Message from the Chair

As Chair of the White Collar Crime Committee, I am very pleased and excited to present to the Committee the winter 2015 issue of the White Collar Crime Committee Newsletter. Thank you to Newsletter editor, Joseph Martini and all of the authors for all of their hard work. I believe that you will find the Newsletter both interesting and informative. I encourage committee members to contribute articles for future editions of the newsletter. As members of the Committee you have a wide range of interests and expertise that I urge you to share with us. If interested, please contact Joe, Committee Vice-Chair Daniel Horwitz or me. If you want to write but are stumped for a topic, Joe, Dan and I are happy to suggest one.

Sincerely,

A.J. Bosco
Chair, White Collar Crime Committee

De-Risking Threatens Religious Access to Banking Services

By Sheila Tendy

For the past year, banks have been cutting ties with businesses that regulators view as "high risk" in order to protect themselves from regulatory scrutiny and potential fines and penalties. Now America's religious organizations appear to be caught in the de-risking vortex.

The Justice Department investigation known as Operation Choke Point was ostensibly launched in order to root out consumer fraud and money laundering. But critics argue that the probe has prompted banks to close the accounts of legal but politically unpopular businesses such as payday lenders and check-cashing services as well as arms dealers and tobacco sellers. Regulatory crackdowns on money laundering have also led banks to sever relationships with a range of cash-based businesses that could expose lenders to heightened scrutiny.

A spate of recent account closings at churches and religiously affiliated charities suggests that de-risking directives are causing collateral damage to faith-based organizations. A disturbing pattern is emerging in which banks close the large deposit accounts of these organizations and cancel their transactions without warning or explanation, giving the affected businesses no opportunity to appeal the decision. This could have potentially devastating consequences for the constitutionally protected right of churches and their faithful to freely exercise their religion.

These organizations are scrambling to find banks that will serve them. Their ability to function on a national level has been disrupted, jeopardizing their members' individual and collective freedom to practice their religion.

Take the example of one of my clients, a large Christian church with hundreds of brick and mortar locations operating in the U.S. The church recently received a notice of account closure from its primary banker.
Approximately half the church’s annual revenue comes from cash donations. But it engages in few cross-border transactions, conducts annual external audits and has written, independently tested cash-handling policies and procedures. A package of information detailing those safeguards, together with a request for an opportunity to present its compliance programs, was forwarded to the bank in response to the closure notice.

The bank denied the request without explanation, save a boilerplate statement that, while the bank had no reason to believe the church was involved in any problematic activity or transactions, it “just didn’t fit with the model of the kind of entity” that the bank wanted to do business with. The church’s subsequent attempts to develop banking relationships with other institutions met with little success.

Title II of the Civil Rights Act of 1964 prohibits discrimination based on religion in places of “public accommodation” that affect interstate commerce. In many state statutes, banks are considered places of public accommodation.

By compelling banks to close the accounts of allegedly high-risk clients, regulators are inadvertently denying churches and other cash-based religious organizations full and equal access to banking services. They simultaneously avoid the proper review and checks to which such government policies would otherwise be subject. The discriminatory effect of the new policies can be directly linked to the push to create desirable “client profiles” by closing the accounts of cash-dependent clients.

This effect is likely unintentional, but nonetheless real. Its origins may lie in a July 2014 letter released by the Federal Deposit Insurance Corp. that attempted to clarify its approach to supervising banking relationships with third-party payment processors. The FDIC had previously instructed banks to be on alert when banking for certain “high-risk” categories of merchants and included a list of the businesses it deemed risky. In its July 2014 letter, the FDIC removed the list in order to avoid misunderstandings. However, this left banks in a position in which they effectively had to guess about which clients might be perceived as posing reputational risk.

In the era of enhanced regulatory scrutiny, banks would rather play it safe and cut off blameless organizations than spend enormous amounts of time, money and energy attempting to predict which businesses will raise red flags. Therefore regulators are inadvertently encouraging the nationwide denial of banking services to legitimate organizations dedicated to faith and community service and protected by the freedom of religion guaranteed in the First Amendment of the Constitution.

Reasonable minds may differ about the desirability of using market-inhibiting regulatory practices to stymie legal but politically unpopular businesses. But surely all Americans can agree that a regulatory framework that threatens the viability of religious practice in a country founded on the notion of freedom of religion is, at the very least, in need of reform.

Incidents of Foreign Bribery Remain Largely The Same: A Circumstance Unlikely to Change

By Robert M. Appleton

Late last year, on December 2, 2014, seeking to measure transnational corruption, the Organization for Economic Co-Operation and Development (OECD), a leading international organization whose purpose is in part is to fight corruption within and throughout its Member States, issued a "Foreign Bribery Report, An analysis of the crime of bribery of foreign public officials" (OECD
Report). The most significant finding of the report is that just a small number of countries have taken successful action against bribery of public officials, in a relatively small number of cases, despite the omnipotence of foreign bribery activity. In analyzing 427 corruption enforcement actions taken by its 41 member states over the past 15 years, the OECD found that since 1999 just 17 countries successfully took action against bribery of public officials. The United States led the effort with 128 successful cases under the Foreign Corrupt Practices Act (FCPA) with Germany, Korea, Switzerland, the United Kingdom and Italy comprising most of the remainder. Only two member countries in Africa or Asia - Japan and Korea - had made a case- Korea with 11, and Japan with 3.

Read more...

**Derisking: FinCEN Has Your Cake and Eats it Too**
*By David L. Hall and Matthew P. Nettleton*

The Department of the Treasury's Financial Crimes Enforcement Center ("FinCEN") wants to have its cake and eat it too, if a recent FinCEN statement is any indication.

**FinCEN and Risk**

FinCEN, among other duties, is responsible for investigating and penalizing financial institutions that violate the Bank Secrecy Act's ("BSA") anti-money laundering ("AML") rules. Violations of the BSA can be costly. Over the past few years, FinCEN has pursued violators with vigor, assessing hundreds of millions of dollars in penalties for AML lapses or failures to file suspicious activity reports ("SARs"). Outside of monetary fines, the reputational damage for financial institutions implicated in money laundering investigations can also be high. And it is not just the institutions themselves feeling the brunt of regulatory scrutiny, as FinCEN recently assessed a $1 million penalty against MoneyGram's former chief compliance officer, in his individual capacity, for his role in his employer's BSA violations. To avoid these penalties, financial institutions must incur the increasing costs - in human resources, software systems, and time - of monitoring an increasingly complex customer base.

Read more...

**The SEC's Broken Windows Enforcement Policy: Is there Anything New Here?**
*By Denver G. Edwards*

Summary: This article examines the Commission's Broken Windows enforcement program and whether it should change how compliance professionals think about carrying out their duties. Historically, the Commission has been perceived as monitoring all areas of the securities markets. Broken Windows does not appear to be a significant shift. Instead, Broken Windows has intensified existing elements of the Commission's enforcement program. Compliance personnel need not overreact to the Commission rebranding as the tough cop on the beat, but they should remain vigilant of business practices within their organizations, leverage technology to monitor their organization's commercial activities, and think creatively about where and how violations may occur.

Read more...
The SEC's Broken Windows Enforcement Policy: Is there Anything New Here?

Denver G. Edwards

Summary: This article examines the Commission's Broken Windows enforcement program and whether it should change how compliance professionals think about carrying out their duties. Historically, the Commission has been perceived as monitoring all areas of the securities markets. Broken Windows does not appear to be a significant shift. Instead, Broken Windows has intensified existing elements of the Commission’s enforcement program. Compliance personnel need not overreact to the Commission rebranding as the tough cop on the beat, but they should remain vigilant of business practices within their organizations, leverage technology to monitor their organization's commercial activities, and think creatively about where and how violations may occur.

In the early 1990s, if you drove a car in New York City and were lucky, men carrying squeegees sprayed water on your windshield and demanded a tip. If you were unlucky, squeegee men, as there were known, merely spat on your windshield, wiped it off with a dirty rag, and then demanded a tip. Subway cars were “tagged” with graffiti and riders felt unsafe. Prostitution and peep shows littered Times Square, and up the street in Bryant Park, the drug trade flourished.

Former Mayor Rudy Giuliani and Police Commissioner Bill Bratton adopted a policing strategy in 1994 known as “Broken Windows” to combat “quality of life crimes.” The theory is that “when a window is broken and someone fixes it, it is a sign that disorder will not be tolerated. But, when a window is not fixed, it is a signal that no one cares, and so breaking more windows cost nothing.” Broken Windows aimed to avoid an environment of disorder that would encourage more serious crimes to flourish and to send a message of law and order. No infraction was too small to be uncovered and punished.

New York is markedly better today than it was in 1994. The squeegee-men have been banished. Subway cars are clean and safe day or night. Times Square is home to “Good Morning America,” and Bryant Park hosts New York Fashion Week in the fall and movie screenings in the summer.

Securities and Exchange Chairwoman, Mary Jo White, was the United States Attorney for the Southern District of New York from 1993 through 2002, and she witnessed New York’s transformation under Broken Windows. Chair White has sought to adapt the Broken Windows approach to regulation of the securities market.

In speech on October 9, 2013, Chair White said that the Commission’s enforcement program intends to be perceived as being “everywhere, pursuing all types of violation of federal securities law, big and small.” “Even the smallest infractions have victims, and the smallest infractions are very often just the first step toward bigger ones,” which “can foster a culture where laws are increasingly treated as toothless guidelines.” The Commission will be a strong cop on the beat and the Division of Enforcement will pursue not just the biggest frauds, but also violations such as control failures, negligence based offenses and strict liability offenses where intent is not required.

**The Broken Windows Enforcement Program**

The Broken Windows enforcement program is comprised of five elements:

- Streamline collaboration with the Department of Justice, Financial Industry Regulatory Authority (FINRA), and state securities regulators;
- Target gatekeepers;
• Leverage the Office of Compliance Inspections and Examinations (OCIE) to understand and monitor the latest risks and to provide effective oversight;
• Incentivize whistleblowers to report wrongdoing; and
• Marshal technology to analyze data efficiently.

Each of the first four elements has been a constant feature of the Commission’s enforcement regime. The Commission routinely works with the Department of Justice to conduct parallel investigations, as evidenced by recent insider trading investigations. Similarly, the Commission works with SROs, such as FINRA, to conduct “sweeps” to target industry-wide behaviors that are detrimental to investors and could jeopardize the integrity of the financial markets. The Commission collaborates with the North American Securities Administrators Association and state securities regulators to get intelligence on developments in state securities markets so that it can target issues before they become systemic problems.

The Commission has increasingly targeted “gatekeepers,” including attorneys and accountants since passage of the Sarbanes-Oxley Act (SOX), and more recently it has targeted broker-dealers who violate the market access rule.

OCIE has been the Commission’s “boots on the ground” to monitor risks posed by registrants since its creation in May 1995. OCIE has been a source of referrals for the Division of Enforcement since its inception. A key difference today, however, is that OCIE examiners specialize in discrete areas and are able to better understand the businesses they are examining, and the Division of Enforcement now values investigating and bringing non-fraud enforcement actions as it does bringing insider trading cases.

The Commission’s whistleblower bounty program has been effective since enactment of the Insider Trading and Securities Enforcement Act of 1988, which mandated payments for tips reporting insider trading. The Dodd-Frank Wall Street and Consumer Protection Act (Dodd-Frank) provides a 10% - 30% bounty for reporting violations of the securities laws in SEC or CFTC enforcement actions that result in monetary sanctions greater than $1 million.

The Commission’s investment in technology is the new feature of its enforcement program and may have the most significant impact on broker-dealer compliance functions. The Commission created the Center for Risk and Quantitative Analytics (CRQA) with a mandate to develop quantitative methods to monitor signs of potential wrongdoing and high risk behaviors. CRQA will feed its findings to the Division of Enforcement to investigate and prevent conduct that harm investors. The Commission has also developed the Advanced Bluesheet Analysis Program to analyze relationship among market participants to identify suspicious trading which may not be readily apparent. It also uses predictive analyses to spot trends, identify aberrational performance, and analyze data from new data sources, such as Form PF. On the examination side, the National Examination Analytics Tool (NEAT) enables the examiners to analyze millions of transaction documents accurately within a short time, and enables OCIE to do more precise and sophisticated examination.

More information about the long-term effectiveness of the Commission’s analytics tools is needed. Based on recent releases from the Commission, the tools are working as intended, and have increased the Commission’s ability to devise sophisticated surveillances of broker-dealer activities. For example, the Staff conducts link analyses, which looks for relationship between two disparate data sources, in insider trading cases. Link analysis has been used to analyze phone records and trading data to determine if two suspects had a phone call with the same person. In another example, the Staff has used link analysis to analyze large volumes of brokerage firm data to identify instances when a corporation allegedly purchased and sold its own stock, with no significant gain or loss, to create fictitiously high trading volume in order to obtain bank financing. The Staff has also used analytics to detect aberrational performance of a hedge fund that
fraudulently claimed it performed better than its peers throughout good and bad markets. These analyses use to take the Staff weeks or months to perform and were subject to human error. Today, these analyses can be completed within days. As a result of the Commission’s zero-tolerance for technical violations or control failures, and their willingness to bring enforcement actions for non-fraud cases, compliance officers will need to rethink how they fulfill their roles to protect their institutions.

**Broken Windows Presents Opportunities for Compliance**

Broken Windows presents two potential opportunities for compliance: (1) a chance for more assertiveness with business units in instituting rigorous controls and testing those controls more frequently; and (2) an opening to negotiate for more resources to respond to the regulatory environment and greater cooperation from other areas of the firm.

Broker-dealers are required by statute/regulations to have written supervisory policies and procedures (WSPs) regarding their activities. Compliance is a partner to a firm’s business units. However, the goal of the firm is to make money for clients, shareholders and employees, and onerous and overly restrictive WSPs may be perceived as limiting legitimate commercial activities for which buy-in from business units is necessary. Broken Windows presents an opportunity to tighten existing WSPs to limit supervisory gaps, require increased cooperation between compliance personnel and line supervisors, offer more training on codes of conduct and ethics for employees and management, and obtain more certifications or attestations regarding a supervisor’s fulfilling his or her supervisory obligation.

Moreover, Broken Window policies may help compliance obtain more resources and organizational support. Currently, compliance initiatives are balanced against interests of the firm, including for example, technology and operations projects that drive the firm’s commercial success. Compliance can cite penalties/fines as evidence of the Commission’s aggressive approach to demonstrate that lack of resources, including personnel or proper technology, create enterprise-wide legal, regulatory, and reputational risks that may have far-reaching consequences for clients, counterparties, shareholders, and may cause personal liability to supervisors and management.

The intensity around the Broken Windows enforcement policy arms compliance with tools to make the case to employees to report violations to compliance in order for the organization to avoid regulatory scrutiny, fines, and penalties. Compliance must balance encouraging employees to report violations internally while not undermining the employee’s right (and perhaps the Commission’s expectation) to report securities violations externally. As a starting point, compliance could appeal to the shared responsibility of each employee to root out bad actors that violate the securities laws, jeopardize investors, and threaten the integrity of the market. It could also promote methods within the organization to facilitate reporting violations, such as toll-free hotlines, an ombudsman position, anonymous e-mail websites to accept tips, and drop-boxes to submit tips regarding violations.

Without suggesting employees should not report externally, compliance could point out to employees that reporting outside (1) does not guarantee an award due to the high threshold (voluntarily providing original information and $1 million sanction), and (2) may have an impact on the organization. For example, in fiscal year 2014, the Commission received 3620 tips of which 139 (3.8%) received the designation of Notice of Covered Action (“NoCA”) and therefore eligible for an award. Since the inception of the program in August 2011, only 5.6% of tips (570 out of 10,193) have received the NoCA designation. The impact of non-qualifying tips include business disruption, lost productivity, costs to retain legal counsel to defend against regulatory investigations, and potential damage the firm’s reputation, and client or counterparty relationships. Compliance should reiterate to employees that external reporting remains an option if the
employee reports a violation internally to a designated person and the violation is not addressed timely. This approach balances the firm’s goal of operating in an efficient, ethical and commercially reasonable manner with the Commission’s interest in protecting investors and the market.

Considerations for Compliance Professionals

Compliance personnel who actively work with a business unit to implement WSPs risks being labeled a supervisor and may be subject to liability for aiding and abetting or failure to supervise. Compliance personnel may minimize the risk of being labeled a supervisor by establishing in meetings with business supervisors that although he or she is an integral part of the business unit’s operations, the business supervisor is the designated supervisor. Compliance personnel must document the supervisory reviews of the business that the supervisor is responsible for overseeing, and should periodically obtain certifications or attestations from supervisors indicating that she or he understands his or her supervisory role and is undertaking his or her supervisory obligations. More generally, compliance should ensure that the firm’s supervisory manual states that compliance personnel are solely responsible for activities within the compliance department.

Compliance personnel should have a predetermined process to investigate, track and document red flags. They must act decisively when red flags surface or if red flags are brought to their attention. Compliance personnel should document each red flag, which business supervisors will address the red flag, and what corrective action will be taken. Compliance personnel must take reasonable steps to follow up with the business supervisor to ensure the issue has been resolved and then must monitor the issue to ensure it does not recur. Compliance personnel should also share information with firm management (particularly if a red flag involves a senior manager), and should be prepared, and have a process in place, to escalate matters to the Board of Directors if management fails to take corrective action.

Membership on firm committees is also an area of concern for compliance personnel. As evidenced in In the Matter of Theodore Urban, membership on certain firm committees may cause the Commission to determine that compliance personnel who, as a member of a committee, learn critical information about a violation have a duty to ensure that corrective action is taken. The Commission’s approach exposes compliance personnel to personal liability that could potentially jeopardize careers and, as a result, may cause qualified candidates to avoid compliance roles.

The Commission’s use of data analytics tools has increased the pressure on compliance personnel to ferret out fraud, technical violations, and control failures. One approach is to conduct surveillances similar to those performed by the SEC’s analytics teams. Some reliable off-the-shelf surveillance may be available, but compliance may have to leverage internal information technology resources and get buy-in from business units to build surveillance tools to counter the SEC. The associated costs may be significant since the Commission’s data analytics program is continuously evolving and broker-dealers would need to keep pace. However, since repeated violations could lead to increasingly severe fines, create the impression that there is a lack of institutional control at firms, personal liability, and could jeopardize firms’ reputation and client relationships, firm may have limited choice.

The other alternative is for compliance personnel to rely on the traditional approach, which is based on developing strong policies and procedures that match the firm’s business and the regulatory environment, and diligent oversight. This approach requires frequent monitoring and testing of the adequacy of business units’ compliance with polices and procedures. It also requires compliance personnel regularly ask where issues could occur, what controls are in place to prevent or detect problems, and what residual risks remain unmitigated by such controls.
Broken Windows has helped the Commission become more efficient in how it implements its enforcement program. Yet, Broken Windows does not represent a substantive change in the Commission's enforcement policy. SOX and Dodd-Frank reiterated to compliance personnel the need to establish strong controls and vigilance to protect their firms, investors, and the integrity of the market. Responsible compliance personnel have heard that message and approach their roles with professionalism and integrity. Broker-dealers should continue to prioritize implementing existing regulations, monitor controls, and thoughtfully consider where violations may occur within their organizations, rather than overreact to the Commission's efforts to rebrand itself as a tough cop on the beat.
The Department of the Treasury’s Financial Crimes Enforcement Center ("FinCEN") wants to have its cake and eat it too, if a recent FinCEN statement is any indication.

**FinCEN and Risk**

FinCEN, among other duties, is responsible for investigating and penalizing financial institutions that violate the Bank Secrecy Act’s (“BSA”) anti-money laundering (“AML”) rules. Violations of the BSA can be costly. Over the past few years, FinCEN has pursued violators with vigor, assessing hundreds of millions of dollars in penalties for AML lapses or failures to file suspicious activity reports (“SARs”).1 Outside of monetary fines, the reputational damage for financial institutions implicated in money laundering investigations can also be high. And it is not just the institutions themselves feeling the brunt of regulatory scrutiny, as FinCEN recently assessed a $1 million penalty against MoneyGram’s former chief compliance officer, in his individual capacity, for his role in his employer’s BSA violations.2 To avoid these penalties, financial institutions must incur the increasing costs – in human resources, software systems, and time – of monitoring an increasingly complex customer base.

On the other hand, FinCEN needs the very entities it regulates to be partners: SARs help regulators identify crimes, including money laundering, smuggling, and terrorist financing. However, as both the penalties for BSA violations and compliance costs rise, banks are faced with a business decision: in light of the risk and expense, should they provide banking services to customers that present higher risks of BSA noncompliance? For a growing number of banks, the answer is no. These banks have started to “de-risk” – that is, they are terminating or declining to open accounts for entities—such as money services businesses (“MSBs”)—perceived to be high AML risks.

**FinCEN Discourages De-Risking**

FinCEN and other regulators are not pleased.

In response to de-risking by financial institutions, FinCEN took the unusual step of issuing an official statement on November 10, 2014 (“November Statement”) stating: “Currently, there is concern that banks are indiscriminately terminating the accounts of all MSBs, or refusing to open

---

accounts for any MSBs, thereby eliminating them as a category of customers.” The November Statement makes clear FinCEN’s opposition to this trend: “FinCEN does not support the wholesale termination of MSB accounts without regard to the risks presented or the banks’ ability to manage the risk… MSBs present varying degrees of risk, and not all money services business are high-risk.” Similar comments against de-risking have been made by Comptroller of the Currency and the international Financial Action Task Force (“FATF”).

In a way, the November Statement is déjà vu all over again. In 2005, banks responded to new FinCEN AML guidelines by severing relationships with MSBs. FinCEN and other financial regulators then issued an advisory touting the importance of MSBs to the financial sector and asserting: “It is essential that banking organizations neither define nor treat all money services businesses as posing the same level of risk.” FinCEN, as in the November Statement, urged banks to view MSBs on a case-by-case basis and use a risk-based approach in determining whether to offer banking services. Since 2005, the AML risks associated with MSBs have only increased.

**Why are MSBs Perceived as More Risky than other Banking Customers?**

The BSA defines an MSB as a financial institution that, among other things, has one or more the following capacities: an issuer or seller of traveler's checks/money orders; a redeemer of traveler's checks; a money transmitter; a check cashier; a dealer in foreign exchange; or a provider of prepaid access. MSBs typically need access to banking services in order to operate.

MSBs, as the Federal Deposit Insurance Corporation, has noted, have been used as conduits for illicit cash and monetary instrument transactions, check kiting, concealment of beneficiaries, and processing forged or fraudulent checks and money orders. The 2014 Federal Financial Institutions Examination Council BSA/AML Examination Manual (“FFIEC Manual”) further notes that banks that maintain account relationships with non-bank institutions like MSBs may be exposed to a higher risk for money laundering activities because many MSBs do not have long-term customer relationships and require minimal or no customer identification, maintain

---

4 Thomas J. Curry, Comptroller of the Currency, Remarks Before the Association of Certified Anti-Money Laundering Specialists, March 17, 2014 (“[D]e-risking has been a topic of much discussion lately… I understand why you would want to be cautious – some types of businesses are more risky than others and require a higher level of due diligence…However, that’s why we support a risk-based approach.”).
7 31 U.S.C. §1010.100(ff)
8 FDIC, Risk Management Manual of Examination Policies, Section 8.1
limited or inconsistent record keeping on customers and transactions, engage in frequent
currency transactions, and often change their product mix or location.\(^9\)

In addition to these inherit risks, the MSB marketplace is changing rapidly. For example, there
is the growth of third-party payment processors (“TPPPs”), bank customers that provide payment
processing services to merchants and other business entities. TPPPs typically use their deposit
accounts to process transactions on behalf of merchant clients that do not have a direct
relationship with the TPPP’s financial institution. A 2012 FinCEN bulletin noted that “Payment
Processors providing consumer transactions on behalf of telemarketing and Internet merchants
may present a higher risk profile to a financial institution than would other businesses.”\(^10\)

Other new payment products (“NPP”) – like mobile banking, pre-paid cards, and non-deposit
instruments – also add to a bank’s AML risk profile, as the nature of NPP transactions can
obscure their true purpose. And then there is virtual currency, such as BitCoin.\(^11\) To provide
banking services to a virtual currency exchange, a bank must expend significant resources to
assess the risks associated with an opaque exchange resulting from the inherently quasi-
anonymous features of virtual currency itself.

A bank that determines an MSB customer presents a relatively high money laundering or
terrorist financing risk, must engage in resource-intensive due diligence. The FFIEC Manual
identifies some of the steps a regulator expects a bank to take in such cases, including: review
the MSB’s BSA/AML program and the results of the MSB’s independent testing of its AML
program; review written procedures for the operation of the MSB; conduct on-site visits; review
a list of agents, including locations, both within and outside the United States, receiving services
directly or indirectly through the MSB account; review written employee screening practices for
the MSB.\(^12\)

Or the bank can make the risk-based decision that it will not deal with MSBs.\(^13\)

**More Responsibilities for Banks on the Way**

In an effort to stem the tide of de-risking, FinCEN tried to strike a conciliatory tone in the
November Statement. FinCEN remarked that “the Bank Secrecy Act does not require, and

\(^10\) FinCEN Advisory, FIN-2012-A010, October 22, 2012
\(^11\) FinCEN Guidance, FIN-2013-G001, March 18, 2013
\(^12\) FFIEC Manual (2014), at 311.
\(^13\) Banks today are also faced with a question about providing banking services to entities in
Colorado and Washington legally engaged in the marijuana industry. A recent report noted that
between February and August 2014, banks filed more than 475 Marijuana Termination
suspicious activity reports — indicating they closed hundreds of accounts because of possible
criminal activity. See Feds Stockpile Reports That Could Incriminate Pot Stores, *USA Today*
stockpile-reports-that-could-close-pot-stores/19806721/
neither does FinCEN expect, banking institutions to serve as the de facto regulator of the money services business industry any more than of any other industry.” It continued: “FinCEN recognizes that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through an institution.” Despite the encouraging words, the November Statement does not provide any respite for banks that have determined the cost of banking MSBs is too high. On the contrary, the message was clear: de-risking will not serve to excuse a bank’s failure to implement a risk-based approach with regard to MSBs.

Adding to the AML burdens of financial institutions, FinCEN seeks to impose new requirements under the BSA. Presently, the BSA requires financial institutions to build its AML program on four pillars: (1) a system of internal controls to ensure ongoing compliance; (2) independent testing; (3) designation of a BSA compliance officer; and (4) training for appropriate personnel.14 In a July 2014 Notice of Proposed Rulemaking (“NPR”), FinCEN proposed adding “a fifth pillar”: customer due diligence (“CDD”) pertaining to understanding the nature and purpose of customer relationships.

FinCEN is also proposing that financial institutions collect more detailed information on the natural persons behind legal entities by identifying and verifying the beneficial owners of legal entity customers, subject to certain exemptions. To this end, FinCEN has proposed a definition of “beneficial owner” that would include two independent prongs: an ownership prong and a control prong. Under the proposed beneficial ownership rule, a covered financial institution would have to identify each individual who owns 25 percent or more of the equity of the covered financial institution’s “legal entity customer” and also one individual who exercises significant managerial control over the legal entity customer. If no individual owns 25 percent or more of the equity interests, the covered financial institution may identify a beneficial owner under the control prong only.

What’s Next?

Thomas Curry, Comptroller of the Currency, speaking on the subject of BSA compliance, stated in a 2014 speech: “It’s clear that we all need to step up our game, both banks and Government alike, because the challenges are growing by the day.” Innovation and technological advances are likely to make MSB activities increasingly complex and thereby render MSBs, compared to other customers, expensive for banks to service. And as regulators increase both their expectations for AML programs and the penalties for BSA violations, the de-risking trend is not likely to slow. Though the November Statement noted that FinCEN was “committed to taking steps to address the wholesale debanking of an important part of the financial system,” the statement did not provide any hints to what those steps might be.

For FinCEN, de-risking is a misnomer: when a bank refuses to deal with an MSB, the money laundering risks do not disappear; they are merely transferred elsewhere. The key question becomes: where? This is an important question, one that FinCEN, not the banking industry, must answer.

14 31 U.S.C. § 5138(h)
Incidents of Foreign Bribery Remain Largely The Same:
A circumstance unlikely to Change

By: Robert M. Appleton, Esq, Day Pitney LLP

Late last year, on December 2, 2014, seeking to measure transnational corruption, the Organization for Economic Co-Operation and Development (OECD), a leading international organization whose purpose is in part is to fight corruption within and throughout its Member States, issued a “Foreign Bribery Report, An analysis of the crime of bribery of foreign public officials” (OECD Report). The most significant finding of the report is that just a small number of countries have taken successful action against bribery of public officials, in a relatively small number of cases, despite the omnipotence of foreign bribery activity. In analyzing 427 corruption enforcement actions taken by its 41 member states over the past 15 years, the OECD found that since 1999 just 17 countries successfully took action against bribery of public officials. The United States led the effort with 128 successful cases under the Foreign Corrupt Practices Act (FCPA) with Germany, Korea, Switzerland, the United Kingdom and Italy comprising most of the remainder. Only two member countries in Africa or Asia – Japan and Korea – had made a case – Korea with 11, and Japan with 3.

For some time now, practitioners, scholars, politicians and the public have asked the question why aren’t more bribery actions pursued, and why aren’t more judgments and convictions achieved, especially in the developing world if these regions are as rife with public corruption as is often asserted. Some commentators, including the OECD report writers, have interpreted the OECD results as confirming that the perception that corruption is largely confined to the developing world is overblown. They offer that the countries higher on the UN’s Human Development Index (HDI) may be largely responsible for foreign bribery cases because almost half of those committing the offenses hailed from, and two-thirds of bribes were also paid to, officials from such countries. The Report concludes that “the data certainly shows that bribes are being paid to officials in economies at all stages of development, not just developing economies, as many might have believed.”

In my experience, however, these conclusions under-report the state of corruption in developing economies, and under emphasize the extensive presence of corruption in public contracting worldwide. The findings are potentially misleading because the OECD analysis is focused only on made prosecutions,
rather than incidents of bribery. Over the past 10 years, after leading, managing and supervising more than 600 forensic investigations, audits, inquiries, examinations and prosecutions of corruption in government and public procurement and contracting in the field and on the ground throughout Africa, Asia and the Middle East in leading international investigation positions, it is clear to me that public bribery remains ubiquitous, and remains largely unaddressed.

While attesting to the contrary, the OECD Report presents just a portion of the story: The OECD did not, and the Report does not, attempt to track *incidents* of corruption, only those cases pursued by some governments, and only those pursued successfully. As the report readily acknowledges, it focused upon just the 427 successfully completed law enforcement cases that have been publicly reported since 1999. There are *many* cases that exist, but aren’t reported because no action has been taken. This piece focuses upon some possible reasons for this anomaly.

First, it is important to emphasize that 17 is a paltry number of countries successfully pursuing corruption, and 427 cases, worldwide, over a fifteen year period is exceedingly small. Based upon my experiences in these regions and in the US, it is evident that corruption remains rife throughout the world, and insufficiently addressed in the developing world for several different reasons. The numbers are in fact much greater, and many more countries should be achieving success.

One of the most important reasons for this anomaly is what sometimes gets called the “culture of corruption”, but might more accurately be described as a customary practice. The payment of sums of money to trigger the award of a contract, or as a gratuity payment in return for the award of a government or public contract, remains not only not illegal or not prosecuted in some places, but indeed an accepted customary practice. In most countries high on the HDI, payments to public officials to influence contract awards is considered corrupt, illegal and immoral. Such is the case in the Nordic countries, where it is universally understood and accepted that corruption barely exists. In many other parts of the world, however, a gratuity to a public official or the entity granting a contract award is a customary gesture, accepted and historically a part of doing business. It is not considered immoral, and often not criminalized, despite the fact that some of these countries are signatories to the *OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* and the UN Convention Against Corruption (UNCAC). It is considered ancillary to the way in which business is conducted, and accepted. As such, governments are hesitant to
criminalize or prosecute the practice, and even those countries that have recently enacted laws or established “anti-corruption bodies”, have been reluctant to enforce the laws, especially when it involves senior government officials in their country.

There are other related reasons for the fact that bribery payments to public officials is not addressed in the criminal justice systems of a number of countries. The legal framework in some countries either does not exist, or, the jurisdiction lacks sufficient legislation to address the crimes in the forms in which they are perpetrated. Further, many countries do not possess the requisite investigative or prosecutorial capacity and resources to address these issues. In investigating these matters throughout Africa, the Middle East and parts of Asia over the last 10 years, I found that many law enforcement bodies were understaffed and under-funded, or their attention was placed upon different priorities. Further, inter-country cooperation in Africa and other regions remains at its infancy. Only rarely could law enforcement count on regional support. Support from international bodies is on the rise, but remains a small contribution, and these bodies, other than OLAF (the European Anti-Fraud Office) lack an ability to bring criminal cases.

Third, and very importantly, many countries do not have laws that allow for extraterritorial jurisdiction, the ability to prosecute matters that occur outside of their national boundaries, committed by its citizens or corporations abroad, and sometimes others. The jurisdiction of most law enforcement bodies remains domestic, meaning they can pursue criminal acts that occur with their boundaries. Thus, if a citizen of their country engages in bribery abroad, or in a neighboring country, it is quite unlikely that the person will be prosecuted by their home country. Rather, enforcing the law is left to the host country, where the contract is awarded. This circumstance significantly curtails the number of foreign bribery cases significantly.

Only a very few countries possess extra-territorial laws that are able to reach foreign corruption. In addition to the US with the FCPA, the United Kingdom recently adopted the UK Bribery Act, which for the first time allows for extraterritorial reach of the bribery laws of Great Britain, and allows law enforcement in the UK the ability to reach acts of corruption abroad. The United States is the leading authority pursuing foreign bribery, where, under the Foreign Corrupt Practices Act, the OECD found that the US Department of Justice and its counterpart the Securities and Exchange Commission (SEC) prosecuted almost five times more public bribery cases than the next closest nation state, Germany (128 and 26 respectively).
Nonetheless, perhaps the most significant reason for the lack of anti-bribery success in many regions is a fear of holding senior government officials accountable. My experience has too often been that as the investigation reaches closer to the party in power, or in the higher ranks of government, the less likely it is that the case is pursued by the host government. I experienced this phenomenon first-hand a number of times. One of the deepest investigations pursued was undertaken in a West African state, where we focused upon allegations of fraud and bribery in the multi-million dollar grants to the country from an international donor over a five year period. Investigations on the ground identified serious irregularities with the uses of the grant funds, and more than half of the grant monies were lost due to corruption and mismanagement. At first, the government cooperated with our investigation in-country, and even coordinated their efforts with us. To their credit, the government appointed a special Magistrate to investigate the case, and under his supervision and authority, the local authorities arrested 16 individuals, mostly smaller business owners and individuals who were responsible for defrauding the grant programs through the submission of fake invoices to trigger the payment of grant funds. The case received significant publicity in the country, and profound support. However, when allegations surfaced of bribery in the senior ranks of a Ministry, and the investigation began to focus upon more senior officials in the government, the government significantly reduced the Magistrate’s authority, and ultimately rendered him powerless - taking him off of the case. We repeatedly requested that the Magistrate be re-instituted, but to no avail. The cases and the investigations died, yet the grant funds continued to flow into the country.

Similarly, referrals of cases to other neighboring countries that were accompanied by detailed reports containing the forensic evidence proving the crimes, were left to languish, and were not pursued. Pursuing such cases and making arrests for bribery and other forms of corruption, is not considered popular – as it results in press attention, perceived embarrassment and feared adverse consequences – namely the loss of further international aid and grant funding. Indeed, some international aid agencies require the return of the grant funds if it is found that corruption has permeated the grant programs and funds have been lost to corruption, theft and misappropriation.

Further, as indicated above, it has historically been customary, and indeed the expectation, for corporations, foreign and domestic, to bestow gifts upon public officials for the benefit and privilege of receiving a contract from them. In a number of such jurisdictions, it is indeed ordinary and routine to pay the
government officials in the ministry a set percentage of the aggregate contract amount as a tribute for the awarding of the contract. It is also customary for percentages of the bribe payments made to be divided amongst a number of government officials once received, and the divided amounts transferred further up the chain of command to more senior officials in the particular ministry in the government. Not only is corruption not prosecuted, other officials join in the spoils of the bribe or gratuity payments.

Between 2010 and 2013, I experienced this phenomena in a South Asian country in connection with an investigation of allegations of corruption in the award of hundreds of millions of dollars’ worth of contracts from the health ministry for the purchase of health products for distribution throughout the country. The contracts had been funded by international donor grant monies that were then used by the particular health ministry to award contracts through public procurement exercises. The procurement exercises were merely window dressing. The investigation identified overwhelming and indeed uncontroverted evidence that one of Asia’s largest global companies, based in the Far East, as well as another European corporation, paid a series of bribes as well as kickbacks amounting to close to $1 million in the aggregate, to government officials in the small south Asian country over an almost 10 year period. The payments were made to relatives of the officials, and into out of country bank accounts in US dollars. The payments were made in exchange for the award of a series of contracts for the provision of these health products, and were made by company representatives, and intermediaries and agents for the companies that acted on the ground in the country.

The emails exchanges in furtherance of the bribe and gratuity payments were open and obvious. The corporate representative openly paid for vacations for the Director of the government ministry, an expensive watch for the Director’s daughter, travel to a medical specialist abroad, and cash and other gifts. Company officials cooperating with the investigation readily acknowledged the fact that in order to earn a contract from the government, gratuity payments and/or bribes had to be paid to the relevant government officials involved in the awarding of the contract. Otherwise, without the payments, the contract would be awarded to a company who agreed to pay. This circumstance was no secret, and was known to the various foreigners and ex-pats that lived in the capitol as well as representatives of the various foreign ministries that maintained a presence in the capital city. Yet, the practice went on unabated, and other international aid agencies and foreign ministries only rang alarm bells and became concerned when they realized our report was going to be made public.
While perhaps customary, evidence was identified that the ministry officials knew that this conduct was improper. The funds were directed to secret offshore bank accounts in the names of third parties, and emails included instructions to delete the messages once read.

Through the review of a myriad of records and emails, and interviewing dozens of whistle-blowers, cooperating witnesses, public officials, and participants in a number of these schemes, including the agents of the corporations and corporate officials who paid the bribes, not only was foreign bribery obvious, it was clear that the payments were a prerequisite for the award of the contracts. It was understood that the payments would be made either in advance, or once the contract was awarded. The amount was calculated as a percentage of the aggregate contract amount, and the Director commanded a 15% payment. Significantly, though, despite the fact that the case was referred to the newly formed anti-corruption commission in the country, the company officials and the corporation have not been prosecuted, nor have the two government officials been charged with any crime. The corporation fired the two senior executives involved in the bribe payments only after we began investigating and they admitted their conduct in interviews with corporate counsel present. The two companies were suspended from further contracts for a time, but beyond that, nothing else has happened.

This case, of course, is not included in the OECD case statistics because no prosecution was pursued and no “case” was successfully made. Yet, the incidents, like many others, are real. In addition to there being no “record” of the case, results such as these diminishes the drive of those who truly seek to halt corruption, and numbs many to the point where the practice is simply accepted, and ignored. Further, international organizations accept these circumstances and may no longer be willing to suspend aid in the wake of corruption, under the belief that a percentage of corruption must be accepted as a cost of international aid. As such, incidents of corruption continue to occur unabated, and many are largely ignored.

Nevertheless, while many multi national and international companies operate at times with impunity in local jurisdictions, a common theme expressed by many corporations though, is a fear of the FCPA. Countless corporate officials of many differing nationalities routinely asked whether the matter would be referred to, and pursued by, the US government under the FCPA, with its extraterritorial reach. The US law remains perhaps the most feared possible repercussion for companies engaged in bribery abroad, even in circumstances
where the company and the foreign official were not US persons or corporations with a US presence.

The FCPA cannot reach all of these bribery schemes, however. In many instances, despite its extraterritorial status, the law does not apply to purely foreign bribery cases. In addition, foreign cases are difficult to make, and they take time. Indeed, the OECD numbers confirm this, as the report finds that law enforcement is responsible for just 13% of case initiations. This is not a surprising result. It is extremely difficult for law enforcement authorities of any nationality to gather foreign evidence, interview foreign witnesses, and execute foreign search and seizure warrants. Requests of the local government can be made, but rarely are such matters pursued in a timely fashion. Compulsory process for most is limited to the home country. To obtain foreign evidence and the right to access witnesses through formal processes, law enforcement in most places must typically use such instruments as Mutual Legal Assistance Treaties or Letters Rogatory, formal processes, which often takes years.

The reality is that the extent of foreign public bribery continues not to be fully known, nor accurately quantified. However, it is axiomatic that way too few countries are successfully pursuing these cases, and way too few cases are being made. Unless attitudes change, and countries act upon foreign bribery in practice as well as denouncing it in policy instruments, and unless resources are applied, proper laws are enacted and truly enforced, and law enforcement throughout the world are given the means and the statutory ability to address these cases, the rates of public corruption will not lessen, and the scourge of public corruption will not be erased.