Regulatory Focus: AML, Cybersecurity and FCPA

Schulte Roth&Zabel

26TH ANNUAL PIF PRIVATE INVESTMENT FUNDS SEMINAR

January 17, 2017

Partner

Washington, DC Office
+1 202.729.7462

New York Office
+1 212.756.2791

adam.hoffinger@srz.com

Practices

Litigation

Complex Commercial Litigation

Securities Enforcement

Securities Litigation

White Collar Defense & Government Investigations

Adam S. Hoffinger

Adam serves as co-chair of Schulte Roth & Zabel's White Collar Defense & Government Investigations Group. He focuses his practice on complex civil and white collar criminal matters, including securities, health care, False Claims Act ("qui tam"), the Foreign Corrupt Practices Act (FCPA), export sanctions, criminal tax, money laundering, antitrust and bankruptcy. He counsels corporations and individuals in compliance matters, internal investigations, and Congressional and regulatory matters. He also represents corporations and individuals in high-stakes civil litigation. Adam has defended numerous high-ranking executives and general counsel from some of the world's largest companies, as well as high-profile staff and members of the Senate, Congress, White House and various government agencies, faced with federal and state criminal investigations and indictments. He is a Fellow of the American College of Trial Lawyers and has successfully tried cases throughout the country.

Adam has been recognized in *Chambers USA* for his "immense talent as a trial lawyer" and "strong advocacy skills," in *The Legal 500 United States* as "an aggressive trial advocate," and in *Benchmark Litigation: The Definitive Guide to America's Leading Litigation Firms and Attorneys* as a "celebrated government investigations practitioner." He has also been recognized in *The Best Lawyers in America, Expert Guide to the World's Leading White Collar Crime Lawyers*, *International Who's Who of Business Crimes Defense Lawyers*, *Global Investigations Review*, *Washingtonian Magazine* and *Washington DC Super Lawyers*. Adam was named "Government Investigations Attorney of the Year" for 2015 and "Life Sciences Star" from 2013 to 2016 in *LMG Life Sciences*. In addition, he was recognized in the *National Law Journal*'s "Hot Defense List" for his jury trial victory on behalf of a former pharmaceutical executive in a criminal case charging conspiracy and violations of the federal Anti-Kickback Statute. Adam is a former Assistant U.S. Attorney for the Southern District of New York, and he received the Director's Award for Superior Performance from the U.S. Department of Justice in 1990. He is an adjunct professor at The George Washington University Law School and has been an instructor at Georgetown University Law Center's National Institute of Trial Advocacy (NITA) since 1992. He also serves on the alumni board of the Fordham University School of Law. Adam frequently speaks about topics of interest to the private funds industry, including audit committee investigations, recovery of assets, and obtaining and negotiating corporate deferred and non-prosecution agreements.

Adam received his J.D. from Fordham University School of Law and his B.A. from Trinity College.

Partner
New York Office
+1 212.756.2201
daniel.hunter@srz.com

Practices

Investment Management
Hedge Funds
Private Equity
Regulatory & Compliance

Daniel F. Hunter

Dan concentrates his practice on the design, structure and regulation of private investment funds, including hedge funds, hybrid funds and private equity funds. He specializes in providing advice to credit funds and advises on insurance dedicated funds. Dan also provides day-to-day regulatory, operational, merger and acquisition, and restructuring advice to his fund clients, and he advises funds regarding the receipt or allocation of seed capital. As part of his compliance practice, he advises clients on the Treasury Forms (TIC Forms) and Bureau of Economic Affairs Forms (BEA Forms).

Dan has been recognized in *The Legal 500 United States* in the Investment Fund Formation and Management and Private Equity Funds categories. A sought-after speaker, he recently presented on topics including the structuring and management of funds, compliance and regulatory issues, and ERISA's impact on private equity and hedge funds. He recently presented an SRZ webinar on "Insurance-Dedicated Funds: Tax and Corporate Issues," and at an SRZ breakfast briefing on "Current Issues Impacting Private Investment Funds." He also spoke at the AIMA Navigating the Landscape of Side Letter Terms Seminar. Dan was recently featured in *The Hedge Fund Journal* article "Co-Investments with SRZ's Leading Fund Formation Group" and is a co-author of *Hedge Funds: Formation, Operation and Regulation* (ALM Law Journal Press). He has served as a guest lecturer at the New York University School of Continuing and Professional Studies, where he taught "Introduction to Hedge Funds." He also serves on the University of Michigan Honors Alumni Council.

Dan received his J.D. from the University of Michigan Law School and his A.B., *cum laude* and *with high honors* in history, from the University of Michigan.

Partner
New York Office
+1 212.756.2588
seetha.ramachandran@srz.com

Practices

Litigation

Bank Regulatory

Financial Institutions

Regulatory & Compliance

Securities Enforcement

White Collar Defense & Government Investigations

Seetha Ramachandran

Seetha focuses her practice on anti-money laundering and OFAC compliance, regulatory investigations and enforcement actions, white-collar criminal defense, and criminal and civil forfeiture matters. She has represented companies and individuals in criminal and regulatory investigations by the DOJ, New York Attorney General, CFTC and SEC, as well as conducted internal investigations. She has also advised a range of companies, including hedge funds, private equity funds, banks, broker-dealers and money services businesses on AML and OFAC compliance, as well as other regulatory issues. As a federal prosecutor for nearly a decade, Seetha spearheaded and oversaw DOJ's first major AML prosecutions, including those of HSBC, MoneyGram, Standard Chartered Bank and ING. Much of her work developing and charging criminal cases under the Bank Secrecy Act (BSA) formed the model for AML enforcement that regulators and prosecutors apply today, making her uniquely well-positioned to advise clients in this area. She also has deep experience negotiating the penalty phase of AML and forfeiture matters large and small, ranging from those involving global financial institutions to individual defendants. Seetha is a former Deputy Chief in the Asset Forfeiture and Money Laundering Section (AFMLS), Criminal Division, U.S. Department of Justice, where she was the first head of the Money Laundering & Bank Integrity Unit — DOJ's criminal litigation unit focused on AML and sanctions enforcement. In this role, she supervised BSA cases against traditional financial institutions like banks, as well as those involving emerging areas of BSA enforcement, such as casino gambling, online payment systems and virtual currencies. Seetha also worked closely with state and federal banking regulators and U.S. Attorneys' offices nationwide, providing expert advice on cases involving the BSA, complex money laundering and financial institutions. Prior to her appointment at AFMLS, Seetha served as an Assistant U.S. Attorney for the Southern District of New York for nearly six years, where she worked in the Complex Frauds, Major Crimes and Asset Forfeiture units. As an Assistant U.S. Attorney, she investigated and prosecuted white collar cases involving a wide range of financial crimes, including bank fraud, mail and wire fraud, tax fraud, money laundering, stolen art and cultural property, and civil and criminal forfeiture cases, and she conducted 10 jury trials and argued 10 appeals before the U.S. Court of Appeals for the Second Circuit. She is also a former law clerk for the Honorable Richard J. Cardamone of the U.S. Court of Appeals for the Second Circuit.

The Legal 500 United States has recognized Seetha as a leading lawyer. She has counseled a range of companies on AML and OFAC compliance programs and procedures, including banks, broker-dealers, hedge funds, private equity firms, loan and finance companies, money services businesses, and online payment companies. An accomplished public speaker, she has presented on topics that include enforcement trends in the financial services industry, effective AML programs and asset forfeiture. Seetha is the co-author of "NYDFS Issues AML/Sanctions Programs and Annual Certification Requirements for Banks, Money Transmitters and Check Cashers" in *Westlaw Journal — Bank & Lender Liability*, "The New AML Rules: Implications for Private Fund Managers" in *The Hedge Fund Journal*, "Federal and State Regulators Target Compliance Officers — Parts I and II" in *The Banking Law Journal* and "The Interplay Between Forfeiture and Restitution in Complex Multi-Victim White Collar Cases" in the *Federal Sentencing Reporter*.

Seetha earned her J.D. from Columbia Law School and her B.A., *magna cum laude*, from Brown University.

Partner
New York Office
+1 212.756.2441
gary.stein@srz.com

Practices

Litigation

Regulatory & Compliance

Securities Enforcement

White Collar Defense
& Government Investigations

Gary Stein

Gary focuses on white collar criminal defense and securities regulatory matters, complex commercial litigation, internal investigations, anti-money laundering issues, civil and criminal forfeiture proceedings and appellate litigation. He represents public companies, financial institutions, hedge funds, other entities and individuals as subjects, victims and witnesses in federal and state criminal investigations and regulatory investigations by the SEC, SROs and state attorneys general. He has conducted numerous internal investigations involving potential violations of the Foreign Corrupt Practices Act, financial statement fraud, money laundering and other matters, and advises companies on compliance with the FCPA and anti-money laundering and OFAC regulations. As a former Assistant U.S. Attorney and chief appellate attorney in the Southern District of New York, Gary investigated, prosecuted, tried and represented the government on appeal in numerous white collar criminal cases involving money laundering, fraudulent investment schemes, bank fraud, insider trading, art theft, illegal kickbacks, terrorist financing and other financial crimes. His civil litigation experience includes claims of fraud and breach of contract, securities class actions and derivative actions, contests over corporate control, and disputes arising from the sale of a business. He has handled more than 150 appeals in federal and state courts involving issues of both criminal law and procedure and complex commercial law. He has successfully argued 15 appeals in the U.S. Court of Appeals for the Second Circuit and led the firm's pro bono representation in *Hurrell-Harring v. State of New York*, which resulted in a historic settlement that lays the foundation for statewide reform of New York's public defense system, and for which he received *New York Law Journal*'s 2015 Lawyers Who Lead by Example Award.

Gary is listed as a leading litigation lawyer in *Benchmark Litigation: The Definitive Guide to America's Leading Litigation Firms & Attorneys*, *The Legal 500 United States* and *New York Super Lawyers*. He regularly presents on FCPA, insider trading and trading compliance, risk management and crisis management issues at conferences and is an accomplished writer. He is the recipient of Burton Awards for Achievement in Legal Writing: In 2008, he won for co-authoring "The Foreign Corrupt Practices Act: Recent Cases and Enforcement Trends," which appeared in the *Journal of Investment Compliance*; and in 2015, he won for authoring "Pension Forfeiture and Prosecutorial Policy-Making," which appeared in the *N.Y.U. Journal of Legislation and Public Policy Quorum*. He is also the co-author of the "Scienter: Trading 'On the Basis Of'" chapter in the *Insider Trading Law and Compliance Answer Book* (Practising Law Institute) and of "The New AML Rules: Implications for Private Fund Managers" in *The Hedge Fund Journal*. He serves on the board of directors of The Legal Aid Society and the board of editors of the *Business Crimes Bulletin*.

Gary obtained his J.D. from New York University School of Law and his B.A. from New York University.

Special Counsel
New York Office
+1 212.756.2290
michael.yaeger@srz.com

Practices

Litigation

Cybersecurity

Securities Enforcement

White Collar Defense
& Government Investigations

Michael L. Yaeger

Michael focuses his practice on white collar criminal defense and investigations, securities enforcement, internal investigations, accounting fraud, cybercrime and data security matters, as well as related civil litigation. He also leads internal investigation and cybercrime-related representations for financial services companies and provides guidance on drafting written information security plans and incident response plans for investment advisers. Michael spent six years serving in the U.S. Attorney's Office for the Eastern District of New York, where he investigated and prosecuted cases in the Criminal Division and the Business and Securities Fraud Section involving securities fraud, investment adviser fraud, bank fraud, cybercrime, intellectual property crimes, tax fraud, money laundering, health care fraud, false claims act cases, Federal Food, Drug, and Cosmetic Act violations, and other regulatory offenses. He also served as the co-coordinator for Computer Hacking and Intellectual Property crimes. Michael clerked for the Honorable Samuel A. Alito, Jr. of the U.S. Court of Appeals for the Third Circuit (now a Justice of the U.S. Supreme Court), and the Honorable Milton Pollack of the U.S. District Court for the Southern District of New York.

The Legal 500 United States has recognized Michael as a leading lawyer in his field. A frequent speaker and writer, he most recently co-authored "Federal Banking Agencies Propose New Cybersecurity Regulations" and "NYDFS Proposes Detailed and Sweeping Cybersecurity Regulation for Financial Services Companies," both published in *Harvard Law School Forum on Corporate Governance and Financial Regulation*, and "Securities, Futures Regulators Increase Scrutiny, Expectations on Cybersecurity" in *Bloomberg Brief – Financial Regulation*. His speaking topics cover issues including cybersecurity and data protection, the convergence of information and physical security of health care information, cyber readiness for financial institutions and managing information security and IT business architecture for hedge funds. He also presents "Treatises and Complex Litigation" as an annual guest lecturer at Yale Law.

Michael earned his J.D. from Yale Law School, where he was the John M. Olin Fellow of the Center for Studies in Law, Economics and Public Policy. He earned his B.A., *with distinction*, from Yale University.

Regulatory Focus: AML, Cybersecurity and FCPA

I. AML

A. Several statutes and regulations aim to prevent the flow of proceeds from crimes and the financing of terrorist operations:

1. The Money Laundering Control Act ("MLCA"), 18 U.S.C. §§ 1956 and 1957.

2. The Bank Secrecy Act ("BSA") of 1970, 31 U.S.C. §§ 5311 – 5330, as amended, including by the USA Patriot Act of 2001, and the BSA's implementing regulations, 31 C.F.R. Chapter X.

3. Economic sanctions enforced by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC") prohibit U.S. citizens, businesses and financial institutions from engaging in transactions with persons designated on OFAC lists or located in prohibited jurisdictions (for example, individuals and entities on OFAC's Specially Designated Nationals and Blocked Persons List).

4. The Anti-Terrorism Act ("ATA"), 18 U.S.C. § 2333(a), provides for a private right of action for damages to any U.S. national "injured in his or her person, property, or business by reason of an act of international terrorism."

B. Money Laundering

1. Under 18 U.S.C. § 1956, it is a crime to attempt to conduct a transaction that actually involves or is represented to involve (i.e., a sting operation) the proceeds of specified unlawful activity or that is an international transaction, with the purpose of concealing the proceeds, promoting specified unlawful activity or avoiding a transaction reporting requirement. Under 18 U.S.C. § 1957, it is a crime to engage in any transaction involving a financial institution with knowledge that the funds derive from specified unlawful activity. The key term "specified unlawful activity" has an extremely broad definition, incorporating literally hundreds of crimes. Under both sections, the government can prove the requisite intent by showing "willful blindness," such that even if the defendant in fact did not know, it is sufficient that the defendant deliberately avoided learning the necessary facts.

2. Offenses under Sections 1956 and 1957 are punishable by fines up to the greater of $500,000 or twice the value of the transactions and 20 years in prison, or both.[1] The government also has the right to pursue civil fines for those offenses up to the greater of $10,000 or the value of the transactions.[2] It is a separate offense under Section 1956(h), subject to the same penalties, to conspire to commit any offense under 1956 or 1957. Although the language of the civil fine provision does not include 1956(h) — suggesting that a civil fine is not available for a conspiracy that did not amount to an offense — the government has nonetheless sought such civil fines.[3]

C. AML Compliance Programs

1. The BSA requires "financial institutions" to have written, effective AML compliance programs. "Financial institutions" include banks; broker-dealers; any entity required to register under the

[1] *See* 18. U.S.C. §§ 1956-57.

[2] *Id.* § 1956(b).

[3] E.g., *United States v. Lloyds TSB Bank PLC*, 639 F. Supp. 2d 314, 324 (S.D.N.Y. 2009) (government's complaint included 1956(h) as a cause of action but the court dismissed the case for lack of subject matter jurisdiction because the transactions at issue had no connection with the United States).

Commodity Exchange Act ("CEA") (including futures commission merchants ("FCMs"); introducing brokers in commodities ("IB-Cs"); commodity trading advisors ("CTAs"); and commodity pool operators ("CPOs")); mutual funds; operators of credit card systems; money services businesses; insurance companies; casinos; loan or finance companies; and dealers of precious metals, stones and jewels. In 2015, the Financial Crimes Enforcement Network ("FinCEN") issued a proposed regulation that would extend this and other AML requirements to investment advisers registered (or required to register) with the SEC ("RIAs") (the "Proposed Rule").[4] Once the final rule is adopted, RIAs will have six months to comply.

2. The Proposed Rule requires that the AML program be in writing, approved by the RIA's board of directors, and address the "four pillars."[5]

   (a) Establish and implement written policies, procedures and internal controls to ensure ongoing compliance. The AML program must be "reasonably designed to prevent the investment adviser from being used for money laundering or the financing of terrorist activities, and to achieve and monitor compliance with the BSA. Regulators want to see a "risk-based" approach in the design of the program.

   (b) The RIA must designate an individual or committee responsible for implementing and monitoring the operations and internal controls of the program (the "AML officer"), who is "knowledgeable and competent" regarding the regulatory requirements and the RIA's money laundering risks. Although the AML officer need not be dedicated full time to BSA compliance (depending on the RIA's size and type of services), he or she must be an officer of the investment adviser and thus that role cannot be delegated to a third-party administrator.

   (c) The RIA must provide ongoing training for appropriate personnel. The nature, scope and frequency of training would be determined by the employees' responsibilities and the extent to which their functions bring them into contact with the BSA's requirements and possible money laundering. In addition to ensuring that such ongoing training complies with the Proposed Rule (e.g., tailoring training to the audience), the RIA should document its practices related to training so that it is prepared for an SEC examination with respect to compliance with the AML rules.

   (d) The Proposed Rule requires independent testing of the AML program on a "periodic basis," explaining that the frequency of testing will depend upon the RIA's assessment of the risks posed. Such testing, designed to ensure that the program is functioning as intended, may be conducted by a qualified outside party — or by employees of the RIA, provided those employees are not involved in the operation or oversight of the AML program.

   (e) Other financial institutions are required to maintain a customer identification program ("CIP") to collect the name, date of birth (for individuals), address and identification number of each account holder who opens an account and to verify enough of that information to form a reasonable belief that it knows the true identity of the account holder.[6] The CIP does not yet

[4] Firms that rely on exemptions from SEC registration therefore would not be subject to the Proposed Rule, such as venture capital fund advisers under Advisers Act Section 203(l), private fund advisers managing less than $150 million with a place of business in the United States under Section 203(m), family offices relying on Rule 202(a)(11)(G)-1, and CTAs whose business is not predominantly securities-related advice.

[5] Recent enforcement actions demonstrate that deficiencies relating to any of these four AML pillars can result in liability under the BSA. E.g., *Oppenheimer & Co., Inc.*, FinCEN Matter No. 2015-01 (Jan. 27, 2015); *Halcyon Cabot Partners, Ltd.*, FINRA Case No. 2012033877802 (Oct. 6, 2015); *Global Strategic Investments, LLC*, FINRA Case No. 2011025676501 (April 27, 2015); *Cobra Trading, Inc.*, FINRA Case No. 2013035340001 (Feb. 17, 2015).

[6] E.g., 31 C.F.R. § 1020.220.

govern private investment funds and will not apply to RIAs under the Proposed Rule; however, FinCEN and the SEC intend to create CIP rules for RIAs through joint rulemaking.

D. Suspicious Activity Reports ("SARs")

1. Under the Proposed Rule, RIAs would be required to file SARs. The purpose of a SAR is to report suspicious transactions that could suggest criminal activity, particularly money laundering and terrorist financing, but also other criminal activity, such as fraud, to regulators and to law enforcement. Entities must electronically file a SAR with FinCEN using FinCEN's BSA E-Filing system within 30 days of the reporting investment adviser's determination that potentially suspicious activity occurred, but must immediately notify appropriate law enforcement authority by phone about "violations that require immediate attention," such as suspected terrorist financing or ongoing money-laundering schemes.

2. A SAR filing will be required for transactions involving at least $5,000 conducted or attempted by, at or through the RIA where the RIA knows, suspects or has reason to suspect that the transaction: involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; is designed to evade the BSA or its implementing regulations; has no business or apparent lawful purpose or is not the sort of transaction the particular customer would normally be expected to engage in, and the RIA knows of no reasonable explanation for the transaction after examining the available facts; or involves use of the RIA to facilitate criminal activity.

3. FinCEN recently issued guidance interpreting the BSA to require filing a SAR when the financial institution "knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or series of transactions." That includes any attempt to compromise a system containing account numbers, credit card numbers, passwords, online banking credentials, balances or other information that could facilitate transactions. FinCEN further interpreted the $5,000 threshold such that the financial institution must report even an unsuccessful attempt if it "put at risk" at least that amount in transactions it could have facilitated.[7]

4. Although the Proposed Rule would allow RIAs to delegate SAR reporting responsibilities to a third party, the RIA remains ultimately responsible. An RIA and another entity subject to the BSA can jointly file a SAR regarding the same conduct. However, all SARs are confidential — disclosing information that would reveal a SAR's existence can constitute a crime, so careful coordination and planning are necessary to submit a joint SAR.

E. Record Keeping and Travel Rules, and Currency Transaction Reports ("CTRs")

1. Financial institutions subject to the BSA (including RIAs if the Proposed Rule is adopted) must record particular information for transmittals of funds in excess of $3,000, including the name and address of the transmittor, the payment instructions received from the transmittor, and information provided about the recipient, and then maintain such records for five years in a manner that is accessible within a reasonable period of time and retrievable by the transmittor's financial institution by reference to the name of the transmittor.

2. Financial institutions must also ensure that the name, address and account number of the transmittor and information provided about the recipient "travels" with the transmittal of funds in

[7] FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime at 4 (Oct. 25, 2016).

excess of $3,000 to the next financial institution in the payment chain, unless the interested party in the transaction is a financial institution such as a bank, broker, dealer or mutual fund.

3. Financial institutions must create and retain records for extensions of credit and cross-border transfers of funds, currency, monetary instruments, checks and investment securities that exceed $10,000. Financial institutions must file CTRs for transactions involving more than $10,000 in currency. When the Proposed Rule goes into effect, RIAs will already be well-equipped to file CTRs as they already file Form 8300 in that circumstance and often do not deal in cash at all.

F. USA Patriot Act Section 314

1. Section 314(a) mandates that financial institutions (including RIAs under the Proposed Rule) search their records upon a law enforcement request made through FinCEN to determine whether they have maintained an account or conducted a transaction with a person that law enforcement has certified is suspected of engaging in terrorist activity or money laundering and supply identifying information for the account or transaction in question. Such requests must be kept confidential.

2. The Section 314(b) safe harbor permits (and encourages) financial institutions and some related entities to share information for the purpose of identifying and reporting money laundering or terrorist activity, protected from civil liability. To avail itself of the safe harbor, the financial institution must provide advance notice to FinCEN of its intent to share information and comply with the information protection provisions such as those in the GLB Act (discussed in Part II).[8]

G. Recent AML Developments

1. Customer Due Diligence ("CDD") Rule

(a) In 2016, FinCEN adopted the CDD rule as a "fifth pillar" that will apply to banks, broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities.

(b) The CDD rule does not yet govern private investment funds and the Proposed Rule would not require RIAs to comply with the CDD rule. However, the CDD rule does apply to financial institution counterparties of RIAs (e.g., prime brokers) and affects what due diligence demands they may have of RIAs.

(c) Financial institutions must conduct ongoing customer due diligence to identify the human beings who own 25 percent or more or who control each account opened on or after CDD goes into effect March 11, 2018 at the time it is opened, except where the account holder is an ERISA plan, bank, broker, dealer, RIA, registered investment company, state-regulated insurance company or a company with equity securities listed on an exchange. Financial institutions may rely on a certification of the account holder about its beneficial owners unless the financial institution knows something that reasonably calls into question the reliability of that certification. When activity inconsistent with the "customer risk profile" the financial institution developed through its diligence is detected in the account, the financial institution must update its beneficial owner information. Private investment funds and other non-exempt entities must provide their beneficial ownership information to the financial institutions with which they open accounts after the effective date.

[8] The detailed requirements of the safe harbor are set forth in 31 C.F.R. § 1010.540.

2. The Panama Papers

In early 2015, more than 11 million documents belonging to Panamanian law firm Mossack Fonseca were leaked and then investigated by the International Consortium of Investigative Journalists ("ICIJ"). That law firm allegedly facilitated the concealment of funds through offshore companies and large banks assisted by forming shell companies for certain high-net-worth individuals and politicians. While the ICIJ thoroughly reviewed the underlying documents, it has not released them, instead providing a searchable database listing the shell companies and beneficial owners the papers demonstrate. The DOJ, SFO and many other prosecuting agencies around the world have launched investigations into the activity revealed in the Panama Papers.[9]

3. FinCEN Geographic Targeting Orders

(a) In 2016, FinCEN implemented geographic targeting orders ("GTOs") that require title insurance companies to report on real estate transactions in specific geographic areas that are above a specified value and made without bank financing (i.e., all cash purchases) by legal entities, to provide the identity of the beneficial owners (any person who directly or indirectly owns at least 25 percent of the entity); the names, addresses and taxpayer identification numbers of every member of an LLC purchaser; and the identity of the individual who was primarily responsible for representing the purchaser in the transaction. The program arises out of a concern that illicit actors are storing or concealing assets in the form of luxury real estate, while hiding their identities through the use of shell companies.

(b) In January 2016, FinCEN issued GTOs covering property over $3 million in Manhattan and over $1 million in Miami-Dade County. Effective August 2016, FinCEN expanded the program into all boroughs of New York City; Miami-Dade, Broward and Palm Beach Counties; Los Angeles County; San Francisco, San Mateo and Santa Clara Counties; and Bexar County (San Antonio, Texas), specifying monetary thresholds particular to each of those regions.[10]

H. Other jurisdictions also have AML laws. For example, the Cayman Islands has extensive laws and regulations relating to money laundering such as the Proceeds of Crime Law, criminalizing the transfer of funds derived from any foreign activity that would be a crime if committed in the Cayman Islands.

I. Recent Adjustments in OFAC Sanctions Policies

1. Cuba

(a) In January 2016, OFAC and the Department of Commerce's Bureau of Industry and Security ("BIS") amended regulations to permit export and re-export to Cuba of various goods aimed to serve the general people of Cuba but not its state-owned enterprises. Various general licenses permitted greater travel to Cuba for specific purposes.[11]

---

[9] While it appears that the DOJ does not yet have direct access to the Panama Papers themselves, the DOJ has sought to obtain those documents and other information from the ICIJ and law enforcement agencies in Panama have conducted raids of Mossack Fonseca's offices. Even if the documents are not revealed or would not be admissible in evidence, the leads the data provide will lead to ample enforcement activity. Rupert Neate, Panama Papers: US launches criminal inquiry into tax avoidance claims, The Guardian (Apr. 19, 2016), *available at* www.theguardian.com/business/2016/apr/19/panama-papers-us-justice-department-investigation-tax-avoidance.

[10] Press Release, FinCEN, FinCen Expands Reach of Real Estate "Geographic Targeting Orders" Beyond Manhattan and Miami (July 26, 2016), *available at* www.fincen.gov/news/news-releases/fincen-expands-reach-real-estate-geographic-targeting-orders-beyond-manhattan.

[11] The general licenses include 31 C.F.R. §§ 515.545 (transmission of informational materials), 515.562 (official government business), 515.563 (journalistic activity), 515.564 (professional research or professional meetings), 515.565 (educational activities or people-to-people travel), 515.566 (religious activities), 515.567 (public performances and exhibitions), 515.574 ("support for the Cuban people"), 515.575 (humanitarian projects) and 515.576 (activities of private foundations or research or educational institutes).

(b) OFAC also permitted U.S. depository institutions to issue, advise, negotiate, pay or confirm letters of credit, including for financial institutions that are Cuban nationals. In October 2016, OFAC issued a general license authorizing U.S. nationals to make remittances to third-country nationals for travel to, from or within Cuba so long as the traveler would qualify for a travel general license if the traveler were subject to U.S. jurisdiction.[12]

(c) Generally speaking, however, U.S. persons remain forbidden from engaging in transactions with Cuba as a country.

2. Iran

In early 2016, Iran verifiably met its nuclear commitments so the United States and EU lifted various "secondary sanctions" so that non-U.S. persons could engage in certain business activities and transactions with Iranian persons. U.S. persons have general license to import Iranian carpets and certain foods but must still facilitate such transactions via a third-country bank or money service; have general license to establish or alter corporate policies to engage in the newly permitted activities, though U.S. persons cannot have any involvement in day-to-day operations affecting Iran; and may apply for specific license for transactions involving aircraft parts. None of those U.S.-person activities can involve a person on the SDN list, though OFAC removed over 400 persons from the SDN and other sanctions lists. Overall, U.S. persons are prohibited from engaging in transactions with Iran as a country.

3. Russia/Ukraine

(a) Following the Russian annexation of Crimea, Ukraine, OFAC and BIS acted pursuant to Executive Order 13662 to impose a sectoral sanctions regime and adding certain entities to the SDN list, to limit Russia's defense and related materials sector. U.S. persons cannot issue financing with maturity of greater than 30 days to various banks on the Sectoral Sanctions Identifications list ("SSI list"), including Russia's largest bank, Sberbank, and defense conglomerate Rostec; nor financing with maturity of greater than 90 days to various companies in the energy sector. Although U.S. persons cannot hold a direct interest in any of the debt governed by the directives OFAC issued pursuant to Executive Order 13662, a general license permits transactions in derivative products linked to the debt those directives prohibit. Nonetheless, U.S. persons must not invest in the new equity of entities on the SSI list.

(b) BIS expanded export restrictions on its BIS Entity List, under which a specific license is required to export or re-export items subject to the Export Administration Regulations to the listed persons, with a presumption of denial.

(c) The EU issued similar economic and export sanctions.

(d) Sanctions vis-à-vis Russia are likely to remain in flux as the new administration takes power and following confirmed intelligence reports of persons associated with Russia hacking political candidates and parties in an effort to influence the 2016 presidential election.

II. Cybersecurity

Information security is not only a good idea — it's a legal obligation. Federal and state laws impose obligations on businesses, including investment advisers, to keep their data secure. Most of these laws focus

[12] Department of the Treasury, Frequently Asked Questions Related to Cuba (Oct. 14, 2016), *available at* www.treasury.gov/resource-center/sanctions/Programs/Documents/cuba_faqs_new.pdf.

on requiring businesses to take reasonable security measures. While it may take regulators and courts years to clearly define what exactly those measures are, best practices that facilitate compliance can and should be developed and followed now.

A. Regulatory Interest in Cybersecurity

Investment advisers must maintain data security not only because of contractual obligations (e.g., under contracts between the firm and investors or commercial vendors), fiduciary obligations or for practical business reasons (e.g., to protect trade secrets), but also because of federal and state statutes and regulations that require data security.

1. Protection of Personally Identifiable Information ("PII")

(a) Historically, applicable laws have been mostly concerned with protecting the PII of human beings (e.g., social security numbers or home addresses).

(b) At present, 47 states (and Washington, D.C., Puerto Rico, Guam and the Virgin Islands) have PII protection laws. These include all states other than Alabama, New Mexico and South Dakota.[13]

2. The Gramm-Leach-Bliley Act ("GLB Act")[14]

(a) The GLB Act requires financial institutions to protect a broad scope of "nonpublic personal information" about the individuals to whom the institutions provide financial products or services, information protected by the Health Insurance Portability and Accountability Act ("HIPAA") and by the Federal Education Rights and Privacy Act ("FERPA").[15]

(b) The Securities and Exchange Commission (the "SEC") and the Financial Industry Regulatory Authority ("FINRA") enforce two GLB Act regulations:

(i) Section 30 of Regulation S-P:[16] Requires brokers, dealers, investment companies and registered investment advisers to adopt written policies and procedures designed to protect "customer records and information."[17]

(ii) Regulation S-ID, the Identity Theft Red Flags Rules: Requires covered entities to develop and implement a written program to "detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account."[18]

(c) The SEC has brought enforcement cases against firms for violating Regulation S-P by failing to follow or enforce cybersecurity policies and procedures.[19] FINRA has also brought supervision and enforcement actions under Regulations S-P and S-ID against broker-dealers.[20]

[13] The National Conference of State Legislatures provides a list of the relevant laws, *available at* www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[14] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006).

[15] 16 C.F.R. § 313.1 *et seq.*

[16] Securities and Exchange Commission, Final Rule: Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. Part 248, Subpart A.

[17] 17 C.F.R. § 248.30.

[18] 17 C.F.R. § 248.201(d)(1).

3. The 1940 Acts

   Poor cybersecurity could potentially create liability under anti-fraud and fiduciary rules of both the Investment Company Act and the Investment Advisers Act, especially given that negligence, and not intentional wrongdoing, may be sufficient to ground liability under the acts.[21]

4. SEC Office of Compliance Inspections and Examinations ("OCIE")

   (a) In 2014 and 2015, OCIE released Risk Alerts announcing that it would make cybersecurity a focus of its exams in those years. [22] The Risk Alerts made clear that OCIE would not confine its exams to PII but would address cybersecurity risks in general, including "misappropriation of funds, securities, sensitive Firm information, or damage to the Firm's network or data."

   (b) Topics that OCIE addressed in the Risk Alerts included: governance and risk assessment, access rights and controls (including remote access); data loss prevention; vendor management; training; and incident response. Although OCIE did not issue a specific cybersecurity Risk Alert in 2016, evaluating cybersecurity remains a major part of OCIE's exams.[23]

   (c) For example, in 2016, the SEC imposed a $1-million fine on Morgan Stanley Smith Barney LLC where an employee accessed customer information and listed it for sale online over a three-year period. The order noted that Regulation S-P requires every broker-dealer and registered investment adviser to adopt written policies and procedures that "address administrative, technical and physical safeguards reasonably designed to: (1) [e]nsure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[24]

5. SEC Enforcement Action: *R.T. Jones*

   (a) In 2015, investment adviser R.T. Jones consented to entry of a cease-and-desist order and a $75,000 fine relating to poor cybersecurity and a breach of PII. Notably, the breach occurred before OCIE began its "cyber sweeps," and the co-chief of the SEC Enforcement Division's

---

[19] *See*, e.g., Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181 (Sept. 11, 2008), *available at* www.sec.gov/litigation/admin/2008/34-58515.pdf; Exchange Act Release No. 64220, Admin. Proc. File No. 3-14328 (April 7, 2011), *available at* www.sec.gov/litigation/admin/2011/34-64220.pdf; Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631 (Sept. 29, 2009), *available at* www.sec.gov/litigation/admin/2009/34-60733.pdf.

[20] *See*, e.g., FINRA Letter of Acceptance, Waiver and Consent No. 2009019893801 (Nov. 21, 2011); FINRA Letter of Acceptance, Waiver and Consent No. 2010022554701 (April 9, 2012); FINRA Letter of Acceptance, Waiver and Consent No. 2008015299801 (April 9, 2010). All of these letters of acceptance are available at http://disciplinaryactions.finra.org. The SEC Investment Management Division issued guidance that provided more detail on the basic steps the SEC staff expect, observing that "fraudulent activity could result from cyber or data breaches from insiders, such as fund or advisory personnel, and funds and advisers may therefore wish to consider taking appropriate precautions concerning information security." SEC, Division of Investment Management, IM Guidance Update (April 2015), No. 2015-02, "Cybersecurity Guidance."

[21] *See, SEC v. Capital Gains Research Bureau*, 375 U.S. 180 (1963) (holding that a violation of § 206(2) may rest on a finding of simple negligence); *SEC v. Steadman*, 967 F.2d 636, 637 (D.C. Cir. 1992) (noting that a violation of § 206(4) does not require that the defendant acted with scienter).

[22] SEC, OCIE, "OCIE's 2015 Cybersecurity Examination Initiative," Vol. IV, Issue 8 (Sept. 15, 2015); SEC, OCIE, "Risk Alert: OCIE Cybersecurity Initiative," Vol. IV, Issue 2 (April 15, 2014).

[23] Securities and Exchange Commission, OCIE: Examination Priorities for 2016, *available at* www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

[24] *In the Matter of Morgan Stanley Smith Barney LLC*, Securities Exchange Act of 1934 Release No. 78021, Admin. Proc. File No 3-17280 (SEC June 8, 2016) at 2, *available at* www.sec.gov/litigation/admin/2016/34-78021.pdf.

Asset Management Unit acknowledged that there was "no apparent financial harm to clients."[25]

(b) The order stated that "from at least September 2009 through July 2013, R.T. Jones stored sensitive [PII] of clients and others on its third party-hosted web server." The server was attacked in July 2013 by "an unauthorized, unknown intruder, who gained access and copy rights to the data on the server," and as a result "the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, was rendered vulnerable to theft." "Shortly after the breach incident, R.T. Jones provided notice of the breach to all of the individuals whose PII may have been compromised and offered them free identity monitoring through a third-party provider."[26]

(c) The order further stated that "the firm failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule [Regulation S-P]." Specifically, the order stated that R.T. Jones's policies and procedures for protecting its clients' information did not include "conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server or establishing procedures for responding to a cybersecurity incident."[27]

6. The CFTC

(a) The National Futures Association ("NFA"), the self-regulatory organization for the futures industry, with the approval of the Commodity Futures Trading Commission ("CFTC"), issued new standards for its members, which became effective March 1, 2016:

(i) Members are required to implement a written information systems security program, and in doing so to consider standards such as ISACA's Control Objectives for Information and Related Technology ("COBIT"), and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (discussed below).

(ii) Members are required to develop an incident response plan to "provide a framework to manage detected security events or incidents, analyze their potential impact and take appropriate measures to contain and mitigate their threat."

(iii) Each member is also required to provide training for its employees on information security that is tailored to the risks the member faces.[28]

(b) CFTC Commissioner Sharon Bowen mentioned that future regulation may: (1) require each registrant to designate a chief information security officer; (2) require registrants to file annual or quarterly reports on the state of their cybersecurity program; (3) require that registrants report any material cybersecurity event to the CFTC promptly (with an example of reports being made "within minutes of a significant breach"); and (4) require an independent audit or annual penetration testing for all registrants.[29] While some of these proposals are consistent

[25] Press Release, Securities and Exchange Commission, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), *available at* www.sec.gov/news/pressrelease/2015-202.html.

[26] *In the Matter of R.T. Jones Capital Equities Management, Inc.*, Investment Advisers Act of 1940 Release No. 4204, Admin. Proc. File No. 3-16827 (SEC Sept. 22, 2015) at 2-3, *available at* www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[27] *Id.*

[28] National Futures Association, Interpretive Notice, NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 20, 2015), *available at* www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.

[29] Sharon Y. Bowen, Commissioner, CFTC, Keynote Address Before ISDA North America Conference (Sept. 17, 2015).

with current best practices, the reporting of any material event "within minutes" would be a new requirement for fund managers.

7. The European Union

   (a) While the United States enacted the GLB Act and Regulation S-P, the EU enacted the Data Protection Directive.[30] One important consequence of the difference between the U.S. and EU regulations is that affiliated groups of companies can share data of a U.S. customer among each other without individual customer approval, but companies must obtain approval from an EU customer prior to sharing the customer's information with an affiliate or otherwise transferring the data outside the EU. Without a safe harbor or equivalent legal mechanism, any U.S. entity doing business in an EU country through an EU subsidiary would need to obtain customer approval for the EU subsidiary to send EU customer data to its U.S. parent. It would be similarly problematic for a U.S. investment adviser to process EU investor data at a global IT back office located in New York or Connecticut.

   (b) Although the EU implemented a safe harbor that allowed U.S. institutions to transfer data between EU and U.S. affiliates if the U.S. institution self-certified as to its reasonable data security protections, concerns over mass surveillance uncovered by Edward Snowden prompted the EU's highest court to rule the safe harbor invalid.[31] The United States and EU have since reached a new agreement known as the Privacy Shield which allows similar self-certifications on behalf of U.S. entities, provides greater transparency and redress rights for EU citizens, and allows most information to be transferred so long as the EU citizen has not opted out. The EU citizen has to affirmatively opt in, however, to permit the transfer of sensitive information if the information will be disclosed to a third party or used for a purpose other than the purposes for which it was originally collected.[32]

8. Many other state and federal laws may affect the cybersecurity measures your fund is required or encouraged to take. At a minimum, your fund should engage in a risk-based approach to assess the threats and vulnerabilities of your information systems in order to protect not only PII but also other assets important to your business, such as trade secrets or infrastructure critical to your business.

B. Recent Proposals Forecast Expansion of Cybersecurity Regulation

Several regulators have recently announced proposed regulations or rules setting forth detailed cybersecurity obligations for the entities subject to their authority and with little regard for the potential conflicts an entity subject to multiple regulators may face in attempting to comply. What is clear is that cybersecurity is becoming even more of a compliance obligation and that funds can expect scrutiny of their information security systems from multiple regulators.

1. The New York Department of Financial Services ("NYDFS") issued a proposed regulation that would require banks, consumer lenders, money transmitters, insurance companies and certain other financial service providers to formalize their cybersecurity program, restrict access so employees and vendors are permitted to access only the information they need, report breaches to the

[30] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

[31] *Maximillian Schrems v. Data Protection Commissioner* [2015] Case C-362/14, ECLI:EU:C:2015*, available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=410849.

[32] The full text of and commentary on the Privacy Shield is available at www.privacyshield.gov. *See also* European Commission, Fact Sheet: EU-U.S. Privacy Shield (July 2016), *available at* http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

superintendent, destroy no longer needed information but preserve logs and access records, and annually certify compliance.[33] Although the NYDFS does not directly regulate private investment funds, they will likely be affected when the banks it regulates begin to require additional representations and warranties from their counterparties.

2. The Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation ("FDIC") issued an advance notice of proposed rulemaking that aims to protect "those entities that are critical to the functioning of the financial sector" and their service providers. The notice urges a risk-based approach that builds cybersecurity into general governance and risk management structures, inventories the internal and external cyber resources on which its business depends, and set out in writing their incident response plans. The notice would require that entities substantially mitigate the likelihood of disruption of any "sector-critical" systems.[34]

C. Some Best Practices

1. NIST Framework

(a) The National Institute of Standards and Technology ("NIST," a division of the U.S. Commerce Department) Framework[35] provides a thoughtful and flexible approach to cybersecurity developed in collaboration between the government and the private sector.

(b) Several of the regulators mentioned in Section A above have explicitly referred to the NIST Framework as a source of guidance for what "reasonable security measures" mean. For example, the 2014 and 2015 OCIE Risk Alerts called upon registrants to "identify any published cybersecurity risk management process standards" upon which the entity modeled its information security architecture and processes.[36] And the proposed regulations described in Section B above claim to further develop the Framework. While the Framework is not law, it should not be ignored lightly because several regulators have endorsed it.

(c) The Framework is meant to remain flexible enough to accommodate technology and business change so it does not prescribe specific tools or products. The Framework has several parts, the "Core," the "Profile" and the "Implementation Tiers":

(i) "The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors."[37] Its "functions" —

[33] Cybersecurity Requirements for Financial Services Companies (Sept. 13, 2016) (to be codified at 23 NYCRR Part 500), *available at* www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf; Joseph P. Vitale et al., NYDFS Proposed Detailed and Sweeping Cybersecurity Regulation for Financial Services Companies (Sept. 15, 2016), *available at* www.srz.com/images/content/1/4/v2/145023/091516-NYDFS-Proposes-Detailed-and-Sweeping-Cybersecurity-Regula.pdf.

[34] Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards, *available at* www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf; Joseph P. Vitale, et al., Federal Banking Agencies Propose New Cybersecurity Regulations (Oct. 26, 2016), *available at* www.srz.com/images/content/1/4/v2/144958/102416-Federal-Banking-Agencies-Propose-New-Cybersecurity-Regula.pdf.

[35] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) ("the Framework"), *available at* www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. The Framework builds on prior standards such as COBIT and ISO 27001.

[36] *See also,* Luis Aguilar, SEC Commissioner, Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference ("At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."), *available at* www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[37] The Framework, at 1.

identify, protect, detect, respond and recover — trace "the lifecycle of an organization's management of cybersecurity risk"[38] and help it learn from past security incidents.

(ii) The Profile is the "alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a 'Current' Profile (the 'as is' state) with a 'Target' Profile (the 'to be' state). … Profiles can be used to conduct self-assessments and communicate within an organization or between organizations."[39]

For example, a firm with a Profile has something to show its vendors and third parties, making it easier to describe what needs to be protected, and what third parties must do before gaining access. Similarly, a firm can request the third party's Profile.

(iii) Framework Implementation Tiers range from partial (Tier 1) to adaptive (Tier 4), describing: (1) "an increasing degree of rigor and sophistication in cybersecurity risk management practices"; (2) the extent to which cybersecurity risk management is informed by business needs"; and (3) the extent to which cybersecurity risk management is "integrated into an organization's overall risk management practices."[40] Firms select the level that meets the firm's goals and "is feasible to implement."[41]

2. Firm-level Risk Assessments

(a) Firms should maintain a detailed inventory and understanding of their cyber infrastructure, including physical devices, the software platforms and applications used on the network, network resources, connections and data flows (including where customer data is housed).[42]

(b) The SEC is concerned with firms' vulnerability to cybersecurity risks in general, including "misappropriation of funds, securities, … [and] Firm information[.]"[43] Managers should accordingly review existing related policies — such as controls on processing redemption requests and IT safeguards — in a cybersecurity context, discover where the gaps are in the firm's security, and close them.

(c) Every fund manager should be prepared to explain how it designed and maintains its infrastructure, its incident response plan and its training for employees.

(d) Keep in mind that threats are not always brute-force attacks. Phishing is a very common tactic that often involves an email with an urgent or dire call to action that attempts to convince the recipient to click on a link to a site that will download malware onto the recipient's computer. Spoofing is a slightly more sophisticated threat in which the communication appears to come from a person who should not be questioned, such as a boss or an important customer. Fund administration company SS&C Technologies is currently facing a lawsuit seeking eight-figure damages where attackers spirited away $6 million by sending emails from a slightly misspelled

[38] *Id.* at 4.

[39] *Id.* at 5.

[40] *Id.* at 9.

[41] *Id.*

[42] Risk Alert, Question 24, at 6.

[43] *Id.* at 7.

version of the client's domain name. SS&C has moved to dismiss the complaint, arguing that the attackers provided valid client credentials for the wire transfers.[44]

(e) FinCEN recently published a helpful and easily digestible advisory outlining various "e-mail compromise" attacks. Some impersonate corporate executives to direct unauthorized transfers and others aim to take the assets of individuals by targeting or impersonating realtors, lenders or financial institutions. The FinCEN advisory provides several examples and lists red flags that can provide insight in crafting the policies entities need to ensure its employees do not inadvertently fall for these schemes.[45]

3. Cybersecurity Personnel

Firms should have well-defined roles and responsibilities for cybersecurity personnel, and to that end should designate a chief information security officer or the functional equivalent[46] — an employee in charge of information security as distinct from IT operations. Compliance personnel should be familiar with the division of labor in the technology department.

4. Records of Cybersecurity Incidents

(a) Firms should maintain appropriately detailed records relating to cybersecurity incidents, including granular detail on various kinds of cybersecurity events, such as the detection of malware on a firm's devices, or the impairment of a "critical firm web or network resource [due to] a software or hardware malfunction."

(b) Such records are a valuable tool for firms conducting internal investigations. For example, the malware used to misappropriate data can sit on a server for months before it is detected, and thus the investigation of a breach may be aided by examining seemingly unconnected events several months or even years prior. Log records (e.g., web server access logs and secure shell server logs) are often essential and should be protected against being overwritten or deleted.

5. Disaster Recovery

Managers should review their existing disaster recovery plans to ensure that they are up-to-date with firm operations and that they take into account cybersecurity and identity theft prevention policies. Note that Regulation S-P requires a written business continuity plan. A good back-up policy is an essential part of protection against "ransomware" attacks, in which the attacker encrypts all of a firm's data and blackmails the firm in exchange for the decryption key.

D. Bring Your Own Device ("BYOD") Challenges

1. Many firms permit employees to use cell phones and other devices to access firm systems — the same devices they use for personal activities.[47] That trend poses challenges in that devices are

[44] Sam Macdonald, SS&C seeks dismissal of CTA's "unmerited" $20m cyber damages claim, HFM Week (Oct. 5, 2016 7:16am), *available at* https://hfm.global/hfmweek/news/ssc-seeks-dismissal-of-ctas-unmerited-20m-cyber-damages-claim.

[45] FinCEN, Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes (Sept. 6, 2016), *available at* www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

[46] The NYDFS Proposed Regulation discussed above would require NYDFS-regulated entities to name a chief information security officer.

[47] In fact, the National Labor Relations Board has held that firms cannot unduly restrict employees' personal use of business devices, as to do so would chill employees' ability to organize; nor can employers restrict employees' speech about their dissatisfaction with the employer on social media. *See Durham Sch. Servs., L.P.*, 360 N.L.R.B. 85 (2014) (prohibition on sharing information "related to the company or any of its employees or customers" was overbroad and too vague under the NLRA); *Landry's Inc.*, No. 32-CA-118213 (N.L.R.B. A.L.J. June 26, 2014) (policy that urged employees not to post about the company was acceptable, however, because it was not an outright prohibition).

easily lost or stolen, could be accessible to employees' friends and family and give malware a new route into the firm's internal systems. Data traveling wirelessly can be intercepted and cloud storage is unsecure and out of the firm's reach.

2. Firms must proceed cautiously before resorting to surveillance or remote wiping of personal devices to secure business data. The Electronic Communications Privacy Act generally prohibits private entities from wiretapping unless certain conditions are met. The Stored Communications Act makes it a crime to gain surreptitious access to stored communications like email, social media messages and text messages. Employers therefore cannot log into employees' web-based email or social media accounts without consent.[48] The Computer Fraud and Abuse Act prohibits anyone from intentionally accessing a computer without authorization, such as when an employer accesses employees' phones, devices, or accounts without authorization.[49] Twenty-four states have passed so-called "anti-snooping" laws prohibiting employers from demanding passwords to access personal email and social networking sites.[50]

3. To avoid running afoul of these statutory protections, and to protect firm information, firms should: obtain advance authorization to access and wipe the firm's information stored on employee-owned mobile devices; consider mobile management software that can separate firm information from personal information; clearly delineate where work cannot be done (e.g., prohibit firm work on personal email accounts); and craft policies and procedures that ensure that employees do not have an expectation of privacy with respect to firm information on their own devices or personal information transmitted using the firm's technology or stored on the firm's systems.

4. Proprietary and Trade Secret Information

   (a) Information is not a trade secret in a misappropriation case unless the employer has taken "reasonable measures to protect" the information.[51] That evidentiary burden is difficult to meet when the information walks out the door every day in employees' pockets.

   (b) Employees can misappropriate firm information in a variety of ways. To protect firm information, in addition to confidentiality agreements or policies, firms should take technical precautions, including restricting access to trade secret data, disabling transmission of information to portable drives, encrypting information and compartmentalizing information (so that no single individual can misappropriate a particular trade secret).

5. Elements of a BYOD Policy

   (a) Restrictions: A comprehensive BYOD policy should include provisions regarding password protection, encryption of firm data that is stored on the device, lock or wipe after a certain number of unsuccessful access attempts, restrictions on the source of apps (e.g., only Apple or Google), and no friends or family access. If a firm chooses to allow cloud storage for corporate data, it should carefully select an enterprise-grade provider with better encryption and the

[48] *See*, e.g., *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008). *But see*, *Front, Inc. v. Khalil*, 2013 N.Y. Misc. LEXIS 3157 (N.Y. Co. 2013) (firm could properly access content stored directly on firm drives even though it reflected personal email and social media content).

[49] *See*, e.g., *Rajaee v. Design Tech Homes, Ltd.,* 2014 U.S. Dist. LEXIS 159180 (S.D. Tex. 2014).

[50] Specifically, Arkansas, California, Colorado, Connecticut, Delaware, Illinois, Louisiana, Maine, Maryland, Michigan, Missouri, Montana, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington and Wisconsin. There is no New York or federal equivalent yet.

[51] *See MidAmerica Prods., Inc. v. Derke*, 2013 N.Y. Misc. LEXIS 1211 (N.Y. Co. 2013) (holding that customer information sheets were not a trade secret because "plaintiffs did not take any reasonable measures to guard the secrecy" when anyone in the office with access to the computer had access to the data).

ability to monitor and wipe what an employee has stored. Employers should also require immediate reporting of lost or stolen devices, use of mobile management software with remote wiping capabilities and use of strong passwords.

(b) Monitoring: In addition, employers should alert employees that they have no privacy expectation in firm data or material transmitted through firm email; firms should get consent to monitor data that is stored, sent from, or received on the device; and firms should get consent to remotely wipe firm information, including upon termination of employment. Firms should obtain advance consent to inspect the device upon termination to ensure firm data is not stored in the personal areas of the device that mobile management software will not wipe.

(c) Coordination with Other HR Policies: Employers should ensure that BYOD policies do not conflict with other HR policies and specify that any other policies such as EEO, anti-harassment, confidentiality and compliance policies apply to work done on the device.

(d) Record Keeping Obligations: Employers should make sure that they have access to and maintain all information that is subject to record keeping obligations. For example, if text messages relate to recommendations or advice by a registered investment adviser, they are subject to the record keeping obligations under Rule 204-2 of the Investment Advisers Act.[52] Policies should allow for retrieval of employee-owned devices for compliance-related inquiries. It is good practice to maintain separate, work-specific, employer-controlled accounts for employees on any platforms used for communicating with clients, even, e.g., LinkedIn.

E. Third-party Risks: Vendor Management

(a) A vulnerability of a third party with access to the firm's internal systems can quickly become the firm's vulnerability. Such third parties include fund administrators, prime brokers, consultants and commercial vendors. There is not yet a standard Due Diligence Questionnaire ("DDQ") to evaluate the cybersecurity of third parties though the American Institute of Certified Public Accountants has released "Service Organization Control" standards that rate the robustness of an entity's written policies and the technical fortitude of its systems.[53]

(b) In choosing a vendor, investigate its creditworthiness; ask for customer references; review key documents such as the vendor's written information security program, business continuity plan, and incident response plan; ask the vendor which standards it follows; require the vendor to commit to follow firm instructions including litigation and regulatory holds; determine the access its vendors will have to your sensitive information and conduct diligence on them.[54]

F. Data Breaches

1. Incident Response Plan

(a) An Incident Response Plan defines a firm's procedures for reporting and responding to security incidents that may compromise the availability, integrity and confidentiality of its information systems, network resources or data. Such a plan might include:

---

[52] OCIE, Investment Adviser Use of Social Media, National Examination Risk Alert (Jan. 4, 2012), at 2; *see* 17 C.F.R. § 275.204-2.

[53] Am. Inst. of CPAs, Service Organization Controls (SOC) Reports for Service Organizations, *available at* www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganization%27sManagement.aspx.

[54] *See also* Robert R. Kiesel, "Model Cybersecurity Contract Terms and Guidance for Investment Managers to Manage Their Third-Party Vendors," 1 *Cybersecurity Law Report*, No. 6 (June 17, 2015), *available at* www.srz.com/resources/model-cybersecurity-contract-terms-and-guidance-for-investment.html.

(i) Developing and testing procedures, and training personnel;[55]

(ii) Assigning responsibility for managing the response to the incident, determining the scope of the incident, and notifying the security incident response team;

(iii) Assessing the risk of continued operations and preventing further loss or damage;

(iv) Determining the cause of a security incident and plugging the holes;

(v) Returning impacted data and services to full operational status; and

(vi) Identifying lessons that make future responses more effective.

(b) Develop responses to the most likely attacks (e.g., phishing and insider threats). Do not just think of the dramatic incidents. A security incident could be a breach by an outside attacker, but it also includes events like the loss of laptops, mobile phones or RSA keys.[56]

(c) Assemble a team that includes various parts of the firm such as tech security, tech operations, PR, audit and legal. Specify points of contact for each department, allocate responsibilities and distribute the list in a way that it can be accessed in an emergency.

(d) Test the response plan — regularly, not just when it is first developed. Update it regularly, especially when significant change occurs, such as switching to a new off-site data center, or implementing a major piece of software — and after every significant incident.

2. Insurance

The market for cyber risk insurance coverage is growing and more financial services entities, including investment advisers, are considering purchasing coverage to mitigate losses associated with data breaches.

(a) Crime Policies and Fidelity Bonds: May cover theft of funds or tangible property such as losses due to computer theft, forgery or electronic fraud but typically do not cover against loss due to stolen data, unauthorized disclosure of information, or system losses due to a virus or other electronic attack.

(b) General Liability Policies: Typically provide coverage bodily injury or property damage caused by an occurrence and do not typically extend to data breach loss.[57]

(c) Cyber Risk Insurance Policies

(i) To apply for cyber risk insurance, an investment manager will need to fill out a fairly extensive application that describes, among other things, the type of confidential records maintained, network and computer systems, security controls, and internal information

[55] Training employees is critical because many security incidents are the result of employee error or misconduct. The consequences of comingling personal and business data and functions on one device are not intuitive to employees. Many problems are not caused by disgruntled employees acting intentionally. Training will go a long way toward mitigating that risk.

[56] One helpful resource is NIST's Computer Security Incident Handling Guide, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Paul Cichonski et al., Computer Security Incident Handling Guide, Special Publication 800-61, Revision 2 (August 2012).

[57] *Zurich Am. Ins. v. Sony*, 2014 WL 3253541 (N.Y. County Feb. 24, 2014) (third party hack of the PlayStation did not constitute a "publication" by Sony and was not covered); *Recall Total Information Mgtmt., Inc. v. Fed. Ins. Co.*, 317 Conn. 46 (Conn. 2015) (loss of computer tapes containing PII was not a "publication" of the information stored on the tapes).

security policies and procedures. The insurer's underwriting and loss control professionals can provide valuable feedback about the manager's information security profile. Cyber risk policies are not yet standardized, so careful attention must be paid to how a particular policy defines the key terms.

(ii) Policies should cover claims by third parties: customers, investors, business partners and regulators. Such claims may be based on damages arising from unauthorized disclosure of personal and financial data, failure to detect and prevent a data breach, and destruction of critical business records. Third-party claims may also include breach of the insured's own written privacy policy or applicable privacy laws and regulations. Some policies also provide coverage for third-party claims for libel, slander, defamation, copyright infringement, invasion of privacy or other claims based on material published on a website or social media space.

(iii) Coverage should include defense costs. News of a data breach are often followed by a purported class action lawsuit seeking damages on behalf of customers. Even if unsuccessful, defense costs for such suits can be significant.

(iv) First-party claims include claims for costs incurred to investigate and respond to data breach incidents. Covered costs should include items such as data restoration costs, forensic analysis of the scope and cause of the breach, legal analysis of reporting and notification obligations, privacy notification services (including credit monitoring), and crisis management expenses, and possibly also business interruption losses and expenses, cyber extortion response costs, and regulatory fines and penalties.

(d) Cyber risk policies typically contain a lengthy list of exclusions, but most simply exclude losses covered by traditional insurance. Other exclusions apply to fraud, intentional illegal conduct or known existing breaches.

3. Reporting

(a) When to report a data breach (and what to report about it) is very fact-specific and depends on applicable state and federal law. Factors that matter include the nature of the data (e.g., whether it was PII), the residence and number of individuals whose information has been compromised, and whether the data was encrypted. Many state laws require that persons whose PII was affected be notified within a reasonable time, but allow postponing that notification in order to cooperate with law enforcement.[58]

(b) While there is often no obligation to report a security breach to the SEC or to prepare any particular document, an internal breach report and documentation may be useful in demonstrating the firm's efforts to address information security concerns.

(c) The firm's investigation and breach report are unlikely to be protected by attorney client privilege or work product. Having a lawyer conduct and direct the investigation, however, can make it more likely that a court will protect the communications made for the purpose of legal advice that occurred during the investigation.

(d) Document as much as possible — actions that are performed by IT, conversations with users and system owners regarding the incident, etc. The point is to know what happened when,

[58] *See*, e.g., Cal. Civ. Code § 1798.82(c); Conn. Gen. Stat. Ann. § 36a-701b(d); Fla. Stat. Ann. § 817.5681(3); Mass. Gen. Laws Ann. Ch. 93H, § 4; N.Y. Gen. Bus. Law § 899-aa(4); and Tex. Bus. & Com. Code Ann. § 521.053(d).

and what the decision-making process was. This information may help a firm to improve its future responses and help protect the firm from second-guessing by litigants. It allows the firm to show that the ultimate solution wasn't the only possible solution, and that the interim theories were reasonable. But to the extent possible, preserve evidence in a way that doesn't alert the suspected culprit. For example, do not assume that you should turn off computers — that will result in loss of volatile memory. Consult law enforcement and your tech and security team before you disconnect from the Internet.

4. Communicating and Working with Law Enforcement

   (a) On the one hand, getting law enforcement involved diminishes the firm's control; criminal cases often (but not always) put related civil suits on hold.[59] On the other hand, reaching out to law enforcement means the firm and law enforcement come into contact on the firm's terms; the Secret Service or FBI may ultimately reach out to the firm anyway if PII was affected. And law enforcement has tools private firms do not (e.g., search warrants, international law enforcement contacts).

   (b) Get outside counsel involved in dealings with law enforcement. And always speak accurately to investigators; though the firm may have to discuss aspects of a hack it has seen but doesn't understand. Consider personal relationships your firm or outside counsel have that may improve the responsiveness of or facilitate communication with law enforcement.

III. FCPA

A. The Foreign Corrupt Practices Act ("FCPA") has two prongs:

1. Anti-bribery provisions prohibit "offering to pay, paying, promising to pay, or authorizing the payment of money or anything of value (tangible or intangible) to a foreign official in order to influence any act or decision of the foreign official in his or her official capacity or to secure any other improper advantage in order to obtain or retain business."[60]

   Apply to bribes paid directly and bribes paid indirectly through third-party intermediaries (e.g., agents, placement agents, sub-agents, consultants, representatives, distributors, resellers, introducers/finders, joint venture partners, brokers, contractors, lawyers, accountants, lobbyists).

2. Accounting provisions require issuers to maintain accurate books and records, and establish a system of internal controls.

   (a) Apply only to issuers (but an issuer's books and records include those of its consolidated subsidiaries and affiliates under its control, including foreign subsidiaries and joint venture partners).

   (b) Do not apply merely because a fund is registered with the SEC, so they are usually not an issue for private investment funds. However, they do apply to portfolio companies that are publicly traded, whether in equity or debt markets.

---

[59] *See* Milton Pollack, *Parallel Civil and Criminal Proceedings*, 129 F.R.D. 201 (S.D.N.Y. 1989); *Parker v. Dawson*, No. 06-CV-6191 JFB WDW, 2007 WL 2462677 (E.D.N.Y. Aug. 27, 2007); *S.E.C. v. Boock*, No. 09 CIV. 8261 (DLC), 2010 WL 2398918 (S.D.N.Y. June 15, 2010); *but see S.E.C. v. Saad*, 384 F. Supp. 2d 692 (S.D.N.Y. 2005) (Rakoff, J.).

[60] While the FCPA only prohibits the bribery of foreign officials, bribery in the private sector may violate other laws, such as: the Travel Act (18 U.S.C. § 1952), the U.S. mail and wire fraud statutes (18 U.S.C. §§ 1341, 1343, 1346), commercial bribery laws, the United Nations Convention Against Corruption (Dec. 11, 2003, 43 I.L.M. 37), among others. Other countries and international orgnizations also have tough anti-bribery laws, such as the Cayman Islands; the United Kingdom; the EU; OAS; World Bank; IMF; OECD Convention on Combating Bribery of Foreign Officials in International Business Transactions.

B. The DOJ and SEC enforce the FCPA; penalties are harsh.

1. Criminal penalties for the anti-bribery provisions: Corporate fine up to $2 million for each violation. Individuals (officers, directors, employees, agents, etc.) can be fined up to $250,000 and imprisoned up to five years for each violation.[61] Fines can also be up to twice the profit gained from the illegal activity or twice the loss resulting from the illegal activity.

2. Criminal penalties for violating the accounting provisions: corporate fine up to $25 million and individuals up to $5 million and/or 20 years in prison.

3. Civil penalties for violating the anti-bribery provisions may include DOJ and/or SEC obtaining injunctive relief and fines up to $10,000 for each violation ($16,000 adjusted for inflation).

4. Civil penalties for violating the accounting provisions may include hefty fines imposed by the SEC or disgorgement of illegal profits.

5. Other adverse consequences include forfeiture of assets, suspension or disbarment from the securities industry or from contracting with the federal government, cross-debarment by multilateral development banks, the suspension or revocation of certain export privileges, shareholder derivative and class action lawsuits, plus other collateral consequences.

6. Rewards and protections are available under whistleblower provisions of the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Act of 2010. The SEC received more than 4,000 whistleblower tips in FY2016, of which 238, or 5.6 percent, involved FCPA allegations.

C. Anti-bribery provisions make it illegal for an "issuer," a "domestic concern" or any "other" person to make corrupt payments, directly or indirectly, to a foreign government official in order to obtain, retain or direct business. 15 U.S.C. §§ 78dd-1 to -3.

1. "Issuer" is any entity with a class of securities registered under the Securities Exchange Act of 1934, including foreign companies with U.S. ADRs.

2. "Domestic concern" means U.S. citizens, nationals and residents as well as companies that have their principal place of business in the United States or are organized under U.S. law.

3. "Other person" means a non-U.S. person, who may be liable if they commit any act in furtherance of an unlawful payment while in the territory of the United States ("territorial jurisdiction"), including (according to the DOJ) "causing" an act in the United States, directly or through agents.

4. Other jurisdictions also have anti-bribery laws, such as the Cayman Islands Anti-Corruption Law. The U.K. Bribery Act, for example, applies to conduct on or after July 1, 2011 by persons subject to the authority of the U.K. Serious Frauds Office ("SFO"). In the few cases under this recent law, penalties are severe.[62]

5. For example, in early 2016, a U.K. construction company was sentenced and ordered to pay £2.25 million after it was convicted under a provision that makes a corporation liable for an "associated person's" act of bribery where a subsidiary made payments (perhaps without the parent's knowledge) to secure a contract in Abu Dhabi. The sentencing judge stated that "The whole point

[61] Fines on individuals cannot be paid by the corporation. 15 U.S.C. § 78dd-2(g)(3).

[62] *See generally* Serious Frauds Office, The Bribery Act 2010 Guidance (Mar. 2011), *available at* www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

of section 7 is to impose a duty on those running such companies throughout the world properly to supervise them."[63]

6. Nonetheless, bribery including "facilitation payments" to obtain or speed up a legally required act were illegal before the U.K. Bribery Act. For example, a small family-run printing company and two of its officers were convicted and fined for corrupt payments both pre- and post-2011 under the Prevention of Corruption Act of 1906.[64]

D. Certain persons can be held liable even though they are not directly involved in the violations:

1. U.S. parents may be held liable for acts of foreign subsidiaries if they participated in or directed the illegal activity, or, under agency principles, if the requisite degree of control exists over the subsidiary's actions.

2. Related persons (i.e., officers, directors, employees or agents of a U.S. issuer or domestic concern or a covered non-U.S. company, or any stockholder acting on their behalf).

3. Under the "control person" theory of liability of § 15 of the Securities Act of 1933 (15 U.S.C. § 77o) and § 20(a) of the Securities Exchange Act of 1934 (15 U.S.C. § 78t(a)), the SEC can impose liability for a securities law violation not only on the person who actually committed the violation but also on an entity or individual that "controls" the violator (directly or indirectly, via stock ownership, agency, or otherwise).[65] Control person liability creates potential exposure for investment funds and their personnel to the extent they exercise control over a portfolio company that is a U.S. issuer by virtue of ownership interest, board representation, and/or involvement in management and financial reporting. For example, a private investment fund that controlled a U.S. issuer that engaged in FCPA violations could face liability under this theory.

E. Elements of an FCPA Violation

1. Payment or offer of money or "anything of value" (no monetary threshold). An offer, promise or authorization of a payment is enough to violate the FCPA, even if no payment has yet been made.

2. Prohibited Recipient

(a) "Foreign official" (i.e., "[a]ny officer or employee of a foreign government or any department, agency or instrumentality thereof, or any person acting in an official capacity for or on behalf of any such government or department, agency or instrumentality"). According to the DOJ/SEC, the instrumentality prong includes employees of state-owned entities or state-controlled entities ("SOEs"), even those SOEs are engaged in commercial activities.[66]

---

[63] Press Release, Serious Frauds Office, Sweett Group PLC sentenced and ordered to pay £2.25 million after Bribery Act conviction (Feb. 19, 2016), *available at* www.sfo.gov.uk/2016/02/19/sweett-group-plc-sentenced-and-ordered-to-pay-2-3-million-after-bribery-act-conviction.

[64] Press Release, Serious Fraud Office, UK printing company and two men found guilty in corruption trial (Dec. 22, 2014), *available at* www.sfo.gov.uk/2014/12/22/uk-printing-company-two-men-found-guilty-corruption-trial; David Connett, Landmark corruption fine levied against Smith and Ouzman, Independent (Jan. 8, 2016), *available at* www.independent.co.uk/news/business/news/landmark-corruption-fine-levied-against-smith-and-ouzman-a6803526.html.

[65] E.g., *SEC v. Nature's Sunshine Products, Inc., Douglas Faggioli and Craig D. Huff*, Case No. 09CV672 (D. Utah, Filed July 31, 2009) (the SEC charged two top executives of a U.S. issuer, in their capacity as control persons, with books and records and internal control violations — the SEC's theory was that the CEO and CFO failed to adequately supervise Nature's Sunshine personnel).

[66] According to the DOJ/SEC, whether a particular entity constitutes an "instrumentality" under the FCPA requires a fact-specific analysis of an entity's ownership, control, status and function. A non-dispositive and non-exclusive list of factors to consider includes: "(1) the foreign state's extent of ownership of the entity; (2) the foreign state's degree of control over the entity (including whether key officers and directors of the entity are, or are appointed by, government officials); (3) the foreign state's characterization of the entity and its employees; (4) the circumstances surrounding the entity's creation; (5) the purpose of the entity's activities; (6) the entity's obligations and privileges under the foreign state's law; (7) the exclusive or controlling power vested in the entity to administer its designated functions; (8) the level of financial

(b) Officials of a "public international organization" (e.g., UN, World Bank).

(c) Foreign political parties, their officials and candidates for foreign political office.

(d) Any person acting as a conduit for payments to any of the above.

3. Corrupt intent, meaning the payment must be for the purpose of influencing any act or decision of a foreign official in his or her official capacity; inducing the foreign official to do or omit to do any act in violation of the lawful duty of such official; securing any improper advantage; or inducing the foreign official to use his or her influence with a foreign government or instrumentality to affect or influence any act or decision of such government or instrumentality.

4. Business Purpose Requirement: Payment must be made for the purpose of assisting the violating party in obtaining or retaining business for or with, or directing business to, any person. That business does not need to be with a foreign government or foreign government instrumentality.

5. Jurisdiction

(a) U.S. issuers, U.S. companies and U.S. individuals liable for prohibited acts committed anywhere in the world, regardless if there is a nexus to the United States.

(b) Non-U.S. persons liable (as noted above) for prohibited acts committed while in the territory of the United States ("territorial jurisdiction"), including (according to the DOJ) "causing" an act in the United States.

F. Enforcement is increasing.

1. The DOJ and the SEC have dramatically increased enforcement efforts in recent years. While only four fines in the FCPA's first 25 years exceeded $1 million, eight- and nine-digit fines are common today. The largest settlement was for $800 million by Siemens.

2. Brazilian construction company Odebrecht and its subsidiary Baskem S.A. pleaded guilty and agreed to pay a total of $3.5 billion to the DOJ, the SEC, and Brazilian and Swiss authorities in connection with millions of dollars of corrupt payments over the span of eight years to influence the state-owned energy company Petrobras. The actual amount it must pay will be determined at sentencing in April.[67]

3. Israeli pharmaceutical Teva pleaded guilty and agreed to pay $519 million to the DOJ and the SEC in connection with alleged corrupt payments in Russia, Ukraine and Mexico. The complaint charged that Teva lacked international controls necessary to prevent and detect the payments, which had been classified as payments to distributors. The sum to be paid to the SEC is $236 million in

support by the foreign state (including subsidies, special tax treatment, government-mandated fees and loans); (9) the entity's provision of services to the jurisdiction's residents; (10) whether the governmental end or purpose sought to be achieved is expressed in the policies of the foreign government; and (11) the general perception that the entity is performing official or governmental functions." While the DOJ/SEC have provided guidance that "an entity is unlikely to qualify as an instrumentality if a government does not own or control a majority of its shares," DOJ/SEC enforcement actions have, in limited circumstances, involved foreign officials employed by SOE in which a foreign government has less than 50 percent ownership (i.e., only where the foreign government has "substantial control" over the SOE at issue).

[67] Richard L. Cassin, DOJ and SEC take small slice of Odebrecht-Braskem $3.5 billion global settlement, FCPA Blog (Dec. 21, 2016 1:18 pm), *available at* www.fcpablog.com/blog/2016/12/21/doj-and-sec-take-small-slice-of-odebrecht-braskem-35-billion.html.

disgorgement, based on the $214 million in profit the SEC alleged Teva gained through regulatory approvals illicitly obtained with the payments.[68]

4. As in other areas, the DOJ continues to express its interest in pursuing individuals and its intent to hold them criminally liable for corporate misdeeds. Indeed, the government's focus on individual liability in criminal cases was publicly announced in September 2015 when the DOJ issued a memorandum written by Deputy Attorney General Sally Quillan Yates entitled "Individual Accountability for Corporate Wrongdoing."[69] The memorandum trumpeted the government's intention to prosecute more individuals generally in white-collar cases. Most significantly, the memorandum requires that companies, funds and other entities identify to the government the individual executives, leaders, managers and employees who many have engaged in wrongdoing.

5. The impact of the Yates Memorandum on FCPA enforcement is still being quantified. 78 percent of individuals charged with FCPA criminal offenses since 2000 were charged in 2008 or later.[70] Recently, five individuals including the owner of several U.S.-based energy companies pleaded guilty to FCPA and other charges for paying bribes to the state-owned Venezuelan energy company and then laundering bribes through the United States.[71]

6. It is too early to say what the new administration holds, but in the months since the election, the Obama administration DOJ has issued a spate of subpoenas to gather documents and other evidence.[72]

G. Ways to Mitigate FCPA Risk

1. Fund Level

(a) Commitment from senior management ("tone from the top" against corruption).

(b) An effective code of conduct with written policies and procedures that are periodically updated (should address: gifts and entertainment expenses, retention of and dealings with agents/third-party intermediaries, facilitation payments, political and charitable contributions).

(c) Designation of an FCPA compliance officer with: (a) direct reporting to and oversight by senior management; (b) autonomy in decision-making; and (c) adequate resources.

(d) A risk-based approach tailored to the organization's specific needs and challenges (each fund's compliance program should be commensurate with the nature and extent of its interaction with foreign government officials).

---

[68] Press Release, SEC, Teva Pharmaceutical Paying $519 Million to Settle FCPA Charges (Dec. 22, 2016), *available at* www.sec.gov/news/pressrelease/2016-277.html.

[69] Memorandum, Salley Quillan Yates, Deputy Attorney General, Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), available at www.justice.gov/dag/file/769036/download.

[70] *See,* DOJ, FCPA Enforcement Actions (Nov. 23, 2016), *available at* www.justice.gov/criminal-fraud/chronological-list.

[71] Press Release, DOJ, Miami Businessman Pleads Guilty to Foreign Bribery and Fraud Charges in Connection with Venezuela Bribery Scheme (Mar. 23, 2016), *available at* www.justice.gov/opa/pr/miami-businessman-pleads-guilty-foreign-bribery-and-fraud-charges-connection-venezuela.

[72] For example, back in 2012, Donald Trump criticized the FCPA as a hindrance to the competitiveness of U.S. businesses' foreign operations in countries like Mexico and China when asked about the investigations into Wal-Mart and its affiliates for alleged improper payments. Mike Koehler, Donald Trump: The FCPA Is a "Horrible Law and It Should Be Changed," FCPA Professor (Aug. 6, 2015), *available at* http://fcpaprofessor.com/donald-trump-the-fcpa-is-a-horrible-law-and-it-should-be-changed.

(e) Training and certifications for all directors, officers, relevant employees, and, where appropriate, agents and business partners.

(f) Clear incentives (i.e., positive measures to drive complaint behavior and negative disciplinary measures to deter unethical/unlawful behavior).

(g) Third-party due diligence.

(h) Confidential reporting and internal investigations.

(i) Continuous improvement via periodic testing and review.

2. Portfolio Investment Level

(a) Risk assessment (key factors include: extent of the company's interaction with foreign governments; use of agents/third-party intermediaries; operating in high-risk jurisdictions).

(b) Review of target's FCPA/anti-bribery compliance program (if it has one).

(c) Examination of agent/consultant relationships (vetting third-party intermediaries via due diligence, approval requirements, documentation).

(d) Background checks on principals.

(e) Questions regarding any FCPA/anti-bribery issues, investigations, etc.

(f) FCPA contractual representations and warranties by third-party intermediaries, including full compliance (no materiality threshold), no financial interest on part of government official and termination rights.

3. Ongoing FCPA compliance for portfolio companies, beginning with establishing a compliance program if one doesn't exist and then ensuring that the program has elements appropriate for the nature of business (e.g., written policies and procedures, FCPA compliance officer, training of employees, employee certifications, due diligence on third-party intermediaries, periodic testing).

4. FCPA Opinion Procedure

Though infrequently used, a party can request a DOJ opinion as to whether certain prospective conduct, such as proposed business ventures involving foreign officials, violates the FCPA. DOJ reviews and must issue an opinion within 30 days after a request is deemed complete. Some of these opinions have addressed the extent of an acquirer's liability for the target's FCPA violations.[73]

[73] Opinion Procedure Release 2003-01 (A U.S. Issuer [Acquirer] sought to purchase the stock of Company A, a U.S. company with domestic and foreign subsidiaries [Target]). During due diligence, Acquirer discovered payments made by Target to individuals employed by foreign state-owned entities. Both companies commenced parallel investigations of Target's activities around the world and disclosed the findings to the government. Pre-acquisition, Acquirer encouraged Target to undertake remedial measures and Acquirer promised DOJ it would implement numerous post-acquisition measures after becoming the owner of Target. DOJ stated that it did not intend to take any enforcement action against the Acquirer for the pre-acquisition conduct of the Target.

Opinion Procedure Release 2004-02 (An Investment Group [Acquirer] sought to acquire certain companies and assets from ABB Ltd. [Target] relating to its upstream oil, gas and petrochemical business). Prior to acquisition, Acquirer and Target agreed to conduct an extensive FCPA compliance review (involving a five-year look-back period, several forensic accountants, 115 lawyers billing over 44,700 man-hours, document review of millions of pages, 165 interviews of employees and agents, visits to 21 countries, 100 staff members, 22 analytical reports and everything was shared with the government). DOJ stated that it did not intend to take any enforcement action against the Acquirer or the recently-acquired Target entities for pre-acquisition conduct.

5. FCPA Liability in the Context of Mergers and Acquisitions[74]

   (a) When a company merges with or acquires another company, the successor company assumes the liabilities of the predecessor company, including FCPA violations, regardless of whether it knows about them.

   (b) According to *A Resource Guide to the FCPA*, a 2012 publication by the DOJ and SEC, those law enforcement agencies have only taken action against successor companies in limited circumstances — generally, in cases involving egregious and sustained violations or where the successor company directly participated in the violations or failed to stop the misconduct from continuing after the acquisition.

   (c) The government expects acquiring companies to conduct risk-based FCPA due diligence on prospective targets and to take appropriate steps if an actual or potential violation is identified in the course of due diligence.

   (d) According to the guide, the DOJ and SEC encourage companies engaging in mergers and acquisitions to take the following actions and "will give meaningful credit to companies who undertake these actions, and, in appropriate circumstances, … may consequently decline to bring enforcement actions."

      (i) Conduct thorough risk-based FCPA and anti-corruption due diligence.

      (ii) Ensure that the acquiring company's code of conduct and compliance policies/procedures apply as quickly as possible to newly acquired businesses or merged entities.

      (iii) Train the directors, officers and employees of newly acquired businesses or merged entities and, when appropriate, train agents and business partners.

      (iv) Conduct an FCPA-specific audit of all newly acquired or merged businesses as quickly as practicable.

      (v) Promptly disclose any corrupt payments that are discovered.

Opinion Procedure Release 2008-02 (A U.S. Issuer, Halliburton Company [Acquirer] bid to acquire the entire share capital of an oil and gas services company that was based in the United Kingdom and traded on the London Stock Exchange [Target]). Because of particular restrictions in U.K. law regarding the bidding process for a public company, Acquirer had insufficient time and inadequate access to information to perform robust pre-acquisition due diligence. Thus, Acquirer sought an opinion from DOJ and submitted a detailed, post-closing plan with strict deadlines for post-acquisition due diligence and remediation related to Target. DOJ stated that it did not intend to take any enforcement action against the Acquirer for: (1) acquisition of the Target, reasoning that the funds contributed as part of this corporate combination transaction could not be considered a "payment" that is "in furtherance of" a bribe given that the Target was publicly listed on a major exchange with a majority of its shares held by large, institutional investors; (2) any pre-acquisition conduct by the Target disclosed to the DOJ during the 180-day period following the closing; and (3) any post-acquisition violations committed by the Target during the 180-day period after closing, provided that the Acquirer disclosed and remediated any illicit conduct.

[74] *See also,* Gary Stein & Jared Wong, FCPA Due Diligence in Mergers and Acquisitions (Lexis/Nexis 2016).

Disclaimer

This information and any presentation accompanying it (the "Content") has been prepared by Schulte Roth & Zabel LLP ("SRZ") for general informational purposes only. It is not intended as and should not be regarded or relied upon as legal advice or opinion, or as a substitute for the advice of counsel. You should not rely on, take any action or fail to take any action based upon the Content.

As between SRZ and you, SRZ at all times owns and retains all right, title and interest in and to the Content. You may only use and copy the Content, or portions of the Content, for your personal, non-commercial use, provided that you place all copyright and any other notices applicable to such Content in a form and place that you believe complies with the requirements of the United States copyright and all other applicable law. Except as granted in the foregoing limited license with respect to the Content, you may not otherwise use, make available or disclose the Content, or portions of the Content, or mention SRZ in connection with the Content, or portions of the Content, in any review, report, public announcement, transmission, presentation, distribution, republication or other similar communication, whether in whole or in part, without the express prior written consent of SRZ in each instance.

This information or your use or reliance upon the Content does not establish a lawyer-client relationship between you and SRZ. If you would like more information or specific advice on matters of interest to you, please contact us directly.

Schulte Roth&Zabel
New York | Washington DC | London
www.srz.com