THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

International Anti-Money Laundering

HARRY DIXON, NICOLE S. HEALY, KAREN VAN ESSEN, ALEXANDER S. BIRKHOLD, FRANCESCA LULGJURAJ, PAIGE MASON, JUNG PAK, AND CHRISTINA ROBERTSON

This article reviews significant legal developments during 2017 in international anti-money laundering in the areas of money services businesses, art, banking, gaming, personal liability, and broker dealers.

I. Introduction

Money laundering and terrorist financing continue to present challenges for regulators worldwide. The Basel AML Index 2017 Report (the index), which ranks countries according to their risk of money laundering and terrorist financing, identified only one low-risk country in the world—Finland.[1] One hundred countries fell into the medium-risk category; fifty-two countries were identified as high risk.[2] The United States ranked just within the thirty lowest-risk countries for its strong anti-money laundering (AML) and counter-terrorist financing (CFT) frameworks.[3]

The index demonstrates that no country is immune from AML/CFT risk because criminals continue to seek out new ways to launder ill-gotten gains.[4] It should also come as no surprise that those countries with strong public and financial transparency and low levels of corruption have lower risk scores.[5] But many lower-risk countries that have a strong presence in the global financial markets, like the United States and the United Kingdom (UK), continue to be a significant source of transactions involving laundered funds, despite having relatively strong AML/CFT regulatory programs.

The Administration changes in the U.S. did not significantly slow the pace of regulatory enforcement actions, especially those concerning AML laws. In fact, U.S. regulatory agencies renewed their commitment to AML and CFT oversight in 2017. In October 2016, the Financial Crimes Enforcement Network (FinCEN) issued guidance addressing cybercrime that expanded suspicious activity reporting requirements to now include

1. BASEL INST. ON GOVERNANCE, BASEL AML INDEX 2017 REPORT 1 (2017), *available at* https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf.

2. *Id.* at 17.

3. *Id.* at 3.

4. *Id.* at 4.

5. *Id.* at 3.

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

cyber-events.[6] Accordingly, financial institutions are directed to report known or suspected transactions by, at, or through the institution that involve or aggregate to $5,000 or more in funds or other assets. In addition, the guidance encourages the voluntary reporting of cyber-events that may not otherwise require a Suspicious Activity Report (SAR). Examples of cyber-events provided by FinCEN include malware attacks, Distributed Denial of Service (DDoS) attacks, and unauthorized access to an institution's network.[7]

Financial institutions are encouraged to incorporate cyber-related information in their Bank Secrecy Act (BSA) /AML monitoring efforts, coordinate communication between AML and cyber security units within an organization, and share cyber-related information between financial institutions. FinCEN asserts that the sharing of malware signatures, IP addresses, and virtual currency addresses can help identify the cybercriminals linked to money laundering and terrorist financing. To this end, "Section 314(b) of the USA PATRIOT Act extends a safe harbor from liability to financial institutions that voluntarily share information with one another for the purpose of identifying and [ ] reporting potential money laundering or terrorist activities."[8]

Much like FinCEN, the Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) also intensified AML oversight this year. Although AML compliance has been an SEC examination priority for years, there was a significant increase in AML related enforcement actions in 2017, particularly against broker-dealers.[9] FINRA's increased AML enforcement this year not only included brokers-dealers but also targeted AML officers as well.[10] Several U.S. enforcement actions this year support the emerging trend to hold compliance professionals personally liable for BSA/AML deficiencies and violations.

In the European Union, the two-year implementation period for member states to achieve full compliance with the Fourth Anti-Money Laundering Directive (AMLD4) concluded on June 25, 2017. AMLD4's emphasis on enhanced customer due diligence, ultimate beneficial ownership, and

6. FINANCIAL CRIMES ENFORCEMENT NETWORK, FIN-2016-A005, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* 1 (2016), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.

7. *Id* at 5-6.

8. *Id.* at 8; *See Financial Crimes Enforcement Network*, *Section 314(b) Fact Sheet*, (2016), *available at* https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

9. *See* David Axelrod, Peter Hardy, Priya Roy and Brad Gershel, *The SEC's New Enforcement Tool?*, LAW 360, (July 12, 2017, 12:22 PM), https://www.law360.com/articles/943332; *See also* OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, *Securities and Exchange Commission*, *Examination Priorities for 2017* (2017), *available at* https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf.

10. *See* Robert Axelrod, *Personal Liability Exposure for AML Compliance Officers: Lessons From Haider*, BLOOMBERG BNA, (Sept. 8, 2017), https://www.bna.com/personal-liability-exposure-n57982087704/.

evidenced-based risk methodology strengthened the existing rules in the fight against money laundering.[11]

Although banking cases account for a majority of the significant enforcement actions in 2017, regulators worldwide continue to scrutinize the rapidly evolving landscape of digital currency and efforts of money services businesses and broker-dealers to comply with AML/CFT regulations.

II. Money Services Businesses

A. BTC-E

On July 26, 2017, FinCEN announced a $110 million fine against BTC-e, a digital currency exchange, for willfully violating U.S. AML laws, and another $12 million civil monetary penalty against its owner and operator, Alexander Vinnik, a Russian national. This is FinCEN's second enforcement action against a virtual currency exchange.[12] BTC-e a/k/a Canton Business Corporation is an Internet-based foreign entity operating as a money serviced business (MSB). FinCEN's jurisdiction extends to foreign MSBs that conduct business as an MSB "wholly or in substantial part within the U.S."[13] Customers located within the United States used BTC-e to conduct tens of thousands of virtual currency transactions. Further, BTC-e transactions were processed through servers located in the U.S.[14]

Among other significant failures, BTC-e did not have an AML program and had never filed a single SAR. BTC-e's Know Your Customer (KYC) program was inadequate; customers created accounts with minimal information and customer verification policies were optional. BTC-e lacked adequate internal controls to mitigate the inherent risks of virtual currencies. In fact, BTC-e serviced currencies that anonymized user data or obfuscated transactions and users openly discussed conducting criminal activity in BTC-e user chat rooms.[15]

FinCEN determined that BTC-e and Vinnik willfully violated money service business requirements by failing to register as a MSB within 180 days of beginning operations or to appoint a U.S.-based agent to accept legal process, a requirement for MSBs located abroad. Although this was the first

11. Council Directive 2015/849, 2015 O.J. (L 141) 73.

12. In 2015, FinCEN, in its first enforcement action against a virtual currency company, fined Ripple Labs Inc., for willful violation of ant-money laundering laws. *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger*, FINCEN, (May 5, 2015), https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual.

13. *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585-01 (July 21, 2011).

14. *In the Matter of: BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, Number 2017-03, p. 3 (July 26, 2017), *available at* https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-27/Assessment%20for%20BTCeVinnik%20FINAL2.pdf.

15. *Id.*

time FinCEN initiated an enforcement action against a foreign-based money service business, it delivered a concrete message that the regulator would hold money transmitters accountable for willfully violating U.S. AML laws, even if they are located abroad.[16]

B. Western Union

On January 19, 2017, the U.S. Department of Justice (DOJ) announced a settlement with The Western Union Company (Western Union) whereby Western Union, the DOJ, and several United States Attorney's Offices agreed to a deferred prosecution agreement (the DPA) relating to the federal government's charges of (i) a deficient anti-money laundering program and (ii) aiding and abetting wire fraud.[17] As part of a global settlement, Western Union also agreed to a stipulated order for permanent injunction and final judgment (the Order) entered by the Federal Trade Commission (FTC), the federal agency focused on protecting consumers from anticompetitive, deceptive, and unfair business practices, concerning charges asserted against Western Union relating to consumer fraud.[18]

According to the DPA, Western Union "(1) willfully fail[ed] to implement an effective anti-money laundering program, in violation of Title 31, United States Code, Sections 5318(h) and 5322 and regulations issued thereunder; and (2) aid[ed] and abet[ted] wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2."[19] The conduct at issue chiefly related to Western Union's agent locations and how Western Union failed to address agents and locations that violated the Bank Secrecy Act.[20] The DPA's Statement of Facts states that Western Union employees "repeatedly identif[ied] Western Union Agent locations involved in or facilitating fraud-related transactions but knowingly fail[ed] to take effective corrective action."[21] The schemes described in the Statement of Facts spanned numerous countries, including but not limited to Spain, the United Kingdom, China, and Mexico.[22]

Western Union is a MSB subject to specific registration and compliance regulatory requirements issued by FinCEN.[23] Western Union uses an electronic money transfer system that enables consumers to send money to

16. *See id.*

17. *See United States v. The Western Union Co.*, no. 1:17-00011 (M.D. Pa. Jan. 19, 2017) (Deferred Prosecution Agreement). *located at URL https://ecf.pamd.uscourts.gov/doc1/15505767889.

18. *See Federal Trade Commission v. The Western Union Co.*, No. 1:17-cv-00110 (M.D. Pa. Jan. 20, 2017) (Stipulated Order for Permanent Injunction and Final Judgment). *located at URL https://ecf.pamd.uscourts.gov/cgi-bin/DktRpt.pl?104534454713954-L_1_0-1.

19. *Supra* note.17.

20. *Id.*

21. *Id.* at Attachment A- Statement of Facts.

22. *Id.*

23. *See, e.g.*, 31 C.F.R. § 1022.210 (2011).

individuals worldwide.[24] In fact, almost 90% of Western Union agent locations are outside the United States.[25] Western Union incorporates several types of agents, but most are independent individuals or entities that have a contractual relationship with Western Union.[26] Unfortunately, MSBs are often a target for financial crime. For instance, a Western Union customer might only generate a single transaction, as compared with a traditional financial institution's customers for whom a bank can engage in ongoing Know Your Customer due diligence. In fact, as recently as March of 2016, FinCEN issued guidance on how a MSB should monitor its agents to prevent the use of the MSB as a facilitator of money laundering and terrorist finance.[27]

With respect to the aiding and abetting charge, Western Union agreed to forfeit $586 million on the basis that those funds are consumer fraud proceeds traceable to violations of Title 18.[28] The DPA gives credit to Western Union for numerous compliance program enhancements made since 2012.[29] The DPA also sets forth elements that comprise a reasonably designed anti-money laundering and anti-fraud program at Western Union.[30] For example, Western Union agreed to design and implement a risk-based Know Your Agent program, as well as to design and maintain procedures for corrective actions against agents and assign AML compliance officers for each country designated by Western Union as high risk for fraud or money laundering.[31]

It is significant for purposes of AML enforcement that the FTC, rather than the DOJ, required the appointment of an independent compliance auditor for Western Union. The Order sets forth various categories of compliance requirements for Western Union, including prohibiting business activities such as "[t]ransmitting a money transfer that [Western Union] knows or reasonably should know is a fraud-induced money transfer;" requiring due diligence on potential and current Western Union agents, thereby prohibiting Western Union from "[f]ailing to ensure that all new Western Union agents have effective policies and procedures in place at each of the agent's locations to detect and prevent fraud-induced money transfers"; and requiring monitoring compliance of Western Union agents, thereby prohibiting Western Union from "[f]ailing to provide appropriate and adequate ongoing education and training on consumer fraud for all

24. *See supra* note 17.

25. *Id.* at 3.

26. *See id.*

27. *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, FIN-2016-G001, *Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring* 1 (2016), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.

28. *See supra* note 17.

29. *Id.*

30. *Id.*

31. *Id.*

Western Union agents."[32] Failure to comply with the terms of the Order could expose Western Union to prosecution.

Following the FTC settlement with MoneyGram International, Inc., another MSB subject to the DOJ and FTC charges,[33] it appears that the FTC will continue to take an active part in cases involving AML violations.[34] Independent compliance auditors appointed pursuant to charges brought under consumer protection laws will review, analyze, and report on the efficacy of a defendant's anti-fraud program, with a particular focus on fraud-induced money transfers.[35] In cases like that of Western Union or MoneyGram, such a program could overlap or even exceed a defendant's AML requirements under the BSA.

Further, although an AML program for an MSB is effective when it is "reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities,"[36] the Order requires extremely specific detail relating to the type of data Western Union must obtain and retain with respect to fraud-induced money transfers. This is in addition to the type of transactional data analysis that the company must conduct to determine whether the agent location has "displayed any unusual or suspicious money transfer activity that cannot reasonably be explained or justified" such as "[u]nusual demographic activity" and "[i]rregular concentrations of send and/or pay activity between the agent and one or more other Western Union agent locations."[37]

III. Art

A. Hobby Lobby

On July 5, 2017, Hobby Lobby, the privately-held company famous for securing a Supreme Court decision permitting it to deny health insurance coverage for contraception to female employees on the basis that providing such coverage violated the owners' personal religious beliefs, entered into a settlement with the U.S. Attorney's Office for the Eastern District of New York for violating federal law prohibiting the importation of falsely identified cultural property.[38] In addition to the fine, Hobby Lobby also agreed to forfeit thousands of ancient cuneiform tablets and clay bullae (clay

32. *Supra* note 18.

33. FTC v. MoneyGram International, Inc., No. 09-6576 (N.D. Ill., Stipulated Order for Permanent Injunction and Final Judgment, October 21, 2009).

34. The FTC alleged that MoneyGram's worldwide network was being used by telemarketing fraudsters to prey on U.S. customers and that MoneyGram ignored warnings from both law enforcement and its own employees about the fraud.

35. *Supra* note 18 at *4; *see*, *e.g.*, 15 U.S.C. § 53(b) & § 6101-08).

36. *See* 31 C.F.R. § 1022.210 (2011).

37. *Supra* note 18.

38. Alan Feuer, *Hobby Lobby Agrees to Forfeit 5,500 Artifacts Smuggled Out of Iraq*, N. Y. Times (July 5, 2017), https://www.nytimes.com/2017/07/05/nyregion/hobby-lobby-artifacts-smuggle-iraq.html.

balls with imprinted seals) originating in the region that is now Iraq.[39] The artifacts were shipped from Israel and the United Arab Emirates (UAE) in boxes falsely labeled as "ceramic tiles" or "tile samples."[40] The case had been pending resolution for some time; Hobby Lobby's owners purchased the artifacts beginning in December 2010, for a total of $1.6 million.[41]

According to the press release and civil *in rem* forfeiture complaint, the violations were not inadvertent. As the press release noted, the "acquisition of the Artifacts was fraught with red flags."[42] Before the acquisition, in July 2010, the company's president and a consultant travelled to the United Arab Emirates to view the artifacts. Although at least two Israeli dealers and a UAE dealer attended the inspection, the Israeli dealers later told Hobby Lobby personnel that the items belonged to the family of a third Israeli dealer. Later, the company was provided with a provenance certificate claiming the artifacts had been in the United States in the 1970s, in the custody of yet another individual, but the company took no steps to verify that information, which was apparently inaccurate because the alleged custodian had not met the third Israeli dealer until 2007, and never stored any items for him.[43]

Significantly, an expert retained by Hobby Lobby wrote a memorandum to Hobby Lobby's in-house counsel that was not shared with others in the company involved in the transactions. The memorandum warned the company against purchasing artifacts from Iraq, and that the company should ensure that all shipping documents were accurate, that there was a high risk that the items would be detained by U.S. Customs and Border Patrol (Customs), and that the failure to accurately identify the country of origin could lead to seizure of the items. The expert further warned that the objects may have been looted from Iraq and that, if so, their acquisition would have violated U.S. law.[44] Despite these warnings, Hobby Lobby made the purchases through multiple intermediaries.

Hobby Lobby appears to have gone out of its way *not* to perform due diligence, *not* to comply with its own acquisition and compliance protocols, and to conduct the transactions in the most suspicious manner possible. Hobby Lobby did not investigate records supplied by two of the three Israeli dealers concerning the provenance of the artifacts. Additionally, at the request of one dealer, it wired payments to seven personal accounts belonging to five people, none of whom was the purported seller listed on

39. *Id.*

40. Press Release, U.S. Attorney's Office E. D. N. Y., *United States Files Civil Action to Forfeit Thousands of Ancient Iraqi Artifacts Imported by Hobby Lobby* (July 5, 2017) *available at* https://www.justice.gov/usao-edny/pr/united-states-files-civil-action-forfeit-thousands-ancient-iraqi-artifacts-imported.

41. *Id.*

42. *Id.*

43. Complaint *in Rem*, *United States v. Approximately Four Hundred Fifty Ancient Cuneiform Tablets and Approximately Three Thousand Ancient Clay Bullae*, CV 17-3980 (E. D. N. Y. June 5, 2017).

44. *Id.*

the invoice and bypassed its internal international department, which routinely conducted foreign transactions and which had noted that the items might be held by U.S. Customs. Further, Hobby Lobby caused the artifacts to be falsely labeled as to their country of origin, value, and description; directed the shipper to falsely claim on the customs declaration forms that the items were valued below the $2,000 reporting threshold; and at the direction of the UAE-based dealer, addressed the shipments to Hobby Lobby and two affiliates, to make it appear as though these were legitimate transactions.[45]

After U.S. Customs seized five shipments and began administrative forfeiture proceedings, Hobby Lobby's counsel requested the initiation of judicial forfeiture. Following extensive negotiations, the parties settled the case. In addition to agreeing to forfeit the artifacts identified in the complaint, and pay a fine of $3 million, Hobby Lobby "agreed to adopt internal policies and procedures governing its importation and purchase of cultural property, provide appropriate training to its personnel, hire qualified outside customs counsel and customs brokers, and submit quarterly reports to the government on any cultural property acquisitions for the next eighteen months."[46]

IV. Banking Cases

A. Deutsche Bank

In January 2017, the New York Department of Financial Services (NYDFS) entered into a consent order with Deutsche Bank AG and its New York branch for violations of New York AML laws in connection with a "mirror trading" scheme among the bank's branches in New York, London, and Russia that resulted in the movement of approximately $10 billion out of Russia. The NYDFS concluded that the bank's compliance failures resulted in missed opportunities to detect, investigate, and halt the scheme over several years. Deutsche Bank agreed to pay a $425 million fine and hire an independent monitor pursuant to the consent order.[47]

The Federal Reserve Board also announced a $41 million penalty and consent cease and desist order against the U.S. operations of Deutsche Bank AG in January 2017 for AML deficiencies. In addition to identifying failures by Deutsche Bank's U.S.-based banking operations to maintain an effective program to comply with the Bank Secrecy Act and AML requirements, the consent order required Deutsche Bank to improve senior management oversight and controls and compliance with AML laws.[48]

45. *Id.*

46. *Supra* note 40.

47. N.Y. State Dept.of Fin. Servs., *Consent Order Under N.Y. Banking Law §§ 39, 44, 44-a* (2017), *available at* http://www.dfs.ny.gov/about/ea/ea170130.pdf.

48. Press Release, Board of Governors of the Federal Reserve System, *Federal Reserve Announces Two Enforcement Actions Against Deutsche Bank AG That Will Require Bank to Pay a*

In January 2017, the U.K.'s Financial Conduct Authority (FCA) also fined Deutsche Bank £163,076,224 for failing to maintain proper AML controls. This is the largest penalty ever imposed by the FCA for failings concerning AML controls. The FCA's Director of Enforcement and Market Oversight, Mark Steward, explained "[t]he size of the fine reflects the seriousness of Deutsche Bank's failings" and warned "[o]ther firms should take notice of today's fine and look again at their own AML procedures to ensure they do not face similar action."[49]

B. MERCHANTS BANK OF CALIFORNIA

FinCEN assessed a $7 million civil money penalty against Merchants Bank of California in February 2017 for willfully violating the Bank Secrecy Act.[50] In addition to failing to establish and maintain an AML program, Merchants Bank did not conduct proper due diligence on its foreign correspondent accounts or report suspicious activity. Of note, FinCEN found that Merchants failed to provide the necessary level of authority, independence, and responsibility to its BSA officers and compliance staff. Bank insiders interfered with compliance staff's efforts to investigate suspicious activity related to insider-owned accounts; many of the transactions were conducted on behalf of insider-owned MSBs. In the press release, FinCEN asserts that these failures resulted in billions of dollars in transactions that were not effectively monitored. The Office of the Comptroller of the Currency (OCC) also identified deficiencies in the Bank's practices as well as violations of previous consent orders and assessed its own $1 million civil money penalty against Merchants Bank.[51]

C. BANAMEX USA

In May 2017, Banamex USA, a Los Angeles-based subsidiary of Citigroup, Inc., agreed to forfeit nearly $100 million and enter into a non-prosecution agreement to conclude a Department of Justice investigation into Banamex's

---

Combined $156.6 Million in Civil Money Penalties (April 20, 2017), *available at* https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170420a.htm.

49. Press Release, Financial Conduct Authority, *FCA Fines Deutsche Bank £163 million for Serious Anti-Money Laundering Controls Failings* (Jan. 31, 2017) (on file with author), *available at* https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure. *See* Letter of Final Notice from Financial Conduct Authority to Deutsche Bank AG (Jan. 30, 2017) (on file with the Financial Conduct Authority), *available at* https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf.

50. Press Release, Financial Crimes Enforcement Network, *FinCEN Penalizes California Bank for Egregious Violations of Anti-Money Laundering Laws* (Feb. 27, 2017), *available at* https://www.fincen.gov/news/news-releases/fincen-penalizes-california-bank-egregious-violations-anti-money-laundering-laws.

51. Merchants Bank of California, N.A., No. 2017-02 (Financial Crimes Enforcement Network Feb. 16, 2017) (Assessment Civil Money Penalty), *available at* https://www.fincen.gov/sites/default/files/enforcement_action/2017-02-27/Merchants%20Bank%20of%20California%20Assessment%20of%20CMP%2002.24.2017.v2.pdf.

alleged Bank Secrecy Act violations. Beginning in 2007 and until 2012, Banamex processed over thirty million remittance transactions to Mexico worth more than $8.8 billion for which Banamex's monitoring system issued nearly 20,000 suspicious transaction alerts. But in response, Banamex conducted less than ten investigations and only filed nine SARs. Significantly, Banamex's limited and manual transaction monitoring system produced paper reports; only two employees were responsible for reviewing those reports in addition to their non-compliance obligations. Even as it expanded its remittance processing business, Banamex did not address control deficiencies or increase staffing. As part of the agreement, Banamex admitted it failed to maintain an effective AML program with adequate controls, polices, and procedures. Banamex also admitted it willfully failed to file SARs.[52]

D. Habib Bank

In September 2017, the NYDFS fined Habib Bank, the largest bank in Pakistan, $225 million for failure to comply with AML laws and regulations at the bank's New York branch. At the conclusion of its investigation, NYDFS determined the bank's serious failures in its AML compliance function resulted in billions of dollars in transactions for a Saudi private bank with reported links to al Qaeda. These transactions were facilitated by a lack of proper AML controls, a failure to adequately identify customers of the same private bank that might be using accounts at Habib bank to transfer funds through New York, and the improper use of a "good guy" list to enable transactions with an identified terrorist, potentially sanctioned persons, and an international arms dealer. Significantly, the investigation was undertaken pursuant to a December 2015 Consent Order that identified previous deficiencies in the Bank's BSA/AML compliance program. The NYDFS noted the Bank failed to rectify its deficiencies despite "more than sufficient opportunity" to correct the problems.[53]

E. Lone Star

FinCEN announced an assessment of a $2 million civil penalty against Texas-based Lone Star National Bank in November 2017 for willful violations of the Bank Secrecy Act. The Consent Order asserted that Lone Star failed to establish and implement an adequate AML program, properly conduct due diligence on a foreign correspondent account, and report suspicious activities. Section 312 of the USA Patriot Act requires that U.S. financial institution that establish, maintain, administer, or manage a

52. Letter from Deborah Connor, Acting Chief Money Laundering and Asset Recovery Section, Dept. of Justice, to Brad Carp and Susanna Buergel, *Banamex USA Criminal Investigation* (May18, 2017) (on file with the Dept. of Justice), *available at* https://www.justice.gov/opa/press-release/file/967871/download.

53. N.Y. State Dept.of Fin. Servs., *Consent Order Under N.Y. Banking Law §§ 39, 44 and 605* (2017), *available at* http://www.dfs.ny.gov/about/ea/ea170907.pdf.

correspondent account in the U.S. for a foreign financial institution take certain AML measures for those accounts. Lone Star's failure to comply with Section 312 resulted in a foreign correspondent bank moving hundreds of millions of U.S. dollars in suspicious cash shipments through the United States. Among other deficiencies, Lone Star did not consider public information about the foreign bank's alleged involvement in securities fraud or verify information provided by the bank regarding the source of funds and purpose of the account. FinCEN Acting Director Jamal El-Hindi stated in the press release that, "(s)maller banks, just like the bigger ones, need to fully understand and follow the 312 due diligence requirements if they open accounts for foreign banks." He continued by noting that those risks are manageable but should not be ignored.[54]

F. Credit Suisse and United Overseas Bank

The Monetary Authority of Singapore (MAS) imposed financial penalties on Credit Suisse and United Overseas Bank (UOB) in May 2017 after completing a two-year review of banks involved in dealings with 1Malaysia Development Berhad (1MDB), a government run strategic development firm.[55] The investigation uncovered several breaches of AML requirements and control inadequacies in violation of MAS Notice 626 – Prevention of Money Laundering and Countering the Financing of Terrorism. Specific issues included lapses in conducting customer due diligence and inadequate review of customer transactions. The MAS imposed fines of approximately S$0.7 million on Credit Suisse and S$0.9 million on UOB. The MAS noted, however, that the banks are currently taking steps to improve AML controls and address the weaknesses uncovered in the investigation.[56]

54. Press Release, Financial Crimes Enforcement Network, , *FinCEN Penalizes Texas Bank for Violations of Anti-Money Laundering Laws Focusing on Section 312 Due Diligence Violations* (Nov. 1, 2017) (on file with author), *available at* https://www.fincen.gov/news/news-releases/fincen-penalizes-texas-bank-violations-anti-money-laundering-laws-focusing; *See* Lone Star National Bank, Assessment of Civil Money Penalty, No. 2017-04 (Feb. 16, 2017) (Assessment Civil Money Penalty), *available at* https://www.fincen.gov/sites/default/files/enforcement_action/2017-11-01/Lone%20Star.ASSESSMENT%20OF%20CIVIL%20MONEY%20PENALTY%20-%20Final%2011.01_0.pdf.

55. In 2015, Malaysia's Prime Minister, Najib Tun Razak, was accused of channeling over nearly 700 million U.S. dollars from 1MDB, a government-run strategic development company, to his personal bank accounts. *See generally Malaysia Controversy*, Wall Street Journal (last visited Jan. 29, 2017, 6:42 PM), http://www.wsj.com/specialcoverage/malaysia-controversy.

56. Monetary Authority of Singapore, *Financial Penalties Imposed on Credit Suisse and UOB for 1-MDB Related Transactions* (May 30, 2017), *available at* http://www.mas.gov.sg/News-and-Publications/Enforcement-Actions/2017/Financial-Penalties-Imposed-on-Credit-Suisse-and-UOB-for-1MDB-Related-Transactions.aspx.

G. Allied Irish Banks Plc

In April 2017, the Central Bank of Ireland fined Allied Irish Banks Plc (AIB) approximately 2.3 million Euro for breaches of anti-money laundering and terrorist financing laws. According to AIB, the settlement with Central Bank concerned issues dating from July 2010 to July 2014. During that period, AIB failed to conduct proper due diligence on customers with accounts that predated the first Irish AML laws, passed in 1995, and did not report suspicious transactions without delay to the proper authorities. The Central Bank said it also discovered breaches in AIB's AML policies and procedures, including in its trade finance business.[57]

H. BNP Paribas

In June 2017, Autorité de Contrôle Prudentiel et de Résolution (ACPR), the French financial regulator, fined BNP Paribas _10 million following a 2015 inspection of the bank that revealed insufficient money laundering controls. Specifically, the ACPR noted the bank did not have enough staff responsible for detecting and reporting suspicious transactions. According to the ACPR, BNP Paribas also lacked adequate tools for detecting unusual customer transactions.[58]

I. Commonwealth Bank of Australia

In August 2017, the Australian Transactions Reports & Analysis Centre (AUSTRAC), Australia's financial intelligence agency responsible for AML and CFT, initiated civil proceedings against the Commonwealth Bank of Australia (CBA) for the bank's failure to comply with AML and terrorist financing laws on more than 53,700 occasions. AUSTRAC claims CBA did not comply with its internal AML program and did not assess the money laundering or terrorist financing risks of its intelligent deposit machines (IDMs) for three years. CBA also allegedly did not provide timely reports to AUSTRAC for 53,506 cash transactions conducted through IDMs that exceeded the cash-reporting requirement from November 2012 to

57. Press Release, Central Bank of Ireland, *Settlement Agreement between the Central Bank of Ireland and Allied Irish Bank, p.l.c.*, (2017) (on file with author), *available at* https://www.centralbank.ie/docs/default-source/news-and-media/legal-notices/settlement-agreements/public-statement-relating-to-settlement-agreement-between-central-bank-of-ireland-and-allied-irish-bank.pdf.

58. *See* Reuters staff, *BNP Paribas fined over weaknesses in anti-money laundering controls*, Reuters, (June 2, 2017, 12:16 PM), https://www.reuters.com/article/us-bnp-paribas-moneylaundering/bnp-paribas-fined-over-weaknesses-in-anti-money-laundering-controls-idUSKBN18T2JI; *see also* Silver Liisma, *BNP Paribas fined EUR 10 million by ACPR for AML failures*, O.R.X., (June 7, 2017), https://managingrisktogether.orx.org/sites/default/files/downloads/2017/07/orxnewsdigestofthemonthjune.pdf

September 2015. CBA allegedly did not timely report, or report at all, suspicious transactions that totaled more than $77 million.[59]

J. Coutts & Co AG

In April 2017, the Hong Kong Monetary Authority (HKMA) imposed a HK$7 million fine on the Hong Kong branch of Coutts & Co AG, for failing to follow anti-money laundering rules. The fine stems from the branch's conduct between 2012 and 2015. Following its investigation, the HKMA determined Coutts violated five provisions of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance. The breaches included, among other things, a failure to establish and maintain procedures for determining if customers were politically exposed persons (PEP). The HKMA also indicated there were no procedures for obtaining senior management approval to maintain relationships with customers identified as PEPs.[60]

The Swiss Financial Market Supervisory Authority also ordered Coutts to pay approximately $6.57 million in illegal profits from transactions in which Coutts breached AML regulations by failing to conduct proper background checks into business relationships associated with 1MDB.[61]

V. Gaming

A. Tabcorp

In March 2017, the Federal Court of Australia levied a record-setting civil penalty against Tabcorp, an international gambling entertainment company, for failing to have a compliant AML/CFT program. The $45 million civil penalty resulted from the Federal Court's determination that Tabcorp violated the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 on 108 occasions over a period of five years. The court also found Tabcorp failed to provide AUSTRAC with reports about suspicious matters on 105 different occasions and did not identify a customer who collected $100,000 in winnings. Paul Jevtovic, the AUSTRAC CEO, noted the "unprecedented civil penalty highlights AUSTRAC's resolve to take enforcement action against reporting entities that engage in significant, extensive and systemic non-compliance." Mr. Jevtovic urges all Boards and

59. Press Release, *AUSTRAC seeks civil penalty orders against CBA*, Australian Transaction Reports and Analysis Centre (August 3, 2017) (on file with author), *available at* http://austrac.gov.au/media/media-releases/austrac-seeks-civil-penalty-orders-against-cba.

60. Press Release, Hong Kong Monetary Authority, The Monetary *AUSTRAC seeks civil penalty orders against CBA*, AUSTRAC (Apr. 11, 2017) (on file with author), *available at* http://austrac.gov.au/media/media-releases/austrac-seeks-civil-penalty-orders-against-cba.

61. Press Release, Swiss Financial Market Supervisory Authority, *FINMA sanctions Coutts for 1MDB breaches*, FINMA (Feb. 2, 2017) (on file with author), *available at* https://www.finma.ch/en/news/2017/02/20170202-mm-coutts/.

senior management "to ensure that they are fully informed of their AML/CFT compliance."[62]

VI. Personal Liability

A. Thomas Haider: MoneyGram International Inc.'s ex-Chief Compliance Officer

In May 2017, Thomas Haider, MoneyGram International Inc.'s former Chief Compliance Officer, agreed to a three-year injunction barring him from acting in a compliance function for any money transmitter. As part of the settlement with FinCEN and the U.S. Attorney's Office for the Southern District of New York, Haider also agreed to pay a $250,000 penalty. In 2014, U.S. authorities sued Haider, seeking a $1 million civil penalty and to hold him personally liable for failing to stop fraudulent transfers and other violations of the Bank Secrecy Act. As part of the settlement, Haider admitted and accepted responsibility for numerous violations, including failing to implement a policy for terminating outlets that posed high fraud risks and structuring MoneyGram's AML program such that analysts responsible for filing SARs with FinCEN did not see information aggregated by MoneyGram's Fraud Department. The case has been considered as a test of the U.S. government's increasing focus on punishing individuals for institutional compliance shortfalls. "Holding [Haider] personally accountable strengthens the compliance profession by demonstrating that behavior like this is not tolerated within the ranks of compliance professionals," acting FinCEN Director Jamal El-Hindi said. FinCEN asserts that this is one of the largest fines ever imposed on an individual.[63]

B. John D. Telfer: Windsor Street Capital AML Compliance Officer

In early 2017, the SEC charged Windsor Street Capital and its anti-money laundering officer, John D. Telfer, with securities violations regarding the unregistered sale of hundreds of millions of penny stock shares without adequate due diligence. According to the SEC, Telfer failed to file

62. Press Release, Australian Transaction Reports and Analysis Centre, *Record $45 million civil penalty ordered against Tabcorp*, AUSTRAC (Mar. 16, 2017) (on file with author), *available at* http://www.austrac.gov.au/media/media-releases/record-45-million-civil-penalty-ordered-against-tabcorp.

63. Press Release, Financial Crimes Enforcement Network, *FinCEN and Manhattan U.S. Attorney Announce Settlement with Former MoneyGram Executive Thomas E. Haider*, FinCEN (May 4, 2017) (on file with author), *available at* https://www.fincen.gov/news/news-releases/fincen-and-manhattan-us-attorney-announce-settlement-former-moneygram-executive; *see* Reuters staff, *Former MoneyGram executive settles closely watched U.S. money laundering case*, Reuters, (May 4, 2017), https://www.reuters.com/article/us-moneygram-intl-moneylaundering/former-moneygram-executive-settles-closely-watched-u-s-money-laundering-case-idUSKBN1802P3.

SARs for nearly $25 million in suspicious penny stock sale transactions beginning in 2013, despite multiple red flags alerting him to the fraudulent scheme. Although Telfer neither admitted nor denied any wrongdoing, pursuant to the terms of his settlement in June 2017, he agreed to be barred from the securities industry and pay a $10,000 penalty.[64]

C. Ronald B. Nicklaus: Pennaluna & Company AML Officer

In February 2017, Ronald B. Nicklas, the former AML Officer of Pennaluna & Company (Pennaluna) and FINRA signed a Letter of Acceptance and Waiver and Consent (AWC) for failing to establish and implement an AML program "reasonably designed to detect and cause the reporting of suspicious activity." During his term as an AML Officer, Pennaluna accepted deposits and subsequently facilitated the sale of millions of shares of securities priced under $5 on eight customer accounts for proceeds totaling just over $1.5 million; three of the five accounts were owned by the same customer. But while Niklas served as the AML Officer, Pennluna failed to identify any red flags or to investigate suspicious transactions. Nicklas consented to a four-month suspension from association with all FINRA members in all principal capacities and a $10,000 fine.[65]

VI. Broker Dealers

A. Wells Fargo Advisors, LLC

On November 13, 2017, Wells Fargo Advisors, LLC entered into a settlement agreement with the Securities and Exchange Commission regarding suspicious activity reporting.[66] Between March 2012 and June 2013, Wells Fargo failed to file fifty SARs concerning activity occurring in U.S. branch offices that focused on international customers.[67] Notably, for a majority of the reports, Wells Fargo failed to file timely SARS on continuing activities that had already been reported by Wells Fargo Advisors. Although Wells Fargo Advisors did not admit or deny guilt, it agreed to a cease and desist order, censure, and to pay a $3.5 million penalty.[68]

B. Windsor Street Capital, L.P.

On July 28, 2017, the SEC issued an order for Windsor Street Capital L.P (Windsor), to pay $200,000 in fines for violating the Exchange Act Section 17(a) and Rule 17a-8. In addition, Windsor was directed to obtain an

64. File No. 3-17813, *SEC Settlement Bars Former Anti-Money Laundering Officer for Gatekeeper Failures*, SEC (June 12, 2017), https://www.sec.gov/litigation/admin/2017/34-80908-s.pdf.

65. *Disciplinary and Other FINRA Actions*, at 13, FINRA (Dec. 2017), *available at* https://www.finra.org/sites/default/files/publication_file/December_2017_Disciplinary_Actions.pdf.

66. *In the matter of Wells Fargo Advisors, LLC*, no. 3-18279, 2017 WL 5248280 (Nov. 13, 2017).

67. *Id.*

68. *Id.*

independent consultant to review and recommend mandatory enhancements to the firm's AML policies and procedures. The Order noted that even though Windsor's AML program identified red flags that triggered an investigation, Windsor failed to file SARs for $24.8 million of potentially illegal stock sales conducted by its customers that met the red flag criteria.[69]

C. Alpine Securities Corporation

On June 5, 2017, the SEC filed a complaint against Alpine Securities Corporation (Alpine) for alleged systematic failure to file SARs for stock transactions that were flagged as suspicious, in violation of the Exchange Act Section 17(a) and Rule 17a-8. The SEC's complaint stated that Alpine omitted from the SARs information supporting the determination to file. Additionally, even though Alpine was aware of a 2012 FINRA's finding that its SARs narratives were inadequate; Alpine did not take any meaningful corrective action.[70]

D. Mariva Capital Markets

In an AWC signed by Mariva Capital Markets (Mariva) on May 15, 2017, FINRA found that Mariva failed to establish and implement an AML program, "reasonably tailored" to Mariva's business, in violation of FINRA Rule 3310 (a). Between late 2013 and early 2015, Mariva facilitated trading of more than $1 billion in Argentinian debt on behalf of a foreign financial institution's affiliate. Although Mariva had an AML program that contemplated general red flags, the program was not designed to detect potentially suspicious activity in the affiliate's account. FINRA found that Mariva's AML program was inadequate and, as a result, Mariva failed to conduct enhanced due diligence on the affiliate's account sufficient to understand the purpose of the account, and anticipate the bond activity. FINRA and Mariva agreed to a censure and a $100,000 fine.[71]

E. Spartan Securities Group, Ltd.

Similarly, in July 2017, Spartan Securities Group Ltd (Spartan) agreed to pay $100,000 for failing to establish and implement an AML program reasonably designed to achieve compliance with BSA. FINRA pointed out that while Spartan conducted trade reviews, it did not have an AML

---

69. *See In the Matter of Windsor Street Capital L.P. (f/k/a Meyers Ass., L.P.) & Telfer*, Exchange Act No. 10392, 2017 WL 3214439 (July 28, 2017). (Order Making Findings And Imposing Remedial Sanctions And A Cease-And-Desist Order Pursuant To Section 8a Of The Securities Act Of 1933 And Sections 15(B) And 21c Of The Securities Exchange Act Of 1934 As To Windsor Street Capital, L.P.)

70. *See U.S. Securities and Exchange Comm. v. Alpine Securities Corp.*, no. Complaint and Jury Demand (S.D.N.Y. 2017) (ECF case).

71. *FINRA Letter of Acceptance, Waiver and Consent to Mariva Capital Markets, LLC*, No. 2015043415301, FINRA (May 9, 2017) *available at* http://www.finra.org/sites/default/files/fda_documents/2015043415301_FDA_SL678098.pdf.

program responsive to Spartan's particular business and capable of aggregating the information necessary to trigger AML red flags and detect patterns of suspicious activity. FINRA pointed to several instances where multiple red flags were present, but Spartan failed to investigate the transaction or file a SAR.[72]

F. Valdes & Moreno, Inc.

In April 2017, an AWC signed by Valdes & Moreno Inc. of Kansas City, Missouri imposed a $20,000 fine for failure to adequately review and investigate potentially suspicious activity. Specifically, V&M failed to adequately review and investigate potentially suspicious activity involving one customer who engaged in ten securities transactions involving the stocks of ten microcap issuers that demonstrated red flags characteristic of a pump and dump scheme. V&M also failed to conduct required due diligence on its single correspondent account for a foreign financial broker-dealer. Additional AML program deficiencies included no documented evidence of risk assessments, enhanced due diligence determinations, or the periodic review of correspondent accounts.[73]

G. Wood Company Inc.

In March 2017, FINRA issued a decision on a formal complaint against Wood Company Inc. (Wood), for failure to implement and enforce its AML procedures and conduct adequate independent AML tests, in violation of FINRA Rules 3310 and 2010. More specifically, Wood hired a broker with a history of disciplinary actions, Edwin Quinones, and then failed to subject him to heightened oversight, to detect and investigate red flags for penny stock trades he executed, and adequately respond to red flags raised by its clearing firm, Pershing. In March 2009, one year after Quinones was hired, Pershing began alerting Wood to trades in Quinones' accounts. Wood's AML Officer initially ignored the inquiry, but later forwarded the email to Quinones. In response, Quinones provided incomplete answers to Pershing. FINRA stated in its decision that the question is not whether the trading constituted a "pump and dump" scheme, but rather, whether the red flags were sufficient to necessitate further investigation. FINRA imposed a $73,000 fine on Wood and prohibited it from liquidating penny stocks in new accounts for a period of two years.[74]

---

72. *FINRA Order Accepting Offer of Settlement to Spartan Securities Group, Ltd.*, no. 2013036389101, FINRA (July 11, 2017), *available at* https://www.finra.org/sites/default/files/fda_documents/2013036389101_FDA_RB7X3580.pdf.

73. *FINRA Letter of Acceptance, Waiver, and Consent to Valdes & Moreno, Inc.*, No. 20160482443301, FINRA (Apr. 25, 2017).

74. *Wood (Arthur W.) Co. Inc.*, 2017 WL 3434112 (N.A.S.D.R.) (March 15, 2017). .

H. Weston Financial Services LLC

More recently in September 2017, Weston Financial Services LLC signed an AWC agreeing to a censure and fine of $20,000 for failing to produce information requested by FinCEN pursuant to BSA regulation 31 C.F.R. 1010.520 which incorporates section 314(a) of the USA PATRIOT ACT.[75] This regulation authorizes "[a] law enforcement agency investigating terrorist activity or money laundering to request that FinCEN solicit, on the investigating agency's behalf, certain information from a financial institution or a group of financial institutions"[76]

75. *FINRA Letter of Acceptance, Waiver and Consent Weston Financial Services LLC*, No. 2013035268401, FINRA (Sept. 27, 2017).

76. 31 C.F.R. § 1010.520 (2011).