including closing the foreign office.

### *Weighting and Conclusion:*

Not all investment advisers are covered and there is no explicit obligation to inform the home supervisors if host country does not permit proper implementation of AML/CFT measures.

**Recommendation 18 is rated largely compliant.**

### **Recommendation 19 – Higher-risk countries**

In its 3<sup>rd</sup> round MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies were that there was no specific requirement in the life insurance sector to establish and retain written records of transactions with persons from/in countries not (or insufficiently) applying *the FATF Recommendations*, and no measures applied to investment advisers and commodity trading advisors. There have been some changes to the FATF standards in this area.

*Criterion 19.1* - **Banks, securities broker-dealers, mutual funds, FCM and IB** are required to apply EDD to correspondent accounts established or maintained in the U.S. for certain categories of foreign banks in the following circumstances: a) foreign banks licensed by a foreign country designated as non-cooperative with international AML principles by an intergovernmental group with which the U.S. concurs (e.g. the FATF); b) offshore banking licenses; and c) a banking licence issued by a foreign



country designated by the Secretary as warranting special measures to address ML concerns: USA PATRIOT Act, s.312, Regulation 31 CFR §1010.610. Such measures may include enhanced scrutiny, monitoring of transactions, obtaining and considering information on AML program of foreign banks, obtaining ownership information about the bank, etc. Such measures apply to establishing and maintaining correspondent accounts, which are defined as “an account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution”: 31 USC § 5318A(e)(i)(B). This definition is broad enough to include “business relationship” with such a foreign bank, given the inclusion in the definition of related financial transactions with such foreign bank. Although the statutory authority is limited to “foreign banks licensed by a foreign country designated as non-cooperative” (as noted above), in practice FinCEN issues an advisory after each FATF Plenary meeting alerting U.S. FIs to the expectations of the FATF regarding jurisdictions subject to any scrutiny by the FATF, whether they are cooperative or not, and these advisories are enforceable pursuant to 31 CFR 1010.610 and 31 USC 5318(h)(1) and its implementing regulations.

*Criterion 19.2* - The U.S. is able to apply countermeasures. The Secretary of the Treasury is authorized under Section 311 of the USA PATRIOT Act (31 USC 5318A) to designate a foreign jurisdiction, institution, class of transaction, or type of account as being of *primary money-laundering concern*, and to impose one or more of five special measures (record-keeping on and reporting of certain transactions; collecting information relating to beneficial ownership; collecting information relating to certain payable-through accounts; collecting information relating to certain correspondent accounts; and prohibitions or conditions on opening/maintaining correspondent or payable-through accounts). The authority to take such action has been delegated to the Director of FinCEN. These special measures can be imposed individually, jointly, or in any combination and in any sequence. The U.S. has relied on this authority in several instances including Iran, DPRK, Nauru, Burma and Ukraine (see [link](#)). These countries were under countermeasures at the time the U.S. invoked Section 311 against them and these Section 311 findings cite the AML/CFT deficiencies identified by FATF. The U.S. may also deny a foreign bank from opening a branch, subsidiary or representative office due to significant AML concerns: 12 CFR §211.24(c).

*Criterion 19.3* - The U.S. has a number of channels to advise FIs about concerns in the AML/CFT systems of other countries: PATRIOT Act s.312. These include alerts and advisories, secured websites maintained by Federal banking agencies, International Narcotics Control Strategy Report (INCSR), OFAC Sanctioned Countries and SDNs and other publications.

### *Weighting and Conclusion:*

Not all investment advisers are subject to the requirements. EDD measures do not apply to business relationships and transactions with natural persons in general from such jurisdictions.

***Recommendation 19 is rated largely compliant.***

### ***Recommendation 20 – Reporting of suspicious transaction***

In its 3rd MER, the U.S. was rated largely compliant with these requirements. The main technical deficiencies were the existence of a threshold for certain categories of suspicious activity reporting and no measures applied to investment and commodity trading advisers.

*Criterion 20.1* - The U.S. requires reporting of suspicious transactions by Covered FIs. Sector-specific BSA regulations<sup>97</sup> generally define *suspicious transactions* as: transactions conducted or attempted where the FI knows or suspects the transaction may involve potential ML or other illegal activity; is designed to evade the BSA or its regulations; has no business or apparent lawful purpose or is inconsistent with the customer's normal transactions and the FI knows of no reason for the transaction. Such regulations also prescribe the filing procedures, which include rules on the timing of reporting. Federal banking regulations place additional reporting requirements in the case of insider abuse and further elucidate the BSA requirements.<sup>98</sup> **Covered FIs** are required to notify law enforcement immediately by telephone and to file a "timely" SAR if the FI identifies a situation involving a violation requiring immediate attention regardless of threshold (i.e. ML/TF activity that is underway) (e.g. 31 CFR §1020.320 (b)(3) and the FFIEC Manual at page 67). The same requirement applies if the FI identifies a violation that requires immediate attention as a result of information received from another FI through an information sharing agreement (pursuant to Section 314(b) of the USA PATRIOT Act. Unless required to be reported immediately, reports of suspicious transactions must be filed with FinCEN no later than 30 calendar days after the date of the initial detection of facts that may constitute a basis for filing a SAR. FIs may take up to 60 days specifically to identify the people involved in the transaction if no suspect was identified at the time the suspicious activity was initially detected. While the assessment team acknowledges the statistics relating to numbers of SARs filed in less than 30 days, the reporting timeframe allowed (30/60 days) raises issues about the promptness of reporting as required under standards.

*Criterion 20.2* - Generally, the implementing regulations create a reporting obligation in respect of suspicious transactions that are over an aggregated transaction value of USD 5 000 (USD 2 000 for MSBs). In addition, the regulations noted at footnote 97 include an aggregated threshold of USD 25 000 where no suspect can be identified. Financial institutions are required to monitor all transactions in order to aggregate those that are suspicious for purposes of meeting the threshold, which the U.S. sees as a benefit to law enforcement. However, the effects of the threshold are partly mitigated by the requirement to immediately notify law enforcement (and in some cases FinCEN) and file a SAR regardless of the threshold in the case of violations requiring immediate attention, such as TF or ongoing ML schemes.<sup>99</sup> Banks are also required to report "any known or suspected

<sup>97</sup> See 31 CFR §1020.320 (for banks); 31 CFR §1023.320 (for securities broker-dealers); 31 CFR §1024.320 (for mutual funds); 31 CFR §1025.320 (for insurance companies); 31 CFR §1026.320 (for FCMs and IBs in commodities); 31 CFR §1022.320 (for MSBs, including sellers of prepaid access); 31 CFR §1029.210 and 1029.320 (for RMLOs); 31 CFR §1030.320 (for housing government sponsored enterprises)

<sup>98</sup> 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (BGFRS); 12 CFR 353 (FDIC); 12 CFR 748 (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).

<sup>99</sup> See e.g. 31 CFR 1020.320(b)(3), and FFIEC Manual, page 67 fn. 63, ("If a bank knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the bank should immediately call FinCEN's Financial Institutions terrorist hot line toll-free number (866) 556-3974. Similarly, if any other suspected violation — such as an ongoing money laundering scheme — requires immediate

Federal criminal violation” “regardless of the amount involved” if the activity involves the bank and “one of its directors, officers, employees, agents or other institution-affiliated parties” is suspected of committing or aiding in the commission of a criminal act.<sup>100</sup>

### *Weighting and Conclusion:*

There are several moderate shortcomings with respect to the scope (non-covered IAs), aggregated thresholds and time allowed to file SARs (30 and 60 calendar days). However, these shortcomings are partly mitigated by the fact that FIs are directed to report to law enforcement immediately, violations requiring immediate attention, such as ongoing ML schemes and terrorist activity, and to file a timely SAR, regardless of the threshold.

***Recommendation 20 is rated partially compliant***<sup>101</sup>.

### ***Recommendation 21 – Tipping-off and confidentiality***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements.

*Criterion 21.1* - Reporting entities and their directors, officers and employees are protected from civil liability for all SARs made to appropriate authorities, including supporting documentation, so long as the reporting relates to a possible violation of U.S. law: 31 USC 5318(g)(3). The safe harbor applies to *disclosures* (rather than *reports*), and to disclosures made jointly with another FI. It is not necessary for the report to be made in good faith to benefit from such protection.

*Criterion 21.2* - Reporting entities, their directors, officers, employees, or agents that report a suspicious transaction may not notify any person involved in the transaction that such a report was made. The same prohibition applies to government officials and employees, other than what is necessary to fulfill their official duties: 31 USC §5318(g)(2). Disclosure of a SAR and any information that would reveal its existence is prohibited (31 CFR 1020.320(e)). Similar regulatory amendments have been issued by various Federal bank regulatory agencies in conjunction with FinCEN. In addition to filing Form 8300 with the FinCEN/IRS, firms which file the form need to furnish a written statement to each person whose name is required to be included in the Form 8300 by January 31 of the year following the transaction. However, this requirement does not apply when Form 8300 is used to voluntarily report an illegal transaction (IRS Form 8300 Reference Guide).

### *Weighting and Conclusion:*

All criteria are met.

***Recommendation 21 is rated compliant.***

---

attention, the bank should notify the appropriate federal banking and law enforcement agencies. In either case, the bank must also file a SAR”). See also FinCEN MSB Manual page 86 fn. 61 for nearly identical language.

<sup>100</sup> See e.g. 12 CFR 21(c)(1).

<sup>101</sup> See discussion in relation to IOs 4 and 6 about effectiveness of the U.S. SAR reporting scheme despite technical compliance issues.

## Recommendation 22 – DNFBPs: Customer due diligence

In its 3<sup>rd</sup> MER, the U.S. was rated non-compliant: casinos were not required to perform enhanced due diligence (EDD) for higher-risk categories of customer, nor was there a requirement to undertake CDD when there is a suspicion of ML/TF; accountants, dealers in precious metals and stones, lawyers and real estate agents were not subject to customer identification and record-keeping requirements; and DNFBP were not subject to specific obligations relating to PEPs, new technologies, introduced business and unusual transactions.

*Criterion 22.1* - DNFBPs are required to comply with the R.10 CDD requirements:

- a) *Casinos*: CDD requirements apply to casinos with gross annual gaming revenue in excess of USD 1 million and in some instances go beyond what is required of FIs: 31 CFR § 1021.410. There are no specific EDD requirements.
- b) *Other DNFBPs*: In the U.S. lawyers, company formation agents, and to a lesser extent accountants, often have a role in relation to creation, operation or management of legal persons and buying or selling of business entities. The business of acting as an agent in the formation and administration of companies is not currently subject to AML requirements, with the exception of the Form 8300 filing obligation and targeted financial sanctions obligations. Lawyers and real estate agents both have a role in relation to buying and selling of real estate. **Real estate agents** are not subject to AML obligations. **Dealers in precious metals and stones** who purchase more than USD 50 000 in covered goods from persons other than other dealers or retailers, or receive more than USD 50 000 in gross proceeds from their sale, have AML program and currency transaction reporting requirements, and are required to file Form 8300 for transactions exceeding USD 10 000 in cash. Sectors such as **lawyers and accountants** that do not have other AML obligations, are subject only to targeted financial sanctions obligations to the obligation to file Form 8300 for cash transactions exceeding USD 10 000, and may choose to use a Form 8300 as a voluntary SAR relating to structuring or any potential illegal activity.

*Criterion 22.2* - **Casinos** are subject to detailed record-keeping requirements which generally meet the requirements of R.11: 31 CFR 1021.410; 31 CFR 1010.410. R.11 only applies to **other DNFBPs** on a very limited basis in relation to their obligation to file Form 8300. States regulate record retention policies for **real estate agents** licensed in their jurisdiction; requirements generally range from 3 to 5 years. States require licensed brokers to retain all listings, deposit receipts, cancelled checks, trust account records, and other documents executed or obtained by the agent in connection with any transaction. They also regulate how long a **lawyer** must retain client case files. Requirements vary, but go some way towards meeting R.11. No obligations are imposed on **company formation agents**.

*Criterion 22.3* - No DNFBPs are subject to obligations relating to R.12.

*Criterion 22.4* - DNFBPs are not subject to obligations specifically relating to R.15. The AML program requirements for **casinos and dealers in precious metals and stones** may go some way towards meeting R.15 obligations for these sectors: 31CFR1021.210(b)(2)(ii) and 31CFR1027.210(b)(1)(i).

*Criterion 22.5* - **Casinos** are not permitted to utilize third party reliance for CDD. **Other DNFBPs** are not subject to obligations that specifically relate to R.17.

*Weighting and Conclusion:*

Only casinos and dealers in precious metals/stones are specifically covered by BSA requirements. Other DNFBPs are covered in a limited way only when reporting via Form 8300. Where there is coverage, the deficiencies noted in relation to R10, R.11 and R.12 flow through to R.22. The assessors noted the risks involving legal persons/arrangements, and to high-end real estate. In the U.S. context, lawyers, accountants and company formation agents often have a significant role in such matters. In this context, the lack of coverage of lawyers, accountants and TCSPs (other than trust companies which are depository institutions), is significant. The assessors agree there is a lesser risk related to real estate agents given their level of involvement in transactions. High-end real estate transactions, where there is no lender involvement but a higher likelihood of involvement of legal entities, pose a higher risk. The current GTOs also address the risk here and results should be considered by the U.S. in deciding how to deal with these risks.

***Recommendation 22 is rated non-compliant.***

***Recommendation 23 – DNFBPs: Other measures***

In its 3<sup>rd</sup> MER, the U.S. was rated non-compliant with these requirements: casinos were the only DNFBP sector required to report suspicious transactions and there was a threshold on that obligation; other DNFBPs were not subject to the tipping off provision or protected from liability when they choose to file a SAR; other sectors were not required to implement adequate internal controls (i.e. AML programs); and there were no specific obligations on other sectors to give special attention to the country advisories relating to countries that have deficient AML controls. Assessors note the risks relating to legal persons and arrangements, and to some extent real estate transactions. In the U.S. context, lawyers, accountants and TCSPs (other than trust companies which are depository institutions) have a significant role in such matters, and therefore are vulnerable sectors.

*Criterion 23.1* - Casinos are required to file SARs above a USD 5 000 threshold: 31 CFR 1021.320; however, casinos also are directed to report immediately, regardless of threshold, any transaction or activity that requires immediate attention. The same 30 and 60 day time periods apply to other SAR reporting as for FIs, raising similar concerns about promptness. No other DNFBPs have SAR reporting obligations although all must report any currency transaction over USD 10 000 and can voluntarily indicate whether they think a transaction is suspicious.

*Criterion 23.2* - Only casinos and dealers in precious metals and stones are required to: have written AML programs which meet most of the requirements of R.18: 31 CFR 1021.210, 31 CFR 1027.210; and appoint a money laundering officer although this officer need not be at management level.

*Criterion 23.3* - Casinos and dealers in precious metals and stones are required to incorporate policies, procedures, and internal controls based on the institution's assessment of the ML/TF risks associated with its products and services. They do not have a specific and separate requirement to perform EDD for business relationships and transactions with persons from high risk jurisdictions. There are no obligations on other sectors.

*Criterion 23.4* - Casinos, and any directors, officers, employees, or agents of such casinos enjoy broad protection from civil liability for making required or voluntary reports of suspicious transactions: 31 USC 5318(g)(3) & 31 CFR 1021.320(f). Persons filing SARs are prohibited from disclosing that a report has been prepared or filed, except to appropriate LEA and regulatory agencies: 31 USC 5318(g)(2) & 31 CFR 1021.320(e). Accountants, lawyers, real estate agents and TCSPs which are not depository institutions are not covered by the voluntary disclosure provisions and protections of 31 USC 5318(g). The protection from liability and tipping off provisions do not apply to businesses that complete the suspicious transaction box on Form 8300.

### *Weighting and Conclusion*

Only casinos and dealers in precious metals and stones are specifically covered by BSA requirements. Other DNFBPs are covered in a limited way only when reporting via Form 8300 and for targeted financial sanctions purposes. Where there is coverage, the deficiencies noted in relation to R18, R.19, R.20 and R.22 flow through to R.23. For the reasons noted above in R.22, the lack of coverage of lawyers, accountants and TCSPs (other than trust companies which are depository institutions), and to a lesser extent real estate agents, is significant.

***Recommendation 23 is rated non-compliant.***

### ***Recommendation 24 – Transparency and beneficial ownership of legal persons***

In its 3<sup>rd</sup> MER, the U.S. was rated non-compliant with these requirements. The technical deficiencies were the absence of any measures to ensure that there was adequate, accurate and timely information on the beneficial ownership and control of legal persons that could be obtained or accessed in a timely fashion by competent authorities. Also, there were no measures taken by those states which permit the issue of bearer shares to ensure that bearer shares were not misused for ML.

*Criterion 24.1* - The formation of U.S. legal entities<sup>102</sup> is governed by State law. Each of the 56 States, territories and the District of Columbia has its own laws for the formation and governance of legal entities. Federal law also applies to them, once formed, in certain areas (e.g. criminal law, securities regulation, taxation). Information about the types and basic features, as well as the process for creation and for recording and obtaining information about legal entities, is publicly available on the relevant website of each State. Generally, the types of legal entities that are formed in the U.S. are the corporation, the limited liability company (LLC), the limited partnership (LP), the limited liability partnership (LLP) and the limited liability limited partnership (LLLP). Corporations and LLCs are the most common, at well over 95% of all legal entities. While the process for obtaining and recording basic information about these entities is there, there is no process or mechanism in any State for obtaining, recording and making public the process of gathering information on beneficial ownership.

*Criterion 24.2* - The U.S. has assessed the ML/TF vulnerabilities of all the types of legal persons that can be created and reviewed their associated risks based on LEAs' experience in conducting financial

<sup>102</sup> The terms "legal entity" and "legal person" are used synonymously to refer to any form of entity that is created by a filing with a State office.



investigations involving legal persons. One of the typical ML methods includes creating legal entities without accurate information being available to authorities about the identity of BO: NMLRA. Front companies, shell companies and shelf companies are misused for illicit purposes, often (in the case of front companies) by intermingling of licit and illicit profits. The U.S. has reported that shell companies (primarily in the form of corporations and LLCs) pose the biggest risk, although the risk is mitigated by some factors including the ability of LEAs to investigate relevant bank records, tax filings and other documents to obtain information about beneficial owners, living and/or having operations in the U.S.

*Criterion 24.3.* The requirements for creating a corporation and LLC vary from State to State. For corporations, every State requires the issuance, upon application, of a corporate governance document (“articles of incorporation,” “certificate of incorporation,” or “charter”) usually by the Secretary of State. This contains the corporation’s name, constitutes proof of its incorporation, form and existence, address of its registered office, and number of shares. For LLCs, although requirements vary across states, the process is similar. A limited partnership (LP) can also be formed by filing a Certificate of Limited Partnership (or similar document) with the State company registry. The following table gives a brief snapshot of information collected at the time of formation, or periodically, by States.<sup>103</sup>

**Table 28. Number of states collecting the indicated information**

Information	Collected during formation		Collected in periodic reports	
	Corporation	LLC	Corporation	LLC
Principal office address	23	31	39	29
Registered agent name and address	49	49	-	-
Signature of registered agent	12	12	-	-
Names of Directors/Officers/managers	17	20	45	32

This information is generally publicly available (in some cases upon payment of a fee). Also, in some States, the names and addresses of directors of corporations are publicly available. Not all information mandated under the FATF standards (e.g. list of directors) is required under all State legal frameworks. However the vast majority of the States (45 of 50) require corporations to provide a list of their directors and/or principal officers, either in their corporate governance document (17), or periodic report (45) filed with the State.

*Criterion 24.4* - Most States require corporations to maintain the basic information discussed under c.24.3 either at their principal office or at an unspecified location. All the States require corporations to maintain a record of their registered shareholders, including names and addresses, and the number and class of shares held by each. However, a majority of the States do not require this information to be maintained in the U.S.

<sup>103</sup> The National Association of Secretaries of States (NASS) Survey.

*Criterion 24.5* - While the founding documents described above must be filed for registration, there is no mechanism to ensure accuracy of the same. In addition, there is no requirement to update any changes to the list of directors/managers (other than through periodic reporting requirements-annual or biennial) in the company registry.

*Criterion 24.6* - No adequate mechanisms are in place to ensure that BO information is obtained by companies and available at a specified location in the U.S. or can otherwise be determined in a timely manner by a competent authority. The exception is for issuers with securities registered with the SEC (around 8 000 out of a total of around 30 million legal entities in the U.S.), whereby any person or group of persons who acquires either directly or indirectly the BO of more than 5% of a class of equity securities registered under Section 12 of the Exchange Act is required to file, among other things, a disclosure schedule with the SEC, disclosing the identity of the beneficial owner and the number of shares they beneficially own. Additionally, section 16 of the *Exchange Act* applies to every person who is the BO of more than 10% of any class of equity security registered under section 12 of the *Exchange Act*, and each officer and director (collectively, "reporting persons") of the issuer of such security. Section 16(a) also requires reporting of changes in such ownership. In addition, all public companies must disclose in their annual report the name and amount and nature of beneficial ownership of: the BOs of more than 5% of any class of the companies' voting securities, and the company's officers and directors. Because of the small number of public companies compared to the total population of legal entities, the assessors ascribe a very low weighting to the SEC measures. Beyond this SEC requirement, there is no requirement for other companies or company registries to obtain and hold up-to-date information on their BO or to take reasonable measures to do so. Deficiencies identified in R.10 and R.22 apply where the mechanism of using existing information (obtained by covered FIs/DNFBPs) is relied upon. In particular, it is noted that for customers that are legal persons, covered FIs/DNFBPs are not required to identify and take reasonable measures to verify the identity of the BOs, except in limited circumstances (c.10.10), the definition of BO in the BSA does not conform to the standard, and there is no specific obligation for any category of FI to understand the ownership and control structure of customers which are legal persons or legal arrangements (c.10.8).

Consistent with c.24.6 (c), the U.S. relies on existing information collected by the IRS which requires legal persons to obtain an EIN if they have income, employees, or are otherwise required to file any documents with the IRS. An EIN is also required under the BSA to open a bank account. To obtain an EIN, a legal entity must designate a "responsible party". *"Responsible party" is defined as the person who has a level of control over, or entitlement to, the funds or assets in the entity that, as a practical matter, enables the individual, directly or indirectly, to control, manage, or direct the entity and the disposition of its funds and assets. The ability to fund the entity or the entitlement to the property of the entity alone, however, without any corresponding authority to control, manage, or direct the entity (such as in the case of a minor child beneficiary), does not cause the individual to be a responsible party).* In its current form, the EIN is insufficient to meet this criterion because: i) the definition of a *responsible party* is not consistent with the FATF definition of *beneficial owner* (i.e., the natural person who ultimately owns or controls a customer need not be identified, the *responsible party* disclosed may be someone other than a beneficial owner, and only one responsible party needs to be disclosed even though there may be several beneficial owners); and ii) not all legal entities are required to obtain an EIN (e.g. forming a private company to hold land does not by itself require registration with either the SEC or IRS, unless

there is a lien or a mortgage on it); and it could remain as a shell after formation. The “responsible party” information is accessible by LEAs for non-tax investigations only through a court order, which the U.S. authorities state is not difficult to obtain.

*Criterion 24.7* - Any changes in *responsible party* (a term which is not consistent with the FATF definition of *beneficial owner*) as provided to the IRS need to be updated within 60 days. Other than for companies registered with the SEC, there is no separate requirement for companies or registries to obtain and keep accurate and updated BO information.

*Criterion 24.8* - State requirements create an obligation to maintain a registered office and registered agent at that office. As noted above, registered agents are not generally required to maintain basic or BO information, although some States require them to maintain names and addresses of directors, officers, LLC managers, etc. However, there is no explicit obligation to ensure that all basic and BO information is available to competent authorities. The primary purpose of registered agents is to provide for service of process and for delivery of tax and other official notices, the scope of responsibilities does not conform to c24.8(a). There are no requirements requiring companies to use the services of DNFBPs in the manner contemplated in c24.8(b); as noted these are not necessary for the company formation process. The U.S. uses the EIN mechanism which is an option contemplated in c24.8(c), but in its current form, that mechanism is insufficient as the information it collects does not align to the FATF BO definition.

*Criterion 24.9* - States retain indefinitely the information regarding legal entities. IRS maintains information collected in the EIN process indefinitely in electronic form. Tax payers are generally required to maintain books and records for tax administration purposes (for at least 3 years from the date return is due or filed). There is no other explicit requirement for companies to maintain information and records for five years after dissolution.

*Criterion 24.10* - In criminal matters, Federal LEAs can utilize judicial processes to obtain records of basic and beneficial ownership through the use of a grand jury subpoena. This involves the assistance of the prosecutor, the Assistant U.S. Attorney (AUSA) assigned to the investigation. Compliance with the subpoena is compulsory and is subject only to the Constitutional bar against self-incrimination (self-incrimination does not extend to legal entities). In most instances, there is a date specified on the subpoena as the deadline to for compliance which ensures timely access to information. As part of any Federal criminal investigation, the prosecutor can also apply to a Federal court for the issue of a search warrant (supported by evidence, generally by way of affidavit) to be executed upon a legal person. In some types of investigations, LEAs have administrative subpoena authority.

*Criterion 24.11* - All States prohibit the issuance of bearer shares or similar instruments.

*Criterion 24.12* - While State law generally requires that the business and affairs of a corporation be managed by or under the direction of the directors, this does not preclude the possibility of them acting as nominees. No State expressly permits corporations to use nominee directors; neither is there an express bar against them. There are no licensing requirements for nominee directors/nominee shareholders or requirements for them to disclose the identity of nominator. There are no other mechanisms to ensure compliance.

*Criterion 24.13* - Failure to obtain an EIN will result in non-compliance with tax filing requirements, and civil and criminal penalties, provided that the legal person is conducting activity which requires an EIN. However, not all legal entities are required to obtain an EIN, and there are no penalties for not updating 'responsible party' (which is not same as 'beneficial owner')<sup>104</sup> information. Failure to file an annual report to State authorities may lead to dissolution of the company: Model Business Corporation Act (MBCA) provisions 14.21, and it is a misdemeanor to sign a false document which is punishable by a fine (no amount is mentioned therein). There are some increased penalties for intentional disregard of applicable information reporting rules. Such penalties are not proportionate and dissuasive.

*Criterion 24.14* - U.S. competent authorities, including the DOJ Office of International Affairs (OIA), provide international cooperation, including investigative support to identify and share, as appropriate, basic and BO information. Most often, information identifying the individuals who own or control a legal entity is found through competent authorities exercising their investigative powers on behalf of foreign counterparts. With court approval, this can include compelling testimony, seizing evidence, and freezing funds. The provision of this information is not always rapid and the information required may not always be available.

*Criterion 24.15* - The DOJ OIA makes and responds to requests for assistance involving other countries and monitors quality of assistance received.

#### *Weighting and Conclusion:*

The major gap is the generally unsatisfactory measures for ensuring that there is adequate, accurate and updated information on BO (as defined by the FATF) which can be obtained or accessed by competent authorities in a timely manner. Other gaps are in the areas of basic information being obtained by State registries, absence of licensing or disclosure requirements for nominee shareholders/ directors, and no requirement for companies to maintain register of shareholders within the country.

***Recommendation 24 is rated non-compliant.***

### ***Recommendation 25 – Transparency and beneficial ownership of legal arrangements***

In its 3<sup>rd</sup> MER, the U.S. was rated non-compliant with these requirements. The technical deficiency was that, although the investigative powers noted were generally sound and widely used, there was minimal information concerning the beneficial owners of trusts that could be obtained or accessed by the competent authorities in a timely fashion.

*Criterion 25.1* - Trusts in the U.S. are governed primarily by State law, whether expressly enacted into legislation or consisting of common law. A total of 31 out of the 50 States have enacted versions of the *Uniform Trust Code of 2000* (the UTC), which is primarily a default statute with most of its provisions being subject to the terms of the trust (see UTC 105(b) for exceptions). The trust law of the remaining 19 states is based on common law, or their own individual codification. State law (statute law or common law) imposes fiduciary duties on trustees (e.g. section 801-813 of UTC).

<sup>104</sup> Also see IMF FSAP Technical Note on AML/CFT: July 2015.

25.1 a) and (b): These duties include keeping records and informing and reporting to the beneficiaries but do not explicitly require trustees to obtain and hold adequate, accurate and current information on the identity of other regulated agents of trust service providers, a protector, if any, all beneficiaries, or the identity of any natural person exercising ultimate effective control over the trust. There may be a trust instrument that sets out the identity of the settlor, the trustee and the terms of the trust, which may refer to a beneficiary or class of beneficiaries, but this is not a legal requirement and parties may rely upon other evidence to prove the existence of a trust (section 103(18) of UTC).

25.1 (c): In the U.S., the only identifiable group of professional trustees is trust companies, which are FIs with fiduciary (trust) powers to act as trustee. However, the BSA does not impose explicit obligations on trustees. Professional trustees are subject to the Covered FI obligations when dealing with clients and this extends to their role as trustee.

*Criterion 25.2* - The UTC and the common law obligate trustees to keep adequate records and to keep beneficiaries reasonably informed. Trust companies are required to keep records for a period of at least 3 years following the termination of the account. State chartered trust companies are subject to the relevant State's record-keeping requirements, but while there are no explicit obligations to keep information accurate and as up-to-date as possible and to update it on a timely basis, it would be necessary for trust companies to do so in order to comply with the explicit obligations mentioned in the preceding paragraph. Records of receipt, disbursement and assets of the trusts may need to be maintained for tax administration purposes.

*Criterion 25.3* - Subsections 810(b) and (c) of the UTC require that trustees ensure that the trust interest appears in third party records, including banks, but this requirement may be overridden by the terms of the trust. There is no provision in the BSA that obligates trustees (aside from trust companies) to disclose their status as trustee to FIs and DNFBPs when forming a business relationship or carrying out an occasional transaction.

*Criterion 25.4* - Trustees are not prevented by law from providing information relating to the trusts to the competent authorities. Competent authorities can access information through court order. LEAs and other competent authorities can also compel production of financial records by issuing administrative, grand jury or civil subpoenas. LEAs have powers of search and seizure in appropriate cases. There is no law that would prevent a trustee from providing FIs and DNFBPs upon request, with information on the BO or the assets held under the trust.

*Criterion 25.5* - LEAs can obtain relevant information held by trustees, and other parties, including FI and DNFBPs, regarding trusts created in, or operating in, the U.S., including information on the residence of the trustee and any assets held or managed by a FI or DNFBP. Information on the ultimate beneficial owner with effective control may not be available, as it is not required to be kept by trustees (ref. c25.1). Competent authorities can use judicial processes to request a warrant to compel a search or seizure, or a subpoena to require testimony be given or records produced. Access to information may not be timely in all cases since this would largely depend on whether the LEA knew that a person or entity was a trustee.

*Criterion 25.6* - The U.S. competent authorities, including DOJ OIA, provide international co-operation. This co-operation includes investigative support to identify and share, as appropriate,

information regarding the relevant parties associated with trusts and other legal arrangements that have a presence in the U.S. It may be necessary for there to be a substantial investigation using investigative powers to obtain any available information and beneficial ownership information may not be available. On that basis, it cannot be said that the information will be provided rapidly. Further, intercept evidence is not available in respect of a MLA request.

*Criterion 25.7* - The trustee, as title holder to the assets of the trust and signatory on trust accounts, is directly and personally responsible for the trust assets and the fulfilling the terms of the trust. There are proportionate and dissuasive sanctions for the failure of a trustee to perform his fiduciary duties including failure to obtain and maintain information on the parties to the trust. Those sanctions include being removed as trustee, having to refund to the trust all trustee fees and commissions, potential monetary damages and even criminal penalties in the event of fraud. However, c25.1 to 25.3 have gaps in coverage, for which there are no proportionate or dissuasive sanctions.

*Criterion 25.8* - BSA sanctions only apply to trust companies. Tax laws provide proportionate and dissuasive sanction for denying IRS timely access to information: a fine of up to USD 1 000 or a prison sentence of up to 1 year, or both, together with the costs of prosecution for failing to comply with an IRS administrative summons; and a fine of not more than USD 25 000 (USD 100 000 in the case of a corporation) or imprisonment for less than 1 year, or both, together with the costs of prosecution for the misdemeanor of failing to supply information at the time required by law or regulations. If a summoned party does not comply with a U.S. court order to produce the requested information, the U.S. court has inherent powers (under U.S. common law) to impose so-called “civil society” sanctions, i.e., daily impositions of fines and/or incarceration, until the summoned person complies with the court’s enforcement order.

### *Weighting and Conclusion:*

Although there are general fiduciary obligations imposed on trustees, these generally address trust law broadly; but do not appear to address obligations on trustees to obtain and hold adequate, accurate and current information on the identity of regulated agents of the trust, service providers, a protector, if any, all beneficiaries, or the identity of any natural person exercising ultimate effective control over the trust. The obligations to keep information accurate and up-to-date only apply to trust companies. Trust instruments that could block the ability of trustees to provide information about the trust to FIs and DNFBPs upon request are not prohibited. LEAs can obtain relevant information provided they know whether a person is a trustee, but there is no enforceable obligation on trustees (apart from trust companies) to declare their status to FIs. Due to the foregoing issues, it cannot be said that information will be provided to foreign authorities rapidly. There are requirements in banking, trust, and tax law that, taken together, meet the 5 year records retention standard but these only apply to trust companies for the most part. The UTC requires trustees to identify property subject to a trust, but that obligation can be overridden by the terms of the trust. It is not known how this provision has been implemented by the non- UTC States. Information may not be obtained in a timely manner or at all in some cases. Overall, it is difficult to weight the impact of the trust company obligations as there is no information on the total universe of trusts that are subject to U.S. law.

***Recommendation 25 is rated partially compliant.***



## **Recommendation 26 – Regulation and supervision of financial institutions**

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements as some securities sector participants were not subject to supervision for AML/CFT requirements.

**Criterion 26.1 - FinCEN** administers the BSA (Treasury Order 180-01), and has authority to examine all financial institutions subject to its regulations<sup>105</sup> for compliance with the BSA and those implementing regulations (31 CFR Chapter X) and to take enforcement actions for violations. FinCEN has delegated BSA examination authority (31 CFR §1010.810) to **FBAs, SEC, CFTC, IRS-SBSE and FHFA**, but has retained AML/CFT civil enforcement authority. **IRS-SBSE**<sup>106</sup> authority is in practice limited to MSBs, as it no longer examines life insurance companies (now conducted by State life insurance prudential supervisors through the NAIC methodology). However, IRS-SBSE retains authority to conduct life insurance company AML/CFT exams, if requested by the States or directed by FinCEN. **FBAs** also have independent authority to charter, supervise, and insure most depository FIs. **SEC** and **FINRA** oversee the securities sector. SEC also has oversight authority over FINRA. Certain intra-State broker dealers, operating only in one State are not registered/regulated by the SEC.<sup>107</sup> **CFTC** oversees derivatives markets. FCMs and IBs are covered FIs subject to BSA requirements. CFTC has further delegated examination authority to SROs: the **NFA**, and the **Chicago Mercantile Exchange Group (CME Group)**. The CFTC oversees NFA and CME Group.

**Criterion 26.2 -** The U.S. does not permit shell banks to be established at the National or State level, and prohibits U.S. FIs from entering into/continuing correspondent banking relationships with foreign shell banks: s.313 USA PATRIOT Act & 31 CFR §1010.630. **FBAs, SEC and CFTC** are the relevant Core Principles (CP) supervisors at the Federal level and the State banking and life insurance supervisors at the State level<sup>108</sup>. All CP supervisors have authority to licence and supervise their respective sector participants. All MSBs must register with **FinCEN**. MSBs are licenced by 47 States and in the District of Columbia and in all other U.S. territories. At the time of the on-site visit, Montana, New Mexico and South Carolina did not license or register money transmitters.<sup>109</sup>

**Criterion 26.3 - FBA** fit & proper processes involve evaluating proposed directors and senior management with respect to expertise, integrity, and any potential for conflicts of interest,

<sup>105</sup> For this purpose, FIs include any : (1) bank; (2) broker or dealer in securities; (3) MSB; (4) telegraph company; (5) casino; (6) card club; (7) futures commission merchant, (8) introducing broker in commodities, (9) mutual fund, (10) life insurance company; (11) dealer in precious metals; (12) operator of a credit card system; (13) residential mortgage loan originator; and (14) housing government sponsored enterprise.

<sup>106</sup> IRS-SBSE routinely examines casinos and MSBs for BSA compliance and is able to examine any entity that does not have a federal functional regulator, per FinCEN authority.

<sup>107</sup> However, this exception from registration is very narrow; since to qualify, all aspects of all transactions must be done within the borders of one state. Thus without SEC registration, a broker-dealer cannot participate in any transaction executed on a national securities exchange or Nasdaq. Also, information posted on the Internet that is accessible by persons in another state would be considered an interstate offer of securities or investment services that would require SEC registration. An intrastate broker-dealer remains subject to the State registration requirements where it conducts business.

<sup>108</sup> CP financial sectors comprise depository FIs, the securities industry, and the life insurance sector.

<sup>109</sup> Since the date of on-site, authorities reported that MSBs in New Mexico and South Carolina are now covered under licensing regime as per the legislative amendments in these states.

consideration of reputation for honesty and integrity. The processes include obtaining details on their educational and professional experience, completing fingerprint cards, and having LEAs conduct background checks. The processes are applied by all relevant FBAs which often overlap or duplicate processes. In addition, the *Change in Bank Control Act* is designed to ensure the probity of persons taking a significant or controlling interest in a bank or a bank holding company.<sup>110</sup> Lastly, a person convicted of any criminal offenses involving dishonesty, breach of trust or ML or who has entered into a pre-trial diversion or similar program is prohibited from owning or controlling, directly or indirectly, an insured institution, or otherwise participating, directly or indirectly, in the conduct of affairs of an insured institution: s.19 FDIC Act. This also applies to holding companies: s.19 FDI Act 12 USC. §1829. **In the securities sector**, the SEC and FINRA can deny registration to entities and individuals that have engaged in certain misconduct, and impose limitations on associated individuals for engaging in certain misconduct: Sections 15(b)(4) and 15(b)(6) of the *Exchange Act*, sections 203(e)-(f) and 203(i)-(k) of the *Advisers Act*, sections 9(b) and 9(d) of the *Investment Company Act*, NASD Rules 1014 and 1017. **In the derivatives sector**, CFTC is specifically authorized to refuse to register persons convicted of certain crimes, and to suspend or modify their registration. **For life insurance companies**, every State uses the Biographical Affidavit (containing background information from persons seeking ownership or management position). **State insurance regulators** are also required to be notified of changes in officers and directors via quarterly and annual statements and, in some states, upon request. **For MSBs**: three states at the time of the on-site visit, did not conduct criminal background checks as they did not licence money transmitters. In all other states and territories, background checks are completed prior to the issuing of licenses, which include criminal background checks. Further, under the BSA, MSBs are also required to complete an initial registration with FinCEN and renew that registration every two years.

*Criterion 26.4* - FIs are subject to the following:

- a) *Core Principles Institutions*: FBAs coordinate their AML/CFT supervision through the FFIEC structure and follow the FFIEC BSA Examination Manual. FBA examinations are conducted every 12-18 months, with the methodology following a RBA. SEC examines registered broker dealers and mutual funds and oversees SROs which have their own compliance monitoring responsibilities for broker-dealers. In the insurance sector, life insurance companies are supervised by State insurance supervisors as requested by FinCEN. The State insurance supervisors include such reviews as part of their regular, standard NAIC examination (e.g. existence of AML programs, risk assessments, independent test plans and its results, record-keeping and internal controls etc.). State banking authorities supervise compliance with BSA/AML requirements at most of the State banks not subject to Federal oversight.
- b) *Other financial institutions*: CFTC's regulatory scheme relies on the supervision activities of the SROs (NFA and CME) and its oversight over SROs. While examination of RMLOs falls within the delegation to the IRS, it is yet to commence. The supervision of housing GSEs is done by FHFA in coordination with FinCEN in accordance with its examination manual.

<sup>110</sup> 12 USC 1817(j). Similar criteria exist in securities and derivatives sectors: ss.15(b)(4) & 15(b)(6) of the *Exchange Act*, ss.203(e)-(f) & 203(i)-(k) of the *Advisers Act*, ss.9(b) & 9(d) of the *Investment Company Act*, NASD Rule 1014, FINRA Rule 8310, CEA ss.8a(2), (3) & (11), 7 USC § 12a(3), (5) & (11).

Supervision and regulation of the MSB sector occurs through coordination between FinCEN, IRS-SBSE, and the State regulatory authorities.

*Criterion 26.5 - FBAs* have authority to conduct more frequent examinations based on the its supervisory strategy, institution's risk profile, the application of an enforcement action, the introduction of new product or service offerings, the identification of ML/TF risks by LEAs in regional or local jurisdictions surrounding the institution and similar issues. SEC-OCIE uses a risk-based approach for selecting firms for examination and draws on a variety of data sources for this. Additionally, FINRA examinations are risk-based, and the frequency of an examination ranges over a 1-4 year cycle. In relation to **MSBs**, the BSA Manual makes it clear that intensity of supervision is based on risk. The **insurance sector** is subject to a lighter touch supervisory regime appropriate to the applicable obligations.

*Criterion 26.6 - FBAs* are required by the statute to include reviews of BSA compliance programs in their examinations, and monitor major events or developments through ongoing prudential supervision of operations and management. For **other FI sectors**, similar requirements apply, though it is unclear if a review of risk assessment is triggered by major events or developments in FIs. For the **life insurance sector**, State insurance regulators include as part of their regular, standard NAIC examination a review of the existence of AML risk assessments and internal controls. The Federal supervisory role is reliant on input from State supervision. The IAIS FSAP of 2015 noted there were 11 MOUs in place between FinCEN and State life insurance supervisors.

#### *Weighting and Conclusion:*

Not all investment advisers are covered. At the time of on-site, three States did not license MSBs, resulting in no background checks.

**Recommendation 26 is rated largely compliant.**

#### **Recommendation 27 – Powers of supervisors**

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements.

*Criterion 27.1* - The Treasury has delegated to FinCEN the authority to implement, administer and enforce BSA compliance with respect to all Covered FIs: 31 USC §5318(a)(3) & 31 CFR §1010. FinCEN has delegated BSA examination authority to the FFR and to the IRS for other covered non-bank FIs, except for life insurance companies. For life insurance companies, FinCEN relies on State insurance supervisors to assess compliance with BSA obligations and report non-compliance issues to FinCEN. It has retained BSA enforcement authority in all delegated cases. The FBAs have their own independent and generally uniform regulations requiring implementation of a BSA/AML compliance program by most depository FIs, and can take enforcement action for non-compliance. While banks may also be chartered by State authorities, a majority of State-chartered banks and credit unions are subject to supervision by an FBA if they are insured by the FDIC, or the NCUA. Most States also conduct BSA/AML examinations under State statutes that require compliance with the BSA. The SEC and FINRA have examination and enforcement authority for compliance with BSA requirements. CFTC and SROs-NFA and CME group (for derivatives) and IRS-SBSE (for MSBs and other non-bank

FIs) have examination authority for BSA compliance and applicable SRO rules. While IRS-SBSE has no enforcement authority, it can refer cases to FinCEN for civil enforcement and FinCEN in turn, can issue a warning letter, or assess a penalty. In the MSB sector, many States also conduct on-site examinations, sometimes in a coordinated manner, through the Nationwide Cooperative Agreement which provides a framework for conducting a single exam by multiple States.

*Criterion 27.2* - FBAs have their own independent authority to conduct inspections of FIs under their domain, aside from FinCEN's delegated authority. Such reviews are performed during on-site examinations, as required by statute. SEC, CFTC (along with SROs), IRS and State regulators have their own authority to conduct reviews both under BSA and their own regulations and rules, wherever applicable.

*Criterion 27.3* - FinCEN and any delegated agency may examine any books, papers, records, or other data of FIs relevant to the BSA record-keeping or reporting requirements. For any investigation for civil enforcement of the BSA, FinCEN may summon a FI/ any of its employees or any person in possession of BSA records to give testimony and produce records. FBAs have separate broad statutory authority to examine all books and records of regulated FI. In addition, FIs must respond to requests for information within 120 hours after receiving the request from a FBA. FBAs also have investigation authority, permitting them to take sworn testimony and issue subpoenas for the production of documents from third parties. In the derivatives sector, every FCM and IB that conducts business with the public must become a NFA member, comply with its rules and cooperate with it in any investigation, inquiry, audit, examination or proceeding. SEC has broad access to its registrants' books and records and also has broad investigation authority. Under its subpoena authority, SEC can compel the production of documents or testimony from any person or entity anywhere within the U.S. In addition, FINRA also has the right of inspection and to require a member/associated person, or other person under its jurisdiction to provide information and to testify. For MSBs, IRS-SBSE can issue summons and receive evidence and examine witnesses. State regulators also generally have full access to the books and records of MSB licensees. State life insurance supervisors have authority under their governing legislation to require life insurance companies to produce any documents required for supervisory purposes.

*Criterion 27.4* - FinCEN is authorized to assess CMPs against Covered FIs and DNFBPs, and their partners, directors, officers, or employees for willful or negligent BSA violations. For criminal liability, FinCEN may pass the matter to the DOJ. FinCEN is authorized to subject unlicensed MSB providers to civil or criminal penalties. State banking regulators also have broad enforcement powers under State law. For life insurance companies, FinCEN has retained the authority to enforce sanctions for BSA violations. FBAs can bring informal and formal action. This includes cease and desist (C&D) orders, CMPs, barring individuals from employment within the industry, restricting or suspending the operation of the institution, revoking the license of the institution (all formal), reprimanding individuals (formal/informal) or referral of the matter to FinCEN for possible CMPs, or a combination of these actions. For the derivatives sector, both CME Group and NFA may file disciplinary complaints against their members for violations of AML program rules. The CFTC has broad sanction authority, including the imposition of CMP. In the securities sector, remedies and sanctions available to SEC are broad and include disgorgement of ill-gotten gains, CMP, compliance with undertakings, imposition of limitations of activities, and C&D powers. Registration of regulated

entities may be suspended or revoked, and regulated individuals may be subject to industry-wide bars or suspensions. FINRA's sanction powers include fines against member firms/associated persons, their suspensions/ bars and undertakings (e.g. review and revise AML procedures or undertake AML training).

### *Weighting and Conclusion:*

All four criteria are met..

***Recommendation 27 is rated compliant.***

### ***Recommendation 28 – Regulation and supervision of DNFBPs***

In its 3<sup>rd</sup> MER, the U.S. was rated partially compliant with these requirements as there was no regulatory oversight for AML/CFT compliance for accountants, lawyers, real estate agents or TCSPs, and the supervisory regime for Nevada casinos was not harmonized with the BSA requirements.

*Criterion 28.1* - Casinos in the U.S. must be licensed under the laws of the State, territory, or tribe where they are located.<sup>111</sup> The State gaming commissions investigate the qualifications of the license applicants prior to issuing a casino license. They also issue and administer regulations on the types of games that can be offered, consumer protection, and internal casino controls. Most licensed gambling in the U.S. takes place on lands administered by 246 Native American tribes. States regulate tribal gaming at a level negotiated through tribal/State compacts. The Federal government regulates it through:

- a) The National Indian Gaming Commission (NIGC), which is the primary Federal regulator, providing oversight, reviewing licensing of gaming management and key employees, management contracts (25 USC 2711), and tribal gaming ordinances;
- b) The Department of the Interior, which oversees the tribal-state compact process, and reviews and approves compacts;
- c) The Treasury which, through FinCEN, regulates and supervises casinos and card clubs for compliance with the BSA; and
- d) The DOJ, which, through the FBI, has Federal investigative jurisdiction over criminal acts directly related to Indian gaming establishments.

The BSA regulatory requirements for casinos and card clubs include requirements for a) an AML program: 31 CFR 1021.210 b) currency transaction reporting: 31 CFR 1021.311 c) suspicious activity reporting: 31 CFR 1021.320; and d) record-keeping: 31 CFR 1021.410. FinCEN has delegated to the IRS BSA compliance examination authority for institutions not under the supervisory authority of a Federal regulator or a self-regulatory agency, including casinos and card clubs with annual gaming revenue over USD 1 million: Treasury Directive 15-41, 31 CFR 1010.810(b)(8). OFAC

<sup>111</sup> 23 States license commercial casinos: Colorado, Delaware, Florida, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Nevada, New Jersey, New Mexico, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, and West Virginia. Source: 2013 American Gaming Association State of the States Survey



has delegated to the IRS authority to review compliance with U.S. economic sanctions: Treasury Directive 15-43.

*Criterion 28.2 and 28.3.* - FinCEN administers the BSA regulatory requirements for dealers in precious metals, precious stones, or jewels, which include requirements for a) AML program 31 CFR 1027.210; and b) Form 8300: 31 CFR 1010.330; and c) record-keeping: 31 CFR 1010.410. FinCEN has delegated authority to IRS to examine dealers in precious metals, precious stones, or jewels (as well as all other non-financial trades and businesses), for compliance with Form 8300 reporting requirements which require them to file reports for currency received in excess of USD 10 000. Beyond this, DNFBPs, most of which are much higher risk than dealers in precious metals and stones are not subject to AML/CTF obligations and not monitored for compliance.

*Criterion 28.4* - Other than the customer identification and record-keeping requirements associated with the filing of Form 8300, broader AML/CFT requirements have not been extended to any category of DNFBP, other than casinos and dealers in precious metals and stones. FinCEN has broad powers to supervise dealers in precious metals and stones for AML/CFT purposes. IRS-SBSE has no civil enforcement authority over Title 31 BSA violations, only FinCEN has that authority. IRS-SBSE reports Title 31 civil violations during and after their BSA examinations to FinCEN. When indicators of potential fraud are identified during an examination, IRS-SBSE will refer the case to IRS-CI for criminal enforcement consideration. The Director of FinCEN, and any agency to which examination has been delegated, may examine any books, papers, records, or other data of non-financial trades or businesses relevant to the record-keeping or reporting requirements of the BSA: see R.35. FinCEN participates in non-bank examinations for selected matters. For any investigation for civil enforcement of the BSA, the FinCEN Director may also summon any person in possession of BSA records to give testimony and produce these records<sup>112</sup>. FinCEN is also authorized to assess civil money penalties against a non-financial trade or business, or a partner, director, officer, or employee of a non-financial trade or business for willful or negligent violations of the BSA: 31 USC 5321; 31 CFR 1010.810(d)), 31 CFR 1010.820(h). Attorneys and accountants are subject to various state licensing and disciplinary regimes which would meet the requirements of 28.4(b). Company formation agents who act as registered agents are subject to registration requirements through the Secretary of State in some States. Though no criminal background check is done, they can be delisted if concerns arise. Real estate agents are also generally licensed through Secretaries of State which may require a criminal background check.

*Criterion 28.5* - The U.S. takes a risk-based approach to the AML/CFT supervision of casinos and dealers in precious metals and stones. The basic examination process is described in the IRS BSA Examination Manual.<sup>113</sup> Other DNFBPs are subject to supervision only in respect of Form 8300 reporting obligations.

### *Weighing and Conclusion:*

There has been significant focus on the casino sector with excellent results however other sectors such as dealers in precious metals and stones have not been subject to similar focus and action.

<sup>112</sup> 31 USC 5318(a)(4),(b),(c),(d),(e); 31 CFR 1010.911-917.

<sup>113</sup> [http://www.irs.gov/irm/part4/irm\\_04-026-006.html](http://www.irs.gov/irm/part4/irm_04-026-006.html)



Other DNFBPs are subject to only limited supervision as a result of their limited obligations. This is a fundamental deficiency when looked at in the context of risk relating to legal persons and high-end real estate in particular.

**Recommendation 28 is rated non-compliant.**

### **Recommendation 29 - Financial intelligence units**

In its 3<sup>rd</sup> MER, the U.S. was rated as largely compliant on the basis of technical deficiencies related to the sharing of terrorism-related requests of information from foreign FIUs to LEA without prior approval from said FIUs. Since then, the FATF standards have been significantly strengthened, imposing new requirements focused on the FIU's strategic and operational analysis functions, and powers to disseminate information upon request and request additional information from reporting entities.

*Criterion 29.1* - The U.S has established an FIU (FinCEN) responsible for maintaining, collecting, processing, storing, analyzing and disseminating the financial and other information collected under the BSA and other authorities, relating to the analysis or investigations of illicit finance (including ML and TF): *31 USC 310(b)*.

*Criterion 29.2* - FinCEN is the central repository for reporting and disclosures filed by reporting entities pursuant to the BSA including SARs<sup>114</sup> and other reporting information including: currency exceeding USD 10 000 on CTRs<sup>115</sup>; *CTR Filing Exemption Form (Designation of Exempt Persons)*; Report of International Transportation of Currency or Monetary Instruments (CMIR); *Foreign Bank Account Report (FBAR)*<sup>116</sup>; and Registration of MSBs<sup>117</sup>. FinCEN is also the repository for *Report of Cash Payments over USD 10 000 Received in a Trade or Business (Form 8300)*<sup>118</sup> which is also filed with the IRS.

*Criterion 29.3* - FinCEN has access to a broad array of information needed to conduct its analysis properly including both direct and indirect access to a wide range of financial, administrative, commercial and LEA databases and/or information. FinCEN can request all supporting documents

<sup>114</sup> Institutions and DNFBPs required to file SARs include banks, casinos and card clubs, money services businesses (except check cashers,) brokers or dealers in securities, mutual funds, insurance companies, futures commission merchants and introducing brokers in commodities, loan or finance companies, and housing government sponsored enterprises, U.S. Postal Service; *31 CFR 1010.311 and casinos: 31 CFR 1021.311*.

<sup>115</sup> For depository institutions, securities-broker dealers, mutual funds, futures commission merchants and introducing brokers in commodities, MSBs, and casinos. For CTR filing obligations for financial institutions other than casinos, see 31 CFR §1010.311. For CTR filing obligations for casinos, see 31 CFR §1021.311(a)-(c).

<sup>116</sup> Both CMIR and FBAR individual reporting requirement legal and natural person: *CMIR: 31 CFR §§1010.306(b), CFR1010.306(d) and FBAR: 31 CFR 1010.306(c)-(e)*.

<sup>117</sup> The registration of money services businesses requirement is available at 31 CFR §1022.380(a)-(f).

<sup>118</sup> Applicable to life insurance companies; dealers in precious metals and stones; operators of credit card systems; and loan or finance companies, and all non-financial trades and businesses :*31 CFR §1010.330 & 31 USC 5331*.

related to the filing of a SAR<sup>119</sup> and may also access some records from reporting entities. Furthermore, FinCEN is able to combine its several authorities to obtain additional information from reporting entities in relation to specific ongoing cases/investigations (see IO.6 analysis). These information gathering powers include GTOs<sup>120</sup>, Demand Letters<sup>121</sup>, FFA rules<sup>122</sup> and information sharing authority under s.314(a), USA PATRIOT Act<sup>123</sup> (see IO.6).

*Criterion 29.4* - FinCEN applies a risk-based approach to analysing SARs, devoting its analytical resources to those SARs considered most valuable to FinCEN and LEAs. It produces data-driven tactical, operational and/or strategic reports employing advanced analytics to identify trends, patterns and explain priority threats to the financial system. The format, length and depth of these strategic and operation products depend on the target audience.

*Criterion 29.5* - FinCEN disseminates a wide variety of products and information both spontaneously and/or upon requests to competent authorities LEAs, BSAAG and requesting countries (via the secure Egmont Group or FinCEN attachés). Federal, State and local competent authorities have, by agreement, direct access to FinCEN databases and its financial intelligence information through its secured website (FinCEN portal).

*Criterion 29.6* - FinCEN protects information in the following ways:

- a) There are multiple rules, guidelines, principles in place governing the information security and confidentiality, along with training and monitoring of access to and use of the database by Federal, State, local and agency personnel.
- b) FinCEN staff must undergo a security clearance which is regularly re-adjudicated. Staff receives annual training on security-related issues, including document handling and confidentiality. FinCEN personnel have a duty not to disclose official information without proper authorization: 31 CFR §0.206 Part I, Subpart B.
- c) Access to FinCEN facilities and information, including IT systems, is secured, protected and restricted.

*Criterion 29.7* - FinCEN is operationally independent and autonomous:

- a) The Director of FinCEN possesses full authority, powers, and duties to administer the affairs and to perform the functions of FinCEN freely: 31 USC §310 and Treasury Order 180-01.
- b) The Director of FinCEN can sign, on his/her own authority, non-binding MOUs with domestic competent authorities, foreign FIU counterparts and foreign AML/CFT financial supervisory agencies.

<sup>119</sup> 31 CFR §1020.320(d) and (e)(depository institutions); 31 CFR §1023.320(d) and (e) (brokers or dealers in securities); 31 CFR §1022.320(c) and (d) (MSBs); 31 CFR §1021.320(d) and (e) (casinos) and 31 CFR §1025.320(e)(insurance companies)

<sup>120</sup> 31 USC § 5326(a); 31 CFR § 1010.370; Treasury Order 180-01.

<sup>121</sup> 12 USC § 1829b (b)(3)(C); 31 CFR § 1020.410(a); 31 CFR § 1010.410(e). See also 12 CFR § 219.23.

<sup>122</sup> 31 USC § 5314; 31 CFR § 1010.360

<sup>123</sup> Codified at 31 USC § 5311 (Notes); 31 CFR § 1010.520.

- c) FinCEN's powers and duties are separated and distinct from those of other units within the Treasury: 31 USC §310.
- d) FinCEN's budget is separate from that of the Treasury. FinCEN is able to spend its budgetary appropriations, deploy necessary resources and make operational decisions to carry out its functions as it sees fit.

*Criterion 29.8* - FinCEN is a founding and active member of the Egmont Group.

*Weighting and Conclusion:*

All eight criteria are met.

***Recommendation 29 is rated compliant.***

***Recommendation 30 – Responsibilities of law enforcement and investigative authorities***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements. The FATF standards in this area were considerably strengthened in 2012.

*Criterion 30.1* - The U.S. has designated DOJ, DHS, Treasury and USPS as responsible for investigating ML, TF and associated predicate offenses: 18 USC 1956(e) and 1957(e); 18 (1956)(c)(7)(d); 18 USC 2339B(e). The DOJ is the central authority for prosecuting violations of Federal laws, including the Federal ML and TF offenses. The FBI is the principal investigative arm within the DOJ to conduct criminal investigations of over 200 Federal crimes. It also has authority to investigate all federal crimes not assigned exclusively to another Federal agency. The remit of DHS (HSI-CI, ICE, USSS), the DOJ (DEA) and Treasury (IRS-CI, USPIS) are described in Chapter 1–Legal institutional framework section. State and local enforcement agencies can work on ML cases on their own (in States criminalizing ML) or with Federal authorities on both ML and TF in the context of task forces.

*Criterion 30.2* - All Federal LEAs noted above are authorized to pursue parallel financial investigations. The vast majority of Federal criminal prosecutions are handled by the U.S. Attorney's Office (USAO) in the district where the offense occurred. Where the USAO does not have the expertise or resources to handle complex ML and TF cases, they can be referred to the DOJ headquarters including the Asset Forfeiture and Money Laundering Section (AFMLS–see Chapter 1).

*Criterion 30.3* - The U.S. has designated competent authorities to expeditiously identify, trace and initiate freezing and seizing of property that is, or may become, subject to confiscation or is suspected of being proceeds of crime. All Federal agencies have access to basic investigative tools including grand jury and administrative subpoenas and have authority to seize and forfeit property as described via criminal or civil procedures as set out in R.4.

*Criterion 30.4* - FinCEN and the enforcement divisions of both SEC and OFAC exercise investigative functions and can complement law enforcement efforts aimed at targeting illicit financial networks. FinCEN conducts parallel financial investigations for BSA violations related to law enforcement investigations into underlying criminal activity. The SEC is responsible for detecting and investigating potential violations of the Federal securities laws and regulations, and for civil and administrative enforcement actions. The CFTC investigates and alleged violations of the CEA and

Commission regulations and can take civil enforcement action. Both the CTFC and SEC can provide assistance on criminal matters to the DOJ and they are both able to obtain non-public information, including bank records, and testimony from individuals and entities. OFAC has the authority to conduct civil investigations and impose administrative penalty against U.S. persons that conduct business in, to, or through the U. S., including FIs that fail to properly to apply TFS and sanction programs.

*Criterion 30.5* - The U.S. allocates authority to investigate ML/TF offenses arising from corruption to the relevant LEAs – including the FBI as the leading enforcement agency handling public corruption and relevant DOJ sections (AMFLS, the Public Integrity Section and the Fraud Section) – all of which have the required powers to identify, trace and initiate freezing and seizing of assets related to corruption at their disposal. The three DOJ units partner with relevant LEAs and FBI's International Corruption Squads in their investigations.

*Weighting and Conclusion:*

All five criteria are met.

***Recommendation 30 is rated compliant.***

***Recommendation 31 - Powers of law enforcement and investigative authorities***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements which were expanded substantially in 2012 and now require LEAs to have a much wider range of powers.

*Criterion 31.1* - The competent authorities may compel the production of records, the search of persons and premises, and the seizing and obtaining of evidence via the use of basic investigate tools and powers including: subpoenas; search, seizure and arrest warrants; and a FBI-specific administrative subpoena to be used in case of terrorism related investigations and national security letters. Relevant LEAs have the power to interview and take witness' statements for use in a criminal investigation and prosecution, and in civil litigation.

*Criterion 31.2* - LEAs have authority to use a wide array of investigative techniques including undercover operations, communication intercepts (18 USC 2510), pen register of phone communication (18 USC 3123), controlled deliveries by mail (39 CFR 233.3), and controlled deliveries in the context of undercover operation: Attorney General 1992 Guidelines on FBI Undercover Operations. Access to computer systems requires a search warrant unless consent of the owner is given. Communication intercepts requires a court order unless one of the parties to the communication consent to the interception.

*Criterion 31.3* - All investigators are trained to conduct financial investigations and/or background investigations to determine to identify assets, and the person who holds and controls (meaning the account holder and any person(s) authorized to use the account, such as the signatories to the account) using traditional investigative techniques (see c.31.1) and without pre-notifying the account holder.<sup>124</sup> Beyond these, they have access to numerous commercial databases and non-

<sup>124</sup> Rule 17 of the Federal Rules of Criminal Procedure 12 USC §3420(i)(2) and 18 USC §1510(b).

commercial databases at Federal and State levels are accessible by authorities to assist with identification of persons and assets to identify assets without notifying the account holder. Where all traditional means of investigations have been exhausted, and where there is credible evidence of terrorist or ML activity, the U.S. has an additional powerful mechanism to identify whether natural or legal persons hold or control accounts, and identify transactions carried out by natural or legal persons or entities suspected of ML/TF. It is however available only in limited circumstances: s.314(a) Program 31 CFR §1010.520 (see R.29-IO.6). Pre-notification to the account holder is not necessary.

*Criterion 31.4* - Federal, State and local LEAs can have direct online access to all BSA data and other reporting information held by FinCEN through FinCEN's Portal (see R.29). BSA data includes CMIR data and a wide range of financial, administrative and LEA information as described under criteria 29.2 and 29.3. On-site access to FinCEN database is also possible.

#### *Weighting and Conclusion:*

Law enforcement and investigative authorities have all powers required to conduct ML/TF investigations. While there are mechanisms in place to identify account holders and their assets, there is no general mechanism to do so. S.314(a) is powerful tool which somewhat mitigates this deficiency, but it is available in limited circumstances only.

***Recommendation 31 is rated largely compliant.***

#### ***Recommendation 32 – Cash couriers***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements.

*Criterion 32.1* - The U.S. has implemented a declaration system applicable to all persons, natural or legal for all incoming and outgoing cross-border transportation of currency and other monetary instruments whether by travelers, or through mail and cargo. The full range of currency and BNI is covered: 31 CFR 1010.100 (mm) & 31 CFR 1010.100(dd).

*Criterion 32.2* - The U.S. has a written declaration system for all cross-border transportations of currency/BNI above USD 10 000 in aggregate, whether the person is acting on his/her own or on behalf of a third party: 31 CFR 1010.340(a). Whoever receives currency/other monetary instruments in excess of USD 10 000 from a place outside the U.S. must also file a Report of International Transportation of Currency or Monetary Instrument (CMIR) within 15 days of receipt to CPB: 31 CFR 1010.340 (b).

*Criterion 32.3* - The U.S. has a declaration system in place.

*Criterion 32.4* - Upon discovery of a false declaration/disclosure of currency or monetary instruments or a failure to declare/disclose them, the funds are subject to seizure/forfeiture and the carrier to arrest/prosecution": 31 USC 5317. The carrier is interviewed to establish the source of the funds and its intended purposes and an investigation is initiated.

*Criterion 32.5* - Dissuasive and proportionate penalties are applicable to whoever makes a false declaration. Currency and monetary instruments subject to reporting may be seized and forfeited if a

report is not filed or contains omissions or misstatements: 31 CFR 1010.830 & 31 USC 5317(b). The civil penalty for such violations may not be more than the amount of the monetary instrument for which the report was required though it may be reduced to the amount forfeited for the violation: 31 USC 5321 (a)(2). Criminal penalties for failing to file a CMIR or causing or attempting to cause a person to file a false CMIR or structuring or assisting any important or exportation of monetary instrument a person to fail to do so include a set fine, imprisonment for not more than 5 years, or both: 31 USC 5324 (d)(1). The penalty doubles if the CMIR violation is combined with any other violation or as part of a pattern of any illegal activity involving more than USD 100 000 in a 12-month period. The fine applicable is less than USD 500 000 for an individual or USD 1 000 000 for an organization and up to a 10 years sentence, or both: USC 5423 (d)(2) & 18 USC 3571 (b)(3) and (c)(3). A criminal penalty of up to 5 or 8 years imprisonment may apply to any material false statement to a U.S. government official (18 USC 1001) while the range of criminal penalties associated with customs violation can also apply: 19 USC §1401(c); 18 USC 542, 545, 554. A penalty of no more than 5 years imprisonment applies to whoever, with the intent to evade the CMIR requirement, knowingly conceals more than USD 10 000 in currency/BNI on the person of such individual or in any conveyance, article of luggage, merchandise, or other container, and transports or transfers or attempts to transport or transfer such currency or monetary instruments from a place within the U.S. to a place outside the country, or vice-versa: 31 USC 5332 (b)(1).

*Criterion 32.6* - CBP transmits all CMIR data electronically to FinCEN. CBP and ICE seizure and arrest reports are also maintained in the TECS (Treasury Enforcement Communications System) database which is accessible to a number of Federal partner agencies including FinCEN.

*Criterion 32.7* - There is adequate coordination among customs, immigration and other relevant authorities. CPB (charged with the management, control and protection of the U.S. borders at and between points of entry) shares a common data management platform with ICE (responsible for investigating the illegal movement of people and merchandise, including currency and other monetary instrument, across the border). ICE also works closely with the DEA's El Paso Intelligence Center which collects and analyses cash data seizures from the Southwestern border. FinCEN provides access to CMIR information system to a host of Federal, State and local law enforcement authorities as well.

*Criterion 32.8* - ICE and CBP have the authority through a number of statutes to stop or restrain unreported or falsely reported currency for a reasonable time: 19 USC 1581 e, 31 USC 5316, 31 USC 5317 d, 31 USC 5332. If there is suspicion that the funds may be related to ML, TF, or associated predicate offenses, civil forfeiture procedures apply (see R.4).

*Criterion 32.9* - The U.S. declaration system allows for international cooperation. Information can be exchanged multilaterally and bilaterally via ICE and CBP attachés posted in U.S. Embassies and Consulates, as well as engagement through Europol, INTERPOL, World Customs Organization Liaison Officers, and pursuant to Customer MLAs, MLATs, and other agreements. CMIR data can also be shared with other FIU. The information is retained in all the instances set out in c.32.9.

*Criterion 32.10* - CMIR reporting requirements pose little burden to legitimate international travel and trade, and do not impede freedom of capital movements. There are strict safeguards to ensure



proper use of the information or data that is reported or recorded: Substantial penalties apply in case of misuse or abuse of information: BSA and Privacy Act.

*Criterion 32.11* - Persons trying to launder funds/BNF by transporting them across the U.S. border may be subject to the penalties applicable for violating the international ML offenses: 18 USC 1956 (2) (see R.3). Persons found with TF-related currency or monetary instruments may be subject to the penalties under the TF offenses: 18 USC 2339A, B and C (see R.5 and R.4). Aside from civil and criminal forfeiture for violating the international ML offense (18 USC 981(a)(1); 982(a)(1)), many other asset forfeiture provisions apply in the case of smuggling of cash/BNF related to ML/TF including civil penalties for not filing or filing a false report (31 USC 5321 and 31 CFR 1010.820), criminal penalties for concealed transportation with the intention of avoiding requirements (31 USC 5322 and 31 CFR 1010.840), search and forfeiture of monetary instruments (31 USC 5318 & 31 CFR 1010.830), and criminal penalties for not filing or filing a false CMIR (31 USC 5324(c)).

#### *Weighting and Conclusion:*

All 11 criteria are met.

***Recommendation 32 is rated compliant.***

#### ***Recommendation 33 - Statistics***

In its 3rd MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies related to inadequate statistics on freezing, seizing, confiscation, BSA data, MLA and extradition.

*Criterion 33.1* - The U.S. maintains comprehensive statistics on the number of:

- a) SARs received, analyzed and disseminated/broken down by type of reporting entity, number of filings by U.S. States and territories, violation reported, suspicious wire transfers, year and month of filing;
- b) Investigations, prosecutions and convictions related to the Federal ML offenses broken down by year, investigating agency, type of offense, number of persons charged and convicted, conviction rate, and sentence (but not by predicate offense). Statistics at State level are not uniformly available;<sup>125</sup>
- c) Investigations, prosecutions and convictions related to the Federal TF offenses broken down by year, type of offense, number of persons charged and convicted, conviction rate, and sentence;
- d) Property frozen, seized and confiscated broken down by Federal seizing agency, forfeiture type (administrative, civil/judicial, criminal), number and value of seized and forfeited assets, but not broken down by ML, predicate for ML and non-predicate for ML: DOJ-AFF statistics. Statistics at State level are not uniformly available;

<sup>125</sup> [Department of Justice Bureau of Justice.](#)

- e) The number of incoming and outgoing MLA and extradition requests relating to both ML and TF, broken down by the grounds for the request and whether it was granted or refused: DOJ-OIA electronic case tracking system; and
- f) The number of requests for assistance made to and received by FinCEN to/from foreign FIUs, including the number of spontaneous referrals.

### *Weighting and Conclusion:*

The U.S. does not maintain comprehensive statistics on the investigations, prosecutions and convictions related to the State ML offenses, or statistics on the property frozen, seized and confiscated at the State level.

***Recommendation 33 is rated largely compliant.***

### ***Recommendation 34 – Guidance and feedback***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements.

*Criterion 34.1* - The U.S. authorities, including supervisors and SRBs, have issued a significant amount of guidance and feedback to assist FIs and DNFBPs in applying national AML/CFT measures and in detecting and reporting suspicious transactions. The majority of this information is publicly available and widely disseminated.

- a) FinCEN: The assessors reviewed about 90 pieces of guidance issued by FinCEN since the previous MER which included sector-specific and general guidance on: recognising suspicious activity; registration requirements for MSBs; application of correspondent banking rules, and CDD obligations etc. FinCEN has published [SAR guidance](#), [BSA forms](#), and [FAQs](#) on its website and on its Secure Information Sharing System. FinCEN also provides direct support to FIs and DNFBPs through the FinCEN Resource Center, a staffed call center which accepts queries by phone, e-mail, or fax.
- b) Guidance on SAR: FinCEN, other Federal financial regulators, and LEAs provide FIs and DNFBPs with formal and informal guidance on the proper filing of SARs and may provide direct or aggregated feedback on filed SARs. Emerging trends in SAR filings are also relayed through FinCEN's outreach to industry (primarily through [speaking events, conferences, and training](#).) Periodically, FinCEN publishes reports to share information gathered as part of its [outreach initiative](#). Direct feedback from FinCEN to individual SAR filers includes filer quality reports. Additional feedback and guidance is provided within the context of individual FI examinations conducted by Federal and State supervisory and examination authorities. FinCEN provides general information in their SAR [guidance](#), bulletins [and forms](#), advisories, [guidance](#) on general applicability issues, and [FAQs](#) on specific issues. FinCEN has a special "hotline" to receive urgent reports of potential TF or major ML activity.
- c) FFIEC publishes a BSA/AML Examination Manual for the use of bank examiners. The Manual, which is updated on a regular basis, also contains guidance for the industry and the

regulatory expectations are upheld through the supervisory enforcement process. The Manual also addresses OFAC requirements for proliferation/WMD obligations.

- d) FinCEN and the IRS published the BSA/AML Examination Manual for MSBs for use by examiners, which also aids MSBs in meeting their AML/CFT obligations. For the insurance sector the NAIC examination manual contains expectations which essentially mirror the sector's BSA/AML obligations.
- e) Federal Functional Regulators also publish AML guidance (for example, FBAs inter-agency statement of 2007 on enforcement of BSA/AML requirements, 2009 guidance on cross-border payment messages, 2010 multi-agency non-binding guidance on *obtaining and retaining BO information* and 2015 the FDIC's statement to encourage institutions to take a risk-based approach on issue of de-risking.
- f) FHFA: In 2015, FHFA issued an advisory bulletin reminding FHL banks of their obligations to establish AML programs and file SARs.
- g) SEC and FINRA: SEC publishes AML guidance for securities broker-dealers and mutual funds. FINRA does the same for its member broker-dealers. SEC staff and FINRA also have regular, periodic meetings with industry groups to provide feedback on AML issues. SEC and FINRA each publish their respective examination priorities which have historically included AML issues. and also publish disciplinary actions on their respective websites.
- h) Guidance is provided on the IRS web site, to educate and assist persons who have the obligation to file Form 8300; and for the tax professionals (such as lawyers or accountants) who prepare and file Form 8300 on behalf of their clients.

### *Weighting and Conclusion:*

Sectors not subject to comprehensive BSA requirements are only covered to some extent because of the limited application of the Form 8300 reporting guidance related to cash transactions. There is a case to align guidance more to vulnerabilities in the minimally covered DNFBP sectors.

***Recommendation 34 is rated largely compliant.***

### ***Recommendation 35 – Sanctions***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiency was that some banking and securities participants were not subject to all AML/CFT requirements and related sanctions at the Federal level.

***Criterion 35.1*** - A range of proportionate and dissuasive criminal, civil and administrative sanctions are available, ranging from disciplinary letters to fines and imprisonment.

- a. ***Targeted Financial Sanctions (R.6):*** All U.S. persons (natural and legal) are prohibited from dealing with persons designated under OFAC's economic sanctions programs. Failure to comply with this may attract penalties, including: a cautionary letter; CMP; referral to the appropriate LEA for criminal investigation and/or possible prosecution; license denial, suspension, modification, or revocation; and a C&D order: 50 USC §1705; 31 CFR §501. Willful

violation of an executive order or implementing regulation issued pursuant to the IEEPA is a criminal offense: 50 USC§1705(c). **For banks**, OFAC and the FBAs have the authority to pursue a broad range of penalties in case of sanctions violations including: cease & desist orders, penalty and removal actions: 31 CFR §501; 12 USC §1818. In the **securities sector**, the SEC examines securities broker-dealers for compliance with OFAC regulations and may also make referrals to OFAC of any potential misconduct identified.

- b. **NPOs (R.8):** IRS may deny/revoke/suspend the tax-exempt status of NPOs not appropriately operating in furtherance of their exempt purposes including if found to be affiliated with terrorism or is designated under R.6: IRC s.501(p). NPOs failing to file the annual Form 990 series or related forms are subject to civil fines of USD 20 per day (up to the lesser of USD 10 000 or 5% of its annual gross receipts) or USD 100 per day (up to USD 50 000 if its annual gross receipts exceed USD 1 million), and/or revocation of tax-exempt status if returns are not filed for 3 consecutive years (See [link](#)). The IRS and DOJ can also impose additional criminal and civil liability under the IRC on tax-exempt U.S. charitable organizations that file false tax forms with the IRS in which the organization conceals their affiliation with a FTO or SDGT, or with a foreign entity connected to an FTO or SDGT.
- c. **Preventive Measures and Reporting (R.9-23):** **FinCEN** may bring an enforcement action for BSA violations. It has sole Federal enforcement authority over FIs and covered DNFBPs. Besides CMPs, FinCEN can take other formal and informal administrative actions: 31 USC §5320. A range of BSA criminal penalties are also available for criminal conduct involving BSA violations. **FBAs and SEC** are empowered under their respective Act for taking a range of supervisory actions, including C&D, CMP, and removal, suspension and prohibition. **FINRA** has independent authority for bringing BSA related enforcement actions. **SEC** can also bring actions for BSA violations (for example, Exchange Act Section 17(a)/ Rule 17a-8) and can bring enforcement actions against SRO for its failure to exercise oversight over members: *Exchange Act* s.19(h). **CFTC** has power to enforce compliance through its enforcement authorities. **CME Group and NFA** can bring disciplinary complaints against members for BSA violations. **DOJ** has authority to bring criminal actions against FIs willfully failing to comply with the statutory and regulatory obligations under Title 31 of the BSA: 31 USC §5322. **DOJ** has criminal enforcement authority for ML violations under 18 USC §§1956 and 1957, and the ability to prosecute unlicensed and/or unregistered MSB under 18 USC §1960. IAs (other than those covered indirectly) and DNFBPs, other than casino and dealers in precious metals and stones are not subject to comprehensive AML/CFT requirements.

*Criterion 35.2* - FinCEN is authorized to seek CMP and equitable and administrative relief against institutions, partners, directors, officers, and employees of FIs and DNFBPs for conduct violating the BSA<sup>126</sup>. These violations can include record-keeping, reporting, or failure to maintain an adequate AML program. FBAs are authorized to take formal administrative action against any officer, director, employee, controlling stockholder, or agent of any depository institution, and in certain cases, any independent contractor (collectively “institution-affiliated party” or IAP) of any depository

<sup>126</sup> 31 USC §5321; 31 CFR §1010.810(d); 31 CFR §1010.820(h).

institution<sup>127</sup>. Such sanctions include C&D orders, orders of suspension, removal or prohibition, and CMPs. Enforcement actions, remedies and sanctions may be ordered against securities broker-dealers, investment companies, and any persons “associated” with them such as directors, senior management and other employees. FINRA is authorized to impose appropriate sanctions on any member firm/associated person for violation of the Federal securities laws and its own rules. IAs (other than those covered indirectly through affiliations with banks, bank holding companies and broker-dealers, when they implement group wide AML rules or in case of outsourcing arrangements) and DNFBPs, other than casinos and dealers in precious metals and stones are not subject to comprehensive AML/CFT requirements. All U.S. persons are prohibited from dealing with persons designated under OFAC’s economic sanctions programs, which includes TFS pursuant to R.6, and designations for involvement in other crime (for example, under the Kingpin Act).

#### *Weighting and Conclusion:*

Investment advisers (other than those covered indirectly) and DNFBPs (other than casinos and dealers in precious metals and stones) are not covered by the full range of AML/CFT obligations, and consequently the related sanctions do not apply to them.

***Recommendation 35 is rated largely compliant.***

#### ***Recommendation 36 – International instruments***

In its 3rd MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies were that not all conduct specified in the Vienna and Palermo Conventions had been criminalised, there were gaps in the scope of foreign predicates related to organized criminal groups, and there was a technical deficiency concerning implementation of targeted financial sanctions (which is no longer assessed under this Recommendation, but which is now addressed in R.6).

*Criterion 36.1* - The U.S. has signed and ratified the Vienna Convention (December 1988 and February 1990 respectively), the Palermo Convention (December 2000 and November 2005 respectively), the TF Convention (January 2000 and June 2002 respectively), and the Merida Convention (December 2003 and October 2006 respectively).

*Criterion 36.2* - The U.S. has fully implemented the TF Convention. Not all conduct specified in Article 3 (Vienna) and Article 6(b)(i) (Palermo) is criminalized (see R.3). The U.S. has broadly implemented the obligations of the Merida Convention.

#### *Weighting and Conclusion:*

The U.S has minor deficiencies in its implementation of the Vienna and Palermo conventions.

***Recommendation 36 is rated largely compliant.***

<sup>127</sup> 12 USC §§1813(u), 1818(b), (c), (e), (g), and (i), and 1786(b), (e), (f), (i), (o), and (r).

**Recommendation 37 – Mutual legal assistance**

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiency related to potential barriers to granting MLA request linked to the laundering of proceeds that are derived from a designated predicate offense that is not covered.

*Criterion 37.1* - The U.S. has a legal basis that would permit for the rapid provision of a wide range of MLA in relation to the investigation, prosecution and related proceedings for ML, TF and associated predicate offenses. A statutory legal framework applies to all MLA requests regardless of whether they are based on a letter rogatory, or letter of request: 18 USC §3512. MLA treaties (MLATs) themselves are also a legal framework under which MLA requests may be executed. Where a bilateral treaty is not in place, the basis for cooperation may often be found in multilateral or regional conventions<sup>128</sup>, and agreements<sup>129</sup>. Additionally, U.S. courts are authorized to provide direct MLA to international tribunals: 28 USC §1782.

*Criterion 37.2* - The U.S. has a central authority for transmitting and executing MLA requests—DOJ-OIA through which must be channeled all requests in criminal matters for legal assistance requiring compulsory measures. DOJ-OIA has a prioritisation system in place for incoming and outgoing requests by which Treaty requests are prioritized above non-treaty requests. Crimes of violence, including terrorism cases, are given a high priority. High priority cases are dealt with by order of arrival or urgency (e.g. trial deadline). There is flexibility to deviate from these prioritizations in exceptional circumstances. However, due to their current IT system, the U.S. is only able to monitor progress and time taken to handle a request.

*Criterion 37.3* - MLA is not prohibited or made to be subject to unduly restrictive conditions. MLA may be provided to foreign investigative authorities in criminal matters, including before a charge is laid and does not specify dual criminality as a condition: 18 USC §3512. Some restrictions may be provided for in treaties and conventions. Where dual criminality applies, this is mainly restricted to requests for assistance requiring the application of compulsory or coercive measures.

*Criterion 37.4* - The U.S. does not refuse requests for MLA on the sole ground that the offense is also considered to involve fiscal matters, even where the applicable MLATs exclude fiscal matters from the scope of assistance<sup>130</sup>. Separate Tax Treaties or Conventions on Tax Information Exchanges also provide additional information exchange mechanisms, including on tax offenses. Likewise, MLA requests are not refused on the sole grounds of secrecy or confidentiality requirements on FIs or DNFBP, except where information is protected by the attorney-client privilege. Attorney-client

<sup>128</sup> Including but not exclusively: the Inter-American Convention on Mutual Assistance in Criminal Matters ("The OAS MLAT"), the Vienna Convention [arts 7-8], the Convention Combating Bribery of Foreign Public Officials in International Business Transactions (OECD) [arts. 9, 11]; the International Convention for the Suppression of the Financing of Terrorism [arts. 12-16]; the Palermo Convention [arts. 18, 21]; Convention Against Corruption (Merida) [arts. 46-49]; Council of Europe Convention on Cybercrime [arts. 25-35].

<sup>129</sup> As of May 2015, the U.S. had 70 such accords in place with 85 territories

<sup>130</sup> For instance the MLATs between the U.S. and Switzerland, the Bahamas and the Cayman Islands exclude fiscal matters, including offences involving taxes, customs duties, governmental monopoly charges and/or exchange control regulations, from the scope of available assistance. Assistance is however generally available for criminal tax matters relating to the proceeds from criminal offences.



privilege may be overcome if it can be shown that the attorney was actively participating in the criminal activities of his/her client.

*Criterion 37.5* - The U.S. maintains the confidentiality of MLA requests received, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. Most MLATs signed by the U.S. contain confidentiality provisions that can be invoked by the requested State. Additionally, subpoenas for documents or testimony, restraining orders, and other compulsory measures may be issued or undertaken with a court order sealing the matter from public disclosure for a certain period of time. Where legal process is required, sealing orders are routinely issued on the basis of the country's invocation of a treaty's confidentiality provision and factual circumstances that counsel confidentiality.

*Criterion 37.6* - Where MLA requests do not involve coercive actions, the U.S. does not make dual criminality a condition for rendering assistance. Most of the bilateral MLATs do not require dual criminality as a condition for granting assistance. Where dual criminality is a condition, this is usually restricted to requests for compulsory or coercive measures. In such instances, gaps in the ML offenses can adversely impact MLA particularly when the foreign request is based on ML activity derived from a predicate offense that does not fall within the definition of SUA or the foreign request does not identify the underlying predicate offense (see R.3 and R.36). Conduct-based dual criminality applies when issuing search warrants necessary to execute a foreign request: 18 USC 3512(e). There is no dual criminality requirement for most court orders issued pursuant to 18 USC §3512 in aid of requests for assistance from foreign authorities.

*Criterion 37.7* - Where dual criminality applies, technical differences between the offense's categorization in the requesting State do not prevent the U.S. from providing the requested assistance. It is enough to determine that the underlying acts are criminalized in both States. The U.S. has not denied any MLA requests on the basis of dual criminality (ML, TF and asset forfeiture).

*Criterion 37.8* - The powers and investigative techniques required under R.31 and which are otherwise available to domestic competent authorities are also available for use in response to MLA requests. When a compulsory process is necessary, an OIA attorney or a Federal prosecutor is routinely appointed as a commissioner to seek any order necessary to execute the request: 18 USC §3512. Where LEAs have entered into case specific MOUs with other countries for ML and TF investigative assistance, additional investigative tools and powers may be used. However, the interception of communications can only be undertaken as a part of a U.S. investigation.

### *Weighting and Conclusion:*

The minor shortcomings identified in R.3 could limit assistance when dual criminality applies. The interception of communications can only be undertaken as part of a U.S. investigation. The OIA case management system is being improved to facilitate the electronic monitoring of the processing of outgoing and incoming requests process and the monitoring of the time taken to handle these.

***Recommendation 37 is rated largely compliant.***

### ***Recommendation 38 – Mutual legal assistance: Freezing and Confiscation***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiency related to potential barriers to granting MLA request linked to the laundering of proceeds that are derived from a designated predicate offense which is not covered.

*Criterion 38.1* - The U.S. has a range of authorities to take action in response to requests by foreign countries to identify, freeze, seize or confiscate laundered property, proceeds, and instrumentalities used or intended for use in ML, TF or associated predicate offenses, or property of corresponding value including:

- a) Providing assistance in identifying and tracing assets mainly via informal police-to-police communication and information sharing networks. Additionally, the U.S. may obtain evidence for court proceedings on behalf of a foreign request including testimony, documents, or tangible items: *18 USC 3512 (see R.37)*.
- b) Restraining or seizing assets located in the U.S. upon the request of a foreign country for preservation purposes: *28 USC 2467(d)(3) A)(i)*.
- c) Enforcing foreign confiscation orders. The U.S. may also restrain untainted property as long as these are subject to forfeiture and provided all other requirements are met: *28 USC 2467*.
- d) Enforcing a foreign confiscation judgment on the condition that the requesting country is party to the *Vienna Convention*, a MLAT or other international agreement with the U.S. that provides for confiscation assistance. The offense must: i) be an offense for which forfeiture would be available under U.S. Federal law if the criminal conduct occurred in the U.S.; or ii) is a foreign offense that is a predicate for a U.S. ML offense: *28 USC 2467 (a)(2) & 18 USC 1956(c)(7)(B)*.
- e) Initiating its own civil forfeiture proceedings against any property, proceeds and instrumentalities: *18 USC 981(b)(4)*. In such cases, the U.S. can proceed if it can state sufficiently detailed facts to support a reasonable belief that the property would be subject to forfeiture under U.S. Federal law, based on its own evidence and evidence from the requesting State, of a predicate offense for confiscation under U.S. law which would make that the property subject to confiscation.

Gaps in the ML offenses and the requirement for dual criminality are potentially an issue when the predicate offense is not one covered in the U.S. However, no MLA request has been denied on the basis of dual criminality (ML, TF and asset forfeiture).

*Criterion 38.2* - The U.S. has authority to provide assistance to requests for cooperation made on the basis of non-conviction-based (NCBF) proceedings and related provisional measures *18 USC 981(b)(4)(A)-(B)*. Provisional measures may also be carried out under the enforcement of a foreign judgment any time, before or after, the initiation of enforcement proceedings by a foreign nation, including NCBF proceedings: *28 USC 2467(d)(3)(A)(1)*.

*Criterion 38.3* - The U.S. has arrangements for coordinating seizure and confiscation actions with other countries; and for managing and disposing of property frozen, seized, or confiscated whether by on its own behalf or on behalf of a foreign government.

*Criterion 38.4* - The U.S. shares the proceeds of successful forfeiture actions with countries that made possible, or substantially facilitated, the forfeiture of assets under U.S. law as set out in free-standing international asset sharing agreements or asset sharing provisions within mutual legal assistance agreements and multilateral treaties by 18 USC §981(i), 21 USC §881(e)(1)(E), and 31 USC §9703(h)(2). AFMLS may negotiate case specific, bilateral asset sharing arrangements even in the absence of specific agreement/treaty.

#### *Weighting and Conclusion:*

In the context of dual criminality requirements, the gaps identified under R.3 may be a barrier to providing freezing and confiscation assistance, particularly when the predicate offense is not covered in the U.S.

***Recommendation 38 is rated largely compliant.***

#### ***Recommendation 39 - Extradition***

In its 3<sup>rd</sup> MER, the U.S. was rated largely compliant with these requirements. The technical deficiencies related to potential barriers to granting extradition request linked to laundering proceeds derived from a designated predicate offense which is not covered, and the list-based treaties not covering ML.

*Criterion 39.1* - The U.S. has mechanisms that enable it to execute extradition requests in relation to ML/TF without delay:

- a) ML and TF are extraditable offenses. The extradition treaties in force between the U.S. and other countries define extraditable offenses by either including felonies (offenses for which punishment is at least one year or more of imprisonment in both countries) or by listing the extraditable offenses by name (approximately 55 treaties). In the first category of treaties, a dual-criminality approach ensures that ML and TF offenses are extraditable if both treaty partners criminalize the underlying ML or TF activity. In the context of the second category of list treaties, the ability to extradite for money laundering and terrorist financing offenses will depend on whether the U.S.s and the extradition treaty partner are State Parties to an applicable multilateral convention which address ML in the context of narcotics trafficking, transnational organized crime, alien smuggling, trafficking in persons, corruption, and cybercrime. Likewise, the *TF Convention* deems TF to be an extraditable offense in the bilateral extradition treaty in force between the U.S. and the extradition treaty partner if both are parties to that convention. This approach may result in occasional gaps.
- b) The OIA has an electronic case management system and clear processes for the timely execution of extradition requests although it cannot be used to monitor time taken to comply with a request. Priority is given to requests premised on serious offenses. TF and ML cases are presumptively serious cases. A judge needs to ascertain key elements prior to certifying an extradition: *18 USC 3181*. The handling of extradition case takes approximately one to four months if a fugitive elects a “simplified extradition” procedure, and at least one year when the extradition is contested.

- c) There are no unreasonable or unduly restrictive conditions on the execution of extradition requests.

*Criterion 39.2* - The U.S. extradites its nationals even where the applicable treaty or convention does not obligate it to do so. Where the applicable treaty does not expressly grant discretionary authority to extradite a U.S. national, the Secretary of State may refuse to issue a surrender warrant for a U.S. national after a U.S. court has determined a fugitive extraditable: 18 USC 3196.

*Criterion 39.3* - Where a dual criminality extradition treaty applies, technical differences between the categorization of the crime in the U.S. and requesting State do not affect the provision of the requested assistance. It is enough if the particular act charged is criminal in both jurisdictions: *Factor v. Laubheimer*, 290 U.S. 276 (1933). Out of over 1 000 incoming extradition cases, during this assessment period, the U.S. denied one based on lack of dual criminality in tax crimes.

*Criterion 39.4* - The U.S. has simplified extradition mechanisms available via a waiver of or consent to extradition, with consent of the fugitive. In urgent circumstances, bilateral extradition treaties (at times in conjunction with 18 USC 3187), permit fugitives to be provisionally arrested in advance of the receipt of a formal extradition request with such provisional detention to last no more than 90 days: 18 USC 3187. Under more recent extradition treaties, provisional arrest requests may be transmitted directly to OIA by the requesting country.

#### *Weighting and Conclusion:*

The absence of multiple bilateral extradition treaties explicitly listing ML/TF as extraditable offenses is mitigated by the fact that major partners are party to multilateral conventions which address ML (in the context of narcotics trafficking, transnational organized crime, alien smuggling, trafficking in persons, corruption, and cybercrime) and/or TF.

***Recommendation 39 is rated largely compliant.***

#### ***Recommendation 40 – Other forms of international cooperation***

In its 3<sup>rd</sup> MER, the U.S. was rated compliant with these requirements. The requirements in new Recommendation 40 are considerably more detailed.

##### *General principles*

*Criterion 40.1* - The U.S. has mechanisms that allow the FIU, LEAs, and financial supervisory authorities to provide to foreign counterparts a wide range of cooperation directly or diagonally. In general, exchanges of information concerning ML/TF may be provided promptly, either spontaneously or upon request, and without unduly restrictive conditions: 31 CFR. §1010.520 (FinCEN); 31 USC §310 and Treasury Order 180-01 (FIU); 12 USC §1818(v)(2) (supervisors).

*Criterion 40.2* - The below framework facilitates other forms of international cooperation:

- a) The competent authorities have a lawful basis for providing cooperation: 31 USC §310(c)(FinCEN); s.21(a)(2) *Securities Exchange Act of 1934*(SEC); s.8(e) and 12(f) *Commodity Exchange Act*, 7 USC §§ 12(e) and 16(f) (CFTC); information sharing arrangements (FBAs).

- b) Nothing prevents them from using the most efficient means to cooperate.
- c) All authorities use clear and secure gateways, mechanisms or channels for cooperation including the Egmont Secure Web and multiple established information sharing networks such as INTERPOL. FBAs seeking assistance may indicate to counterparts their preferred manner in which information is to be transmitted.
- d) The competent authorities have processes for prioritising and executing requests including applying the Egmont Group's Principles of Information Exchange prioritisation processes. FinCEN's response times are about 2 months for routine requests, one to two days for urgent requests (e.g. impending court dates or law enforcement actions), and two days to a week for TF-related requests. FBAs information sharing agreements with and foreign authorities seek timely cooperation and notification. U.S. LEAs foreign-based attachés led to developed companion channels that permit effective and expeditious information exchange both informally and once the formal request is received.
- e) The competent authorities have clear processes for safeguarding the information received.

*Criterion 40.3* - FinCEN, the FBAs and LEAs all have comprehensive networks of bilateral and multilateral agreements, MOUs and protocols to facilitate international cooperation with a wide range of foreign counterparts.

*Criterion 40.4* - All U.S. competent authorities will provide feedback in a timely manner if requested by foreign counterparts from whom they have received assistance.

*Criterion 40.5* - U.S. competent authorities do not refuse requests for cooperation on the grounds listed in this criterion. If a U.S. investigation was in the covert stage, a competent authority may delay or reasonably condition the provision of assistance to a foreign authority if to do otherwise would alert the subjects of the investigation, but would not categorically refuse assistance.

*Criterion 40.6* - FinCEN, FBAs, CFTC, SEC, and LEAs have controls and safeguards to ensure that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorization has been given by the requested competent authority: 31 USC §310(c); 12 USC §1818(v); Title 18 USC §1906; *Exchange Act* s.24(d); *Commodity Exchange Act*, 7 USC § 12(a)(1); 18 USC §3512.

*Criterion 40.7* - The competent authorities are required to maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning confidentiality, privacy, and data protection. Information from foreign counterparts is protected in the same manner as information from domestic sources. The authorities are able to refuse to provide information if the requesting authority cannot protect the information effectively<sup>131</sup>.

<sup>131</sup> *Right to Financial Privacy Act* 12 USC §§3401-3422; *Privacy Act* 5 USC §552a; *Federal Information Security Management Act* 44 USC §§3541-3549; *Bank Secrecy Act* 31 USC §§5311-5332 & 31 USC §310(c); *Federal Information Security Management Act*.

*Criterion 40.8* - The competent authorities are able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically<sup>132</sup>.

*Exchange of information between FIUs*

*Criterion 40.9* - FinCEN has an adequate legal basis for providing co-operation on ML, associated predicate offenses and TF.<sup>133</sup>

*Criterion 40.10* - FinCEN provides feedback to its foreign counterparts, upon request, whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

*Criterion 40.11* - FinCEN has the power to exchange all information required to be accessible or obtainable directly or indirectly by it, particularly under Recommendation 29, and any other information which it has the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity: 31 CFR §1010.520 (information sharing).

*Exchange of information between financial supervisors*

*Criterion 40.12* - Financial supervisors (FBAs, SEC, CFTC, FinCEN and State life insurance supervisors) have a legal basis for providing co-operation with their foreign counterparts (regardless of their respective nature or status), consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes<sup>134</sup>.

*Criterion 40.13* - Financial supervisors (FBAs, SEC, CFTC, FinCEN) are able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, in a manner proportionate to their respective needs<sup>135</sup>.

*Criterion 40.14* - Financial supervisors (FBAs, SEC, CFTC, FinCEN) are able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other supervisors that have a shared responsibility for financial institutions operating in the same group:

- a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors is public and can be shared without restriction.
- b) prudential information, in particular for Core Principles supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness<sup>136</sup>, and

<sup>132</sup> FinCEN: 31 USC §310(c); FBAs: s.8(v) *Federal Deposit Insurance Act* 12 USC. §1818(v); SEC: s.21(a)(2) *Exchange Act* 15 USC §78u(2); LEAs: 28 USC §1782 & Title 18 USC §3512; CFTC: s.12(f) *Commodity Exchange Act*, 7 USC § 16(f);

<sup>133</sup> 31 USC §310, 31 CFR §1010.950, Treasury Order 180-01, FinCEN's System of Records (Treasury/FinCEN.001), 31 USC §5311 (Declaration of Purpose); and 31 CFR §1010.520 (information sharing).

<sup>134</sup> FBAs – S.8(v) *Federal Deposit Insurance Act* 12 USC §1818(v), SEC – s.21(a)(2) *Exchange Act* 15 USC §78u(2); FinCEN – 31 CFR §1010.520 (information sharing).

<sup>135</sup> FBAs – s.15 *International Banking Act* 12 USC §3109; FinCEN - 31 USC §310 and Treasury Order 180-01; FinCEN – 31 CFR. §1010.520 (information sharing).



- c) AML/CFT information, such as internal AML/CFT procedures and policies of FIs, CDD information, customer files, samples of accounts and transaction information<sup>137</sup>.

*Criterion 40.15* - The financial supervisors are able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, authorize or facilitate foreign counterparts in conducting inquiries themselves in the U.S. to facilitate effective group supervision<sup>138</sup>.

*Criterion 40.16* - The financial supervisors ensure that they have the prior authorization of the requested financial supervisor for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information.

*Exchange of information between law enforcement authorities*

*Criterion 40.17* - Federal LEAs are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, associated predicate offenses or TF, including the identification and tracing of the proceeds and instrumentalities of crime. Requests for simple investigative assistance and information sharing can be made by foreign police authorities to their DEA, FBI, IRS-CI, or HSI/ICE counterparts in-country, who can pass the request for informal assistance to the appropriate agents in the U.S. If compulsory measures are necessary, the foreign government can make a treaty request or send a letter rogatory. The U.S. has LEA and DOJ attachés posted around the globe who can facilitate assistance in support of foreign investigations. It will also provide informal assistance and information through the CARIN for inquiries relating to the identification and tracing of the proceeds and instrumentalities of crime.

*Criterion 40.18* - The LEAs are able to use their powers, including any investigative techniques available (see Rec31), to conduct inquiries and obtain information on behalf of foreign counterparts. LEAs respect principles and restrictions set out in agreements with Interpol, Europol or Eurojust and individual countries.

*Criterion 40.19* - LEAs are able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangements to enable such joint investigations. All Federal LEAs (i.e. DEA, FBI, ICE-HSI, IRS-CI, and USSS) maintain offices outside the U.S. through which they coordinate with foreign counterparts, including on joint investigations.

*Exchange of information between non-counterparts*

*Criterion 40.20* - FinCEN is able to exchange information indirectly with non-counterparts and does so in practice: 31 USC §310 and 31 CFR §1010.950. The method of such an exchange is determined on a case-by-case basis. When exchanging information with non-counterparts, indirectly or directly

<sup>136</sup> FBAs – 12 USC §§326, 1817(a)(2)(C), 1818(v), 3109; 12 CFR §4.37(c); 12 USC §3109(a); SEC – s.24(c) *Exchange Act*, 15 USC §78x; Rule 24c-1 implementing Section 24(c) of the Exchange Act. CFTC – 7 USC § 12(e)

<sup>137</sup> FinCEN – 31 USC §310 and Treasury Order 180-01.

<sup>138</sup> FinCEN – 31 USC §310, 31 CFR. §1010.950; Treasury Order 180-01; FinCEN's System of Records (Treasury/FinCEN.001); MOUs with foreign counterparts. FBAs – MOUs with foreign counterparts; participation in supervisory colleges which afford members the opportunity to confer regularly on supervisory matters of significance to the group as a whole.

FinCEN takes steps to ensure that the non-counterpart(s) involved in the exchange submit(s) an appropriate request(s) and institutes proper controls to protect shared information.

*Weighting and Conclusion:*

All 20 criteria are met.

***Recommendation 40 is rated compliant.***

*Summary of Technical Compliance – Key Deficiencies*

Compliance with FATF Recommendations		
Recommendation	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	PC	<ul style="list-style-type: none"> <li>Lack of sufficient and effective mitigation measures against vulnerabilities of the high-end real estate agents, lawyers, accountants, trustees and CFAs due to non-coverage under comprehensive BSA AML/CFT regime.</li> <li>Exemptions and thresholds not supported by proven low risk.</li> <li>Scope issue: All investment advisers are not covered</li> </ul>
2. National cooperation and coordination	C	The Recommendation is fully met.
3. Money laundering offense	LC	<ul style="list-style-type: none"> <li>Mere possession is not criminalised and mere acquisition through the commission of the predicate offense is not considered ML.</li> <li>Tax crimes are not specifically predicates for ML.</li> <li>The list of predicate offenses for ML does not explicitly extend to all conduct that occurred in another country.</li> </ul>
4. Confiscation and provisional measures	LC	<ul style="list-style-type: none"> <li>The power to confiscated instrumentalities is not available for all predicate offenses.</li> <li>There is no general provision to freeze/seize non-tainted assets prior to a conviction to preserve them in order to satisfy a value-based confiscation order.</li> </ul>
5. Terrorist financing offense	C	The Recommendation is fully met.
6. Targeted financial sanctions related to terrorism & TF	LC	<ul style="list-style-type: none"> <li>TFS have not been applied to all persons designated by the UN pursuant to UNSCRs 1267/1988/1989</li> <li>Designations are not always implemented without delay.</li> </ul>
7. Targeted financial sanctions related to proliferation	LC	<ul style="list-style-type: none"> <li>TFS have been not been applied to all persons designated by the UN pursuant to UNSCRs 1718 and 1737.</li> </ul>
8. Non-profit organisations	LC	<ul style="list-style-type: none"> <li>The required 5 years retention period for records of domestic and international transaction and other information is not met in all circumstances.</li> <li>Not all houses of worship apply to IRS for preferential tax treatment and not all are subject to state requirements in terms of licensing/registration.</li> </ul>
9. Financial institution secrecy laws	C	The Recommendation is fully met.
10. Customer due diligence	PC	<ul style="list-style-type: none"> <li>Lack of CDD requirements to ascertain and verify the identity of BO (except in very limited cases).</li> <li>Scope issue: Not all investment advisers are covered.</li> <li>FIs (other than in the securities and derivatives sectors) are not explicitly required to identify and verify the identity of persons authorized to act on behalf of customers</li> <li>FIs are not explicitly required to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship, or understand the ownership and control structure of customers that are legal persons/arrangements.</li> <li>Beneficiaries of a life insurance policy are not specifically required to be included as a relevant risk factor in determining whether</li> </ul>

Compliance with FATF Recommendations		
Recommendation	Rating	Factor(s) underlying the rating
		enhanced CDD measures are applicable.
11. Record keeping	LC	<ul style="list-style-type: none"> <li>5 year record retention requirement restricted to account files, business correspondence and results of any analysis that are supporting documentation for a SAR.</li> <li>Existence of thresholds for triggering the record-keeping requirement.</li> </ul>
12. Politically exposed persons	PC	<ul style="list-style-type: none"> <li>Scope issue: MSBs, life insurance companies and all investment advisers are not covered.</li> <li>Domestic and international organizations PEPs are not specifically covered.</li> <li>The requirements of c.12.1 apply to family members and close associates of foreign PEPs but not those of domestic or international organizations.</li> <li>Concerns about the scope of BO identification in case of foreign PEPs.</li> </ul>
13. Correspondent banking	LC	<ul style="list-style-type: none"> <li>No specific requirement to obtain senior management approval before opening a new correspondent account.</li> <li>No explicit obligation to make a determination of a correspondent's reputation or quality of its AML controls and supervision.</li> </ul>
14. Money or value transfer services	LC	<ul style="list-style-type: none"> <li>No formal agent monitoring requirements for MSBs.</li> </ul>
15. New technologies	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisers are covered.</li> <li>No explicit requirements for FIs to address the risks presented by new technologies, though, the NMLRA does address risk related to new technology, and measures in place in the FFIEC Manual relating to new products and services are frequently interpreted by FIs and supervisors to address the risk of new technologies, and some enforcement measures reflect this.</li> </ul>
16. Wire transfers	PC	<ul style="list-style-type: none"> <li>Requirements apply subject to a USD 3 000 threshold for both domestic and international wire transfers.</li> <li>No explicit requirements to include all the originator and beneficiary information in the transmittal order;</li> <li>No explicit requirements to verify originator and beneficiary information below the threshold in case of suspicion of ML/TF</li> <li>No explicit requirements for MSBs to consider information from both the ordering and beneficiary sides for SAR determination</li> <li>No explicit obligations for intermediary or beneficiary FIs on executing, rejecting or suspending transactions due to lack of required information.</li> </ul>
17. Reliance on third parties	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisers are covered.</li> <li>No specific obligations on relying FIs to immediately obtain core CDD information from the relied upon FI.</li> </ul>
18. Internal controls and foreign branches and subsidiaries	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisers are covered.</li> </ul>
19. Higher-risk countries	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisors are covered.</li> <li>EDD measures do not apply automatically to business relationships and transactions with natural persons in general from jurisdictions</li> </ul>

Compliance with FATF Recommendations		
Recommendation	Rating	Factor(s) underlying the rating
		identified by FATF as having strategic AML/CFT deficiencies.
20. Reporting of suspicious transaction	PC	<ul style="list-style-type: none"> <li>• Scope issue: Not all investment advisers are covered.</li> <li>• Existence of thresholds for filing SARs.</li> <li>• Time allowed to file SARs (30 and 60 calendar days) does not meet the promptness criteria.</li> </ul>
21. Tipping-off and confidentiality	C	<ul style="list-style-type: none"> <li>• The Recommendation is fully met.</li> </ul>
22. DNFBPs: Customer due diligence	NC	<ul style="list-style-type: none"> <li>• Scope issues: <ul style="list-style-type: none"> <li>◦ Other than casinos, DNFBPs are only subject to limited CDD obligations (R.10) when filing Form 8300 reports.</li> <li>◦ Other than casinos, R.11 only applies to DNFBPs on a very limited basis in relation to their obligation to file CTRs, and does not apply to company formation agents at all.</li> <li>◦ No DNFBPs are subject to R.12. DNFBPs are not subject to R.15, although the AML program requirements for casinos, and dealers in precious metals and stones may go some way towards meeting these requirements.</li> </ul> </li> <li>• Where there is coverage, the deficiencies noted in relation to R10, R.11 and R.12 flow through to R.22.</li> </ul>
23. DNFBPs: Other measures	NC	<ul style="list-style-type: none"> <li>• Scope issues: <ul style="list-style-type: none"> <li>◦ No DNFBPs (other than casinos) are subject to R.20.</li> <li>◦ No DNFBPs (other than casinos and dealers in precious metals/stones) are subject to R.18.</li> <li>◦ No DNFBPs (other than casinos, dealers and precious metals and stones) are subject to R.19.</li> <li>◦ No DNFBPs (other than casinos) are subject to R.22</li> </ul> </li> <li>• Where there is coverage, the deficiencies noted in relation to R18, R.19, R.20 and R.22 flow through to R.23.</li> </ul>
24. Transparency and beneficial ownership of legal persons	NC	<ul style="list-style-type: none"> <li>• Generally unsatisfactory measures for ensuring that there is adequate, accurate and updated information on BO as defined by the FATF, that can be obtained or accessed by competent authorities in a timely manner.</li> <li>• No mechanism to ensure accuracy of basic information being obtained by State registries and keep the information up-to-date.</li> <li>• Absence of licensing or disclosure requirements for nominee shareholders/ directors.</li> <li>• No requirement for companies to maintain register of shareholders within the country</li> </ul>
25. Transparency and beneficial ownership of legal arrangements	PC	<ul style="list-style-type: none"> <li>• Although there are general fiduciary obligations imposed on trustees, these generally address trust law broadly; but do not appear to address obligations on trustees to obtain and hold adequate, accurate and current information on the identity of regulated agents of the trust, service providers, a protector, if any, all beneficiaries, or the identity of any natural person exercising ultimate effective control over the trust.</li> <li>• The obligations to keep information accurate and up-to-date only apply to trust companies.</li> <li>• Trust instruments that could block the ability of trustees to provide information about the trust to FIs and DNFBPs upon request are not prohibited.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
		<ul style="list-style-type: none"> <li>LEAs can obtain relevant information provided they know whether a person is a trustee, but there is no enforceable obligation on trustees to declare their status to FIs.</li> <li>Due to the foregoing issues, it cannot be said that information will be provided to foreign authorities rapidly.</li> <li>There are requirements in banking, trust, and tax law that, taken together, meet the 5 year records retention standard but these only apply to trust companies for the most part.</li> <li>The UTC requires trustees to identify property subject to a trust, but that obligation can be overridden by the terms of the trust.</li> <li>Information may not be obtained in a timely manner or at all in some cases.</li> </ul>
26. Regulation and supervision of financial institutions	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisers are covered.</li> <li>At the time of on-site, three States did not license MSBs, resulting in no background checks.</li> </ul>
27. Powers of supervisors	C	The Recommendation is fully met.
28. Regulation and supervision of DNFBPs	NC	<ul style="list-style-type: none"> <li>Scope issue: Other than for casinos, dealers in precious metals and stones, and in relation to examination for Form 8300 compliance, there are no competent authorities designated to supervise DNFBPs' compliance with AML/CFT obligations.</li> </ul>
29. Financial intelligence units	C	The Recommendation is fully met.
30. Responsibilities of law enforcement and investigative authorities	C	The Recommendation is fully met.
31. Powers of law enforcement and investigative authorities	LC	<ul style="list-style-type: none"> <li>While there are mechanisms in place to identify account holders and their assets, there is no general mechanism to do so. S.314(a) is powerful tool but available in limited circumstances.</li> </ul>
32. Cash couriers	C	The Recommendation is fully met.
33. Statistics	LC	<ul style="list-style-type: none"> <li>The U.S. does not maintain comprehensive statistics on the investigations, prosecutions and convictions related to the State ML offenses, or statistics on the property frozen, seized and confiscated at the State level.</li> </ul>
34. Guidance and feedback	LC	<ul style="list-style-type: none"> <li>Sectors not subject to the comprehensive AML/CFT requirements are only covered to some extent because of the limited application of the Form 8300 reporting guidance related to cash transactions.</li> <li>There is a case to align guidance more to vulnerabilities in minimally covered DNFBP sectors.</li> </ul>
35. Sanctions	LC	<ul style="list-style-type: none"> <li>Scope issue: Not all investment advisers are covered, and DNFBPs (other than casinos and dealers in precious metals/stones) are only partly covered.</li> </ul>
36. International instruments	LC	<ul style="list-style-type: none"> <li>The U.S has minor deficiencies in its implementation of the Vienna and Palermo conventions (see R.3).</li> </ul>
37. Mutual legal assistance	LC	<ul style="list-style-type: none"> <li>Where dual criminality applies, the minor shortcomings noted in R.3 may be a barrier to granting MLA request.</li> </ul>



Compliance with FATF Recommendations		
Recommendation	Rating	Factor(s) underlying the rating
		<ul style="list-style-type: none"> <li>The interception of communications can only be undertaken as part of a U.S. investigation.</li> <li>The OIA case management does not currently allow the monitoring of the time taken to incoming and outgoing requests.</li> </ul>
38. Mutual legal assistance: freezing and confiscation	LC	<ul style="list-style-type: none"> <li>In the context of dual criminality requirements, the gaps identified under R.3 may be a barrier to providing freezing and confiscation assistance, particularly when the predicate offense is not covered in the U.S.</li> </ul>
39. Extradition	LC	<ul style="list-style-type: none"> <li>The U.S. does not have multiple bilateral extradition treaties explicitly listing ML/TF as extraditable offenses.</li> </ul>
40. Other forms of international cooperation	C	The Recommendation is fully met.

## GLOSSARY OF ACRONYMS<sup>139</sup>

Technical compliance

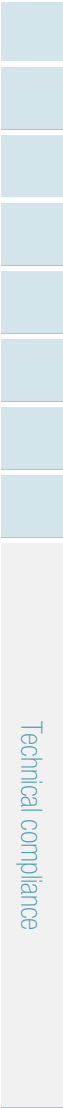
ABA	– American Bar Association
AFMLS	– Asset Forfeiture and Money Laundering Section
AG	– Attorney General
AGOCC	– Attorney General’s Organized Crime Council
APA	– Administrative Procedure Act
ATF	– The Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	– Assistant United States Attorney
BCSC	– Bulk Cash Smuggling Center
BGFRS	– Board of Governors of the Federal Reserve System
BIFS	– Border Intelligence Fusion Section
BIS	– Bureau of Industry and Security
BNI	– Bearer-Negotiable Instrument
BSA	– Bank Secrecy Act
BSAAG	– Bank Secrecy Act Advisory Group
CARIN	– Camden Inter-agency Asset Recovery Network
C&D	– Cease and Desist
CBP	– Customs and Border Protection
CEA	– Commodity Exchange Act
CFR	– Code of Federal Regulations
CFTC	– Commodity Futures Trading Commission
CIP	– Customer Identification Program
CME	– Chicago Mercantile Exchange
CMIR	– Report of International Transportation of Currency or Monetary Instruments
CMP	– Civil Monetary Penalty
CNTOC	– Counter-Narco-terrorism Operations Center
CPC	– Counterproliferation Center
CPI	– Counterproliferation Investigations
CPO	– Commodity Pool Operator
CPOT	– Consolidated Priority Organization Target
CSG	– Counterterrorism Security Group
CTA	– Commodity Trading Advisor
CTR	– Currency Transaction Report
D.C.	– District of Columbia
DEA	– Drug Enforcement Administration
DHS	– Department of Homeland Security
DHHS	– Department of Health and Human Services
DOJ	– Department of Justice

<sup>139</sup> Acronyms already defined in the FATF 40 Recommendations are not included in this Glossary

DOJ-AFF	– DOJ’s Asset Forfeiture Fund
DOJ-OIA	– Department of Justice Office of International Affairs
DTO	– Drug Trafficking Organizations
E2C2	– Export Enforcement Cooperation Center (E2C2)
EDD	– Enhanced Due Diligence
EDTF	– El Dorado Task Force
EIN	– Employer Identification Number
E.O.	– Executive Order
FBA	– Federal banking agency
FBAR	– Report of Foreign Bank and Financial Accounts
FBI	– Federal Bureau of Investigation
FBI-ITOS	– FBI Counterterrorism Division’s International Terrorism Operations Section
FBI-TFOS	– FBI Terrorist Financing Operations Section (FBI-TFOS)
FCM	– Futures Commission Merchant
FDA	– Food and Drug Administration
FDIC	– Federal Deposit Insurance Corporation
FFA	– Foreign Financial Agency
FFIEC	– Federal Financial Institutions Examination Council
FFR	– Federal Functional Regulator
FinCEN	– Financial Crimes Enforcement Network
FINRA	– Financial Industry Regulatory Authority
FISA	– Foreign Intelligence Surveillance Act
FR	– Federal Register
FTO	– Foreign Terrorist Organization
FTF	– Foreign Terrorist Fighter
GTO	– Geographic Targeting Order
HCFAC	– Health Care Fraud and Abuse Control Program
HEAT	– Health Care Fraud Prevention and Enforcement Action Team
HGSE	– Housing Government-Sponsored Enterprise
HIDTA	– High Intensity Drug Trafficking Areas
HIFCA	– High Intensity Money Laundering and Related Financial Crime Area
IB	– Introducing Broker
ICE	– Immigration and Customs Enforcement
ICE-HSI	– Immigration and Customs Enforcement - Homeland Security Investigations
IEEPA	– International Emergency Economic Powers Act
IFR	– Interim Final Rule
IGRA	– Indian Gaming Regulatory Act
INTERPOL	– International Criminal Police Organization
IOSCO	– International Organization of Securities Commissions
IOC-2	– International Organized Crime Intelligence and Operations Center
IPC	– Interagency Policy Committee
IRC	– Inland Revenue Code
IRS	– Internal Revenue Service
IRS-CI	– Internal Revenue Service – Criminal Investigation
IRS-SBSE	– IRS Small Business and Self-Employment Division
IRS-TEGE	– IRS’s Tax Exempt/Government Entities Division
JTTF	– Joint Terrorism Task Force
LLC	– Limited Liability Company
LP	– Limited Partnership
LLP	– Limited Liability Partnership

LLLP	– Limited Liability Limited Partnership
MMET	– Multi-State MSB Examination Taskforce
MRA	– Matters Requiring Attention
MRBA	– Matters Requiring Board Attention
MRIA	– Matters Requiring Immediate Attention
MSB	– Money Services Business
MTRA	– Money Transmitter Regulators Association
NACHA	– National Automated Clearinghouse Association
NCBF	– Non-Conviction Based Forfeiture
NCPC	– National Counterproliferation Center
NFA	– National Futures Association
NCTC	– National Counter Terrorism Center
NCUA	– National Credit Union Administration
NIGC	– National Indian Gaming Commission
NMLS	– Nationwide Multi-State Licensing System
NPRM	– Notice of Proposed Rulemaking
NSC	– National Security Council
OCC	– Office of the Comptroller of the Currency
OCDETF	– Organized Crime Drug Enforcement Task Forces
ODNI	– Office of the Director of National Intelligence
OECD	– Organization for Economic Co-operation and Development
OEE	– Office of Export Enforcement
OFAC	– Office of Foreign Assets Control
OFC	– OCDETF Fusion Center
OIA	– Office of Intelligence and Analysis
OMB	– Office of Management and Budget
ONDCP	– Office of National Drug Control Policy
RFPA	– Right to Financial Privacy Act
RICO	– Racketeer Influenced and Corrupt Organizations Act
RMLO	– Residential Mortgage Lenders and Originator
RPOT	– Regional Priority Target List
SAR	– Suspicious Activity Report
SDN	– Specially Designated Nationals
SDT	– Specially designated terrorists
SEC	– Securities and Exchange Commission
SOD	– Special Operation Division
SRB	– Self-Regulating Bodies
SUA	– Specified Unlawful Activity
TCO	– Transnational Criminal Organization
TOC	– Transnational Organized Crime
TEOAF	– Treasury Executive Office for Asset Forfeiture
TFF	– Treasury Forfeiture Fund
TFFC	– Office of Terrorist Financing and Financial Crimes
TFI	– Office of Terrorism and Financial Intelligence
TIN	– Tax Identification Number
U.S.	– United States
UN	– United Nations
USAO	– United States Attorneys' Offices
USC	– United States Code
USCG	– United States Coast Guards

USMS	– United States Marshalls Service
USSS	– United States Secret Service
USPIS	– United States Postal Inspection Service
USPS	– United States Postal Service
WMD PF	– Weapons of Mass Destruction Proliferation Finance





© FATF and APG

[www.fatf-gafi.org](http://www.fatf-gafi.org) | [www.apgml.org](http://www.apgml.org)

December 2016

## **Anti-money laundering and counter-terrorist financing measures - United States *Fourth Round Mutual Evaluation Report***

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in the United States as at the time of the on-site visit on 18 January - 6 February 2016. The report analyses the level of effectiveness of the United States' AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.