2015 Year-End Cross-Border Government Investigations and Regulatory Enforcement Review

BakerHostetler

Table of Contents

Globalization has connected people, companies, and products across national borders more than ever. Goods and services developed in one part of the world are readily available in other parts of the world and technology is increasingly and seamlessly connecting markets globally. But as globalization has created a true international marketplace, regulators and law enforcement agencies have increasingly extended their reach beyond national boundaries to police the global arena. The U.S. government in particular has aggressively sought to regulate and enforce U.S. laws against foreign nationals and companies, even in circumstances where a substantial portion of the scrutinized conduct occurs outside U.S. jurisdiction. Foreign regulators are similarly ratcheting up enforcement efforts against U.S. individuals and entities. As the U.S. and other countries seek to regulate the same individuals, entities, and conduct, in increasingly similar ways, parallel international investigations and enforcement have been on the rise.

Our increasingly global regulatory and enforcement environment presents unique challenges to companies that operate trans-nationally. Companies with global reach now face a web of overlapping domestic and foreign regulatory requirements. Companies must now also frequently defend against investigations and proceedings commenced by multiple regulators across multiple jurisdictions. This environment also presents unique difficulties for defending against cross-border investigations and enforcement, as applicable laws concerning data privacy, labor and employment, and the attorney-client privilege, among other areas, vary by jurisdiction and need to be reconciled.

The BakerHostetler *2015 Year-End Cross-Border Government Investigations and Regulatory Enforcement Review* focuses on the key developments and trends in cross-border investigations and government enforcement actions that emerged over the course of 2015. In this issue, you will find highlights and analysis of important cross-border legislation, regulation, and enforcement actions over the past year in the areas of securities fraud, accounting fraud, anti-money laundering, racketeering, and trade sanctions. The report also covers the foreign expansion of U.S. whistleblower programs in 2015, as well as areas of common focus by regulators in different jurisdictions and the parallel development of tools used to combat alleged violations. In addition, the report addresses recent developments in the U.S. government's authority to obtain data stored overseas. Analysis of the developments and trends highlighted in this report identifies what can be expected in 2016: increased parallel regulation by different governments over the same conduct and increased aggressiveness by the U.S. government to enforce U.S. law on conduct engaged in by foreign nationals and companies overseas, all leading to increasing challenges for companies operating in multiple jurisdictions.

We encourage you to read this report in conjunction with BakerHostetler's other year-end reviews, including: "Foreign Corrupt Practices Act 2015 Year-End Update," "2015 Year-End Securities Litigation and Enforcement Highlights," and "BakerHostetler 2015 Year-End Review of Class Actions." These can be found at bakerlaw.com.

This report is edited by Jonathan B. New and Patrick T. Campbell. Contributing writers are David M. McMillan, Shawn P. Hough, Marco Molina, Frank M. Oliva, and Denise Vasel.

I. Securities Fraud

I. Securities Fraud

The current age of globalization and interconnected marketplaces has increasingly prompted regulators of different jurisdictions to regulate the same conduct, particularly in the securities arena, where the impact of securities law violations can be felt across national borders. The U.S. government has also been aggressively enforcing U.S. securities laws against individuals and entities located outside the U.S. for conduct substantially occurring overseas. From legislation and enforcement actions targeting manipulative "spoofing" to the first-ever criminal conviction for insider trading based on hacked information to regulation of the post-2008 financial crisis credit default swap markets, 2015 saw a number of key developments in cross-border securities law issues.

A. "Anti-Spoofing": Cross-Border Legislation, Regulation, and Criminal Enforcement

The "Flash Crash" of May 6, 2010 saw the Dow Jones Industrial Average plummet 1,000 points in a matter of minutes. Subsequent investigation revealed that a U.K.-based trader named Navinder Singh Sarao and his repeated use of a high-frequency trading tactic known as "spoofing" – placing sham orders to artificially inflate or depress the price of a security, and then making bona fide trades on the opposite side of the sham order to take advantage of the manipulated price – may have been the primary cause.[1] Congress and regulators have since set out to curb the manipulative practice: first, with Congress's enactment of a package of anti-spoofing legislation under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) and the Commodity Exchange Act (CEA), followed by the U.S. Securities and Exchange Commission's (SEC) adoption of a new rule to enforce these laws.[2]

It appears that more regulation will soon follow. Complementing a 2012 white paper issued by the U.S. Commodities Futures Trading Commission (CFTC) that sought feedback on proposed anti-spoofing regulations,[3] in March 2015 the U.S. Financial Regulatory Authority (FINRA) proposed a set of rules that would require developers of trading algorithms – such as those used by the Flash Crash trader – to register and undergo qualification examinations.[4] The final rules are expected to be approved by the SEC sometime in early 2016. FINRA has also issued guidance on effective supervision and control practices for firms engaging in algorithmic trading strategies.[5] And on January 5, 2016, it announced its plans to issue report cards that will grade those firms on these practices. In May 2015, CFTC Chairman Timothy Massad said that the CFTC has analyzed all the feedback about the white paper and "will make a determination in the near future on what additional measures, if any, might be necessary to address automated trading."[6]

Foreign regulators have also undertaken anti-spoofing measures. In April 2014, the European Union announced the adoption of a new market abuse regulation and a new directive that will take effect in July 2016.[7] Among other things, the new laws aim to curtail "abusive algorithmic and high-frequency trading strateg[ies]" by way of criminal sanctions.[8] The UK's Financial Conduct Authority (FCA) has recovered millions of dollars in penalties from alleged spoofers in recent years.[9] And high-profile European-based exchanges,

1 Findings Regarding the Market Events of May 6, 2010, Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (Sept. 30, 2010), https://www.sec.gov/news/studies/2010/marketevents-report.pdf.

2 Section 747 of Dodd-Frank created section 4c(a)(5) of the CEA, which makes spoofing unlawful. 7 U.S.C. § 6(c)(a)(5). The SEC promulgated Rule 15c3-5 under the Securities Exchange Act of 1934 to ensure that brokers adopt controls and procedures designed to ensure compliance with this anti-spoofing legislation. 17 C.F.R. § 240.15c3-5.

3 Commodity Futures Trading Commission, "Concept release on risk controls and system safeguards for automated trading environments;" proposed rule. 78 Fed. Reg 177 (Sept. 12, 2013), 56,541–56,574.

4 Financial Regulatory Authority, Regulatory Notice 15-06, Registration of Associated Persons Who Develop Algorithmic Trading Strategies (March 2015), https://www.finra.org/sites/default/files/notice_doc_file_ref/Notice_Regulatory_15-06.pdf.

5 Financial Regulatory Authority, Regulatory Notice 15-09, Equity Trading Initiatives: Supervision and Control Practices for Algorithmic Trading Strategies (March 2015), https://www.finra.org/sites/default/files/notice_doc_file_ref/Notice_Regulatory_15-09.pdf.

6 Speech, Commodity Futures Trading Commission, Remarks of Chairman Timothy Massad before the Energy Risk Summit USA 2015 (May 12, 2015).

7 Press Release, European Commission, European Commission seeks criminal sanctions for insider dealing and market manipulation to improve deterrence and market integrity (Feb. 4, 2014), http://europa.eu/rapid/press-release_IP-11-1218_en.htm.

8 *Id.*

9 Kit Chellel, The Spoofing Traders Who Were Ordered to Pay $9 Million, Bloomberg (Aug. 12, 2015), http://www.bloomberg.com/news/articles/2015-08-12/traders-who-spoofed-market-must-pay-9-million-u-k-judge-says.

including the Deutsche Börse, have introduced new surveillance software that is meant to detect unusual trading patterns.[10]

International commodity exchanges including the Intercontinental Exchange (ICE) and the CME Group, Inc. (CME) have also recently adopted anti-spoofing rules. In August 2014, CME adopted Rule 575, which explicitly prohibits entering trade orders "with the intent . . . to cancel the order before execution or to modify the order to avoid execution."[11] And in January 2015, ICE modified Rule 8A.10 of its trading rules to specifically prohibit spoofing-related activity.[12] The Japan Securities and Exchange Surveillance Commission has also brought enforcement actions against spoofers,[13] and the China Securities Regulatory Commission announced in 2015 that it will increase its efforts to regulate spoofing in Chinese markets.[14] As part of these efforts, in August 2015 Chinese exchanges and authorities froze 24 accounts that were suspected of having spoofed the Chinese markets in Shanghai and Shenzhen.[15]

Although U.S. regulators have initiated dozens of civil enforcement actions and disciplinary proceedings against alleged "spoofers," the first-ever criminal conviction in the United States for spoofing was obtained in 2015. In October 2014, the U.S Department of Justice (DOJ) charged commodities trader Michael Coscia with 12 counts of spoofing and commodities fraud stemming from his alleged use of automated trading to make and then cancel non-bona fide trades through CME in Chicago and ICE in Europe.[16] European regulators and ICE officials testified against Coscia during his trial. On November 4, 2015, a federal jury in Chicago convicted Coscia on all 12 counts.[17] The commodities fraud counts carry maximum sentences of 25 years in prison and a $250,000 fine, while the spoofing counts carry maximum sentences of 10 years in prison and a $1 million fine. Sentencing of Coscia is scheduled for March 17, 2016.

In addition to this landmark verdict, the DOJ also secured another spoofing-related guilty plea in 2015. On January 12, 2015, the DOJ indicted Canadian resident Aleksandr Milrud in the District of New Jersey for commodities fraud stemming from his spoofing-related activity.[18] Milrud was charged with devising, in Canada, a plan to spoof the U.S. securities markets using a web of brokerage accounts that he controlled in China and South Korea. On September 14, 2015, Milrud pleaded guilty to one count of conspiracy and now faces up to five years in prison as well as penalties and disgorgements totaling more than $500,000. There is also a pending SEC enforcement action against Milrud, which will likely result in additional monetary fines and other penalties.

These prosecutions complement the purported DOJ's active case against the purported Flash Crash trader, Navinder Singh Sarao.[19] On April 21, 2015, UK authorities arrested Sarao in London based on a DOJ criminal complaint that accused him of having significantly caused the Flash Crash in 2010 through spoofing-related activity. On September 3, 2015, an Illinois federal grand jury indicted Sarao on 22 counts of fraud and commodity manipulation, which carry a maximum of 380 years in jail. Sarao, who lives in London, is currently fighting extradition on the grounds that the U.S. charges would not be criminal offenses under English law and that – even if they would be – he should be tried in the UK. His extradition hearing was held in February 2016 and the judge indicated he would issue a decision by March 23, 2016.

10 Scila Press Release, Duetsche Börse Prolongs Cooperation with Scila-Deutsche Börse Trading Surveillance Office to Continue to Use State of the Art Surveillance Technology (Dec. 7, 2015), http://scila.se/deutsche-borse-prolongs-cooperation-with-scila-deutsche-borse-trading-surveillance-office-to-continue-to-use-state-of-the-art-surveillance-technology/#.

11 Letter, CME Group, Inc., Adoption of Rule 575 ('Disruptive Practices Prohibited') and Issuance of CME Group Market Regulation Advisory Notice RA1405-5 (Aug. 28, 2014), http://www.cftc.gov/filings/orgrules/rule082814cmedcm001.pdf.

12 Notice, Intercontinental Exchange, Rule Amendment Notice #92 (Jan. 14, 2015), https://www.theice.com/publicdocs/futures_canada/member_notices/2015_01_13_Rule_Amendment_Notice_92.pdf.

13 Japan Exchange Regulation, Addressing Unfair Trading Straddling Markets (September 2015), http://www.jpx.co.jp/english/regulation/ensuring/preventing/about-unfair-trading/tvdivq0000000fi0-att/eg01.pdf.

14 Gabriel Wildau, China targets high-frequency traders in 'spoofing' probe, Financial Times (July 31, 2015).

15 Gabriel Wildau, Citadel account suspended in China amid 'spoofing' probe, Financial Times (Aug. 3, 2015).

16 Press Release, Department of Justice, High-Frequency Trader Indicted For Manipulating Commodities Future Markets In First Federal Prosecution For Spoofing (Oct. 2, 2014), http://www.justice.gov/usao-ndil/pr/high-frequency-trader-indicted-manipulating-commodities-futures-markets-first-federal.

17 *Id.*

18 Press Release, Department of Justice, Canadian Man Charged in First Federal Securities Fraud Prosecution Involving 'Layering' (Jan.13, 2015), http://www.justice.gov/opa/pr/canadian-man-charged-first-federal-securities-fraud-prosecution-involving-layering.

19 Press Release, Department of Justice, Futures Trader Charged with Illegally Manipulating Stock Market, Contributing to the May 2010 Market 'Flash Crash' (Apr. 21, 2015), http://www.justice.gov/opa/pr/futures-trader-charged-illegally-manipulating-stock-market-contributing-may-2010-market-flash.

B. First-Ever Insider Trading Case Based on Information Hacked Abroad

In what has been called the first criminal case involving a securities fraud scheme involving hacked inside information,[20] in August 2015 the DOJ charged nine defendants for their role in a scheme to profit from stolen nonpublic information about corporate earnings announcements.[21] According to the DOJ, two Ukrainian hackers spearheaded the scheme over a period of five years, using advanced techniques to hack into newswire services and steal hundreds of corporate earnings announcements before they were publicly released.[22] The hackers allegedly created a secret web-based location to transmit the stolen data to traders in Russia, Ukraine, Malta, Cyprus, France, and the United States.[23]

On December 21, 2015, Georgia-based real estate developer Alexander Garkusha pleaded guilty to one count of conspiring to commit wire fraud in connection with the charges.[24] The DOJ had alleged that Garkusha used non-public information from the Ukrainian hackers to place illicit trades in stocks, options, and other securities, while funneling a portion of his illegal profits to the hackers in return.[25] According to the DOJ, the scheme enabled the defendants to make over $100 million in illicit profits.[26]

Garkusha, who was born in Russia and is a U.S. citizen, agreed to forfeit $125,000 in profits he made as a result of his participation in the scheme.[27] Some of the other defendants are scheduled to face trial in October 2016;[28] others reside in Ukraine, and international warrants have been issued for their arrest.[29] 34 defendants face related civil charges by the SEC.

C. Credit Default Swaps

According to regulators, the 2008 financial crisis revealed the need for more comprehensive regulation in the credit default swap industry. Efforts began with an agreement at the 2009 G20 Pittsburgh Summit to enhance derivatives-related regulations, and continued with the enactment of Title VII of Dodd-Frank. Those efforts continued apace in 2015. As discussed below, both U.S. and European regulators are hard at work revamping their swap-related regulations, and law enforcement agencies on both sides of the pond continue to investigate and bring cases against entities and individuals for alleged fraud involving credit default swaps. These developments should be closely watched in 2016.

1. Cross-Border Regulation of Credit Default Swaps

In speeches in April[30] and September[31] 2015, CFTC Chairman Massad made clear that the CFTC intends to fine-tune and strengthen its credit default swap regulations. Among other things, the CFTC contemplates a new package of regulatory amendments aimed at incentivizing market participants to register and trade through the newly created swap execution facilities, or "SEFs." The CFTC hopes that increased SEF registration will make this market more transparent to regulators and market participants. The CFTC has also proposed regulations aimed at limiting the amount of paperwork necessary for these actors to trade through these platforms and streamlining the process for correcting erroneous trades.[32] But perhaps the biggest proposal is a regulation designed to ensure the anonymity of swaps traders, which assuages financial institutions' fears that disclosure of their swaps trades would negatively affect other dealings with bank counterparties.[33]

The European Union also introduced comprehensive legislation designed to implement the hallmarks of the

20 Kayla Robbins, West Forsyth man pleads guilty in international trading scheme, Forsyth County News (Dec. 24, 2015), http://www.forsythnews.com/section/6/article/29028/.

21 Press Release, Department of Justice, Nine People Charged In Largest Known Computer Hacking And Securities Fraud Scheme (Aug. 11, 2015), http://www.justice.gov/usao-edny/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme.

22 *Id.*

23 Press Release, Securities and Exchange Commission, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015), http://www.sec.gov/news/pressrelease/2015-163.html.

24 Nate Raymond, Trader pleads guilty in U.S. insider trading hacking case, Reuters (Dec. 21, 2015), http://www.reuters.com/article/usa-crime-garkusha-idUSL1N14A23W20151221

25 *Supra* note 21.

26 *Id.*

27 *Supra* note 20.

28 *Id.*

29 *Supra* note 21.

30 Katy Burne and Andrew Ackerman, CFTC Fine-Tunes Rules Covering Swap Trading Venues, Wall Street Journal (Apr. 23, 2015), http://www.wsj.com/articles/cftc-fine-tunes-rules-covering-swap-trading-venues-1429801528.

31 Speech, Commodity Futures Trading Commission, Remarks of Chairman Timothy Massad before the 3rd Annual OTC Derivatives Summit North America (Sep. 29, 2015), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-28.

32 CFTC, Amendment to Swap Data Recordkeeping and Reporting Requirements for Cleared Swaps. 17 C.F.R. Part 45 (Aug. 31, 2015), http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2015-21030a.pdf.

33 *Id.*

2009 G20 Pittsburgh Summit. In 2012, the European Union passed the European Market Infrastructure Regulation ("EMIR"), which, among other things, requires derivative contracts to be traded on exchanges or electronic trading platforms and implements other measures designed to reduce risk in the credit derivative markets.[34] Although EMIR has led to more than 10 billion reports in Europe regarding credit derivative swap trading activity,[35] many of its key mandates will not take effect until 2017.[36]

In the past year, there have been increasing tensions between U.S. and European Union regulators regarding the implementation of the 2009 G20 Pittsburgh Summit agreement due to the CTFC's expansive interpretation of its jurisdiction. European regulators have resisted recognizing U.S.-based clearinghouses, given the lack of harmonization, to date, of the respective laws of each jurisdiction. The concern is that European market participants will be subject to two nonequivalent sets of regulations. The European Union contemplated the imposition of higher capital charges on banks clearing through U.S.-based central counterparties but has since relented in this regard, according to a December 2014 speech by CFTC Chairman Massad.[37] In March 2015, Massad announced that the CFTC is considering tweaks to their regulations to remain more in lockstep with the European regulations.[38]

2. Enforcement

In early 2012, JPMorgan Chase & Co.'s (JPM) chief investment office (CIO), which was responsible for managing hundreds of billions in excess deposits, lost at least $6.2 billion dollars in credit derivative trading.[39] In a classic case of cross-border enforcement, after JPM restated its earnings in July 2012, U.S. authorities and UK authorities – including the SEC, the CFTC, the DOJ, and the FCA – investigated and brought actions concerning the JPM credit derivative losses.

In the United States, the DOJ and SEC filed charges against Javier Martin-Artajo, a former managing director and trading supervisor in the bank's London office, and Julien Grout, a former trader working under Martin-Artajo's direction.[40] The former employees were charged with conspiracy, falsifying books and records, wire fraud, and submitting false filings to the SEC.[41] The DOJ's criminal action, however, has not moved forward because it has been unable to secure the extradition of Grout or Martin-Artajo, who are foreign nationals residing in France and Spain, respectively.[42] The SEC case is in discovery.

U.S. and UK authorities also investigated JPM itself. Among other things, the regulators accused JPM of misstating financial results, lacking effective internal controls to detect and prevent its traders from fraudulently overvaluing investments to conceal hundreds of millions of dollars in trading losses,[43] employing a manipulative device in connection with the bank's trading of credit derivative swaps,[44] mismarking the SCP's positions at issue, and market misconduct.[45] To settle these charges, JPM paid over $1

34 Press Release, European Commission, Commission adopts technical standards for the Regulation on OTC derivatives, central counterparties and trade repositories (Dec. 19, 2012), http://europa.eu/rapid/press-release_IP-12-1419_en.htm?locale=en.

35 Banking & Insurance, EMIR II: Requirement, improvements, developments (Aug. 11, 2015), http://en.finance.sia-partners.com/emir-ii-requirements-improvements-developments.

36 Explanatory Memorandum, European Commission, Commission Delegated Regulation (June 5, 2015), http://ec.europa.eu/finance/financial-markets/docs/derivatives/20150605-delegated-act_en.pdf.

37 Speech, Commodity Futures Trading Commission, Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

38 Katy Burneand Andrew Ackerman, CFTC Fine-Tunes Rules Covering Swap Trading Venues, Wall Street Journal (Apr. 23, 2015), http://www.wsj.com/articles/cftc-fine-tunes-rules-covering-swap-trading-venues-1429801528.

39 United States State Permanent Subcommittee on Investigations, "JPMorgan Chase Whale Trades: A Case History of Derivatives Risks and Abuses" (Mar. 15, 2013), http://www.hsgac.senate.gov/subcommittees/investigations/hearings/chase-whale-trades-a-case-history-of-derivatives-risks-and-abuses.

40 Kevin McCoy, Ex-JPMorgan traders charged in $6B loss, USA Today (Aug. 15, 2013), http://www.usatoday.com/story/money/business/2013/08/14/jp-morgan-loss-charges/2652077/.

41 *Id.*

42 Nate Raymond, Ex-JPMorgan traders, citing arrest risk, avoid SEC deposition in N.Y., Reuters (Oct 21, 2015), http://www.reuters.com/article/us-usa-jpmorgan-londonwhale-idUSKCN0SF2D420151021.

43 Press Release, Securities and Exchange Commission, JP Morgan Chase Agrees to pay $200 million and admits wrongdoing to settle SEC charges (Sep. 19, 2013), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539819965.

44 Press Release, Commodities Futures Trading Commission, CFTC Files and Settles Charges Against JPMorgan Chase Bank, N.A., for Violating Prohibition on Manipulative Conduct in Connection with "London Whale" Swaps Trades (Oct. 16, 2013), http://www.cftc.gov/PressRoom/PressReleases/pr6737-13.

45 Press Release, Financial Conduct Authority, JP Morgan Chase Bank N.A. fined £137,610,000 for serious failings relating to its Chief Investment Office's "London Whale" trades, (Sept. 19, 2013) http://fca.org.uk/news/jpmorgan-chase-bank-na-fined.

billion in fines.[46] Notably, as part of its settlement agreements with the SEC and CFTC, JPM was required to admit certain facts underlying the regulators' charges and publicly acknowledge that it engaged in reckless and manipulative conduct and violated the federal securities laws.[47]

In the UK, after obtaining a settlement with JPM, the FCA dropped both Martin-Artajo and Grout from its own probe into the trading losses. The FCA explained that it decided to stop investigating Martin-Artajo and Grout because they were the subject of pending U.S. criminal proceedings and were not working in the UK.[48] Grout challenged the FCA's decision to drop him from its investigation, claiming that his inability to respond to the FCA's allegations could affect the case against him in the U.S. Grout's challenge was denied by a UK court in March 2015, however.[49]

The FCA faced additional challenges in connection with its investigation of the case. Martin-Artajo and Achilles Macris, JPM's former London-based international chief investment officer who supervised the traders implicated in the trading losses, filed challenges against the FCA in a London court alleging that they were improperly identified in the FCA's enforcement notice against JPM in September 2013. Although Martin-Artajo's challenge is still pending, Macris won an appeal relating to his challenge before the London Court of Appeal. In May 2015, the London Court of Appeal found that the FCA's use of the term "CIO London management" in its enforcement notices – a deliberate and easily identifiable reference to Macris – without providing him with an opportunity to respond to the allegations was improper.[50] Court of Appeal Judge Elizabeth Gloster stated that the reference to "CIO London management" in the FCA's reports and notices "was in context clearly a reference to a particular individual, and not to a body of people."[51]

The decision, which is currently being appealed,[52] could have an impact on how the FCA drafts enforcement notices and conducts its investigations in the future. The decision could force the regulator to describe its decisions more carefully and to provide individuals referenced in its notices with more opportunity to respond to allegations.[53] A number of other individuals have initiated similar appeals with the UK courts concerning FCA enforcement notices related to the foreign exchange market and LIBOR manipulations.[54]

Despite Macris' challenge, however, on February 9, 2016, he was fined by the FCA £792,900 in connection with his role in the trading losses.[55] According to the FCA, Macris failed to be "open and cooperative" about concerns regarding the trading activity that led to the more than $6 billion in losses the bank experienced in 2012.[56] Specifically, the FCA alleged that Macris failed to provide it with information about the full extent of difficulties concerning the credit derivative positions at issue during meetings and telephone calls Macris had with the regulator in March and April of 2012.[57]

D. Benchmark Rates

LIBOR, the London Interbank Offered Rate, is a benchmark interest rate based on the rates at which banks lend unsecured funds to each other on the London interbank market.[58] Banks all over the world use LIBOR as a base rate for setting interest rates on consumer and corporate loans such

46 David Henry, Scandals cost JPMorgan $1 billion in fines, Reuters (Sept. 19, 2013), http://www.reuters.com/article/us-jpmorgan-whale-idUSBRE98I0JL20130919

47 *Supra* notes 43-45.

48 Financial Services: Regulation and Risk, "'London Whale' related judicial review of the FCA fails," http://fsregulation-risk.com/2015/03/11/london-whale-related-judicial-review-of-the-fca-fails/.

49 *Id.*

50 Kit Chellel, Ex-JPMorgan Executive Wins Appeal on FCA London Whale Report, Bloomberg Business (May 19, 2015), http://www.bloomberg.com/news/articles/2015-05-19/ex-jpmorgan-executive-wins-appeal-over-fca-london-whale-report-i9v4tql0.

51 Leanna Orr, London Whale Boss Wins Privacy Case Against Regulator, Chief Investment Officer (May 20, 2015), http://www.ai-cio.com/channel/REGULATION,-LEGAL/London-Whale-Boss-Wins-Privacy-Case-Against-Regulator/.

52 *Supra* note 50; Nicholas Ralph, Supreme Court grants permission for FCA appeal identification ruling, Lexology (Dec. 11, 2015), http://www.lexology.com/library/detail.aspx?g=8b42ad2c-36cf-4cbc-9435-52e37b5cfba9.

53 Alan Ward, Why bankers must be allowed to speak out in their own defense, Law 360 (May 26, 2015), http://www.cityam.com/216388/why-bankers-must-be-allowed-speak-out-their-own-defence.

54 Suzi Ring, Ex-Barclays Forex 'Cartel' Trader Ashton Loses Identity Case, The Washington Post (Jan. 13, 2016), http://washpost.bloomberg.com/Story?docId=1376-O0W8S06JIJW101-7QI6D92AJ17MBJJSM5SF901TGK.

55 DealBook, Ex-JPMorgan Executive Fined $1.1 million in 'London Whale' Case, The New York Times (Feb. 9, 2016), http://www.nytimes.com/2016/02/10/business/dealbook/ex-jpmorgan-executive-fined-1-1-million-in-london-whale-case.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0.

56 *Id.*

57 Damian Fantato, FCA fines JP Morgan trader £793k over London Whale Trades, FT Adviser (Feb. 9, 2016), http://www.ftadviser.com/2016/02/09/regulation/fca-fines-jpmorgan-london-whale-boss-nearly-k-JN6aRJhQwypKWAWJcgOVfL/article.html.

58 James McBride, Understanding the Libor Scandal, Council on Foreign Relations (May 21, 2015), http://www.cfr.org/united-kingdom/understanding-libor-scandal/p28729.

as auto, student, and home loans.[59]

The foreign currency exchange spot market (the "FX market"), which permits traders to buy, sell, exchange, and speculate on currencies, is one of the world's largest and most actively traded financial markets, with trading volume that has averaged as high as nearly $5 trillion a day.[60]

Both LIBOR and the FX market are examples of how alleged securities fraud can be world-wide in nature and lead to cross-border enforcement.

1. LIBOR

In 2015, developments continued in the fallout from the 2012 LIBOR manipulation allegations, with criminal convictions on both sides of the Atlantic. In August 2015, former UBS and Citigroup trader Tom Hayes was convicted in Britain on charges he was the "ringmaster" of a network of more than 25 traders from 16 banks engaged in an attempt to manipulate LIBOR for their own personal gain.[61] And in November 2015, former Rabobank traders and British citizens Anthony Allen and Anthony Conti became the first to be convicted in the U.S. of charges relating to the manipulation of LIBOR rates.[62] Allen and Conti were convicted on charges of conspiracy and wire and bank fraud based on their rigging of yen and U.S. dollar LIBOR. They face up to 30 years in prison.[63]

Hayes, Allen, and Conti were just a few of the many traders alleged to have manipulated LIBOR by asking employees responsible for submitting the LIBOR rates to provide figures that would benefit the traders' positions rather than submitting the rates banks would pay to borrow money.[64] The banks allegedly manipulated the rates by misrepresenting that they could borrow money at artificially low rates to make themselves appear less risky.[65]

The successful prosecutions of Hayes, Allen, and Conti have been viewed as landmark victories for both British and U.S. financial authorities, which view prosecutions relating to the LIBOR scandals as a top priority.[66] At the end of January 2016, however, a London jury acquitted six other former brokers who allegedly conspired to help Hayes in his efforts to manipulate the LIBOR and defraud investors.[67]

The LIBOR scandal has also resulted in massive fines for banks all over the world. As of May 2015, as penalties for their roles in the alleged fraud, global banks such as Barclays, UBS, Dutch Rabobank, Deutsche Bank, RBS, Société Générale, JPM, and Citigroup have paid over $9 billion in fines to a range of U.S. and European regulators.[68]

2. The FX Market

On May 20, 2015, five of the largest banks in the United States and Europe – Citicorp, JPM, Barclays PLC, the Royal Bank of Scotland plc, and UBS AG – entered into another round of settlements with the DOJ, the Federal Reserve, the New York Department of Financial Services, the CFTC, and the FCA in connection with their alleged manipulation of the FX market.[69] Citicorp, JPM, Barclays PLC, and the Royal Bank of Scotland plc pled guilty to charges of conspiring to manipulate the price of U.S. dollars and euros exchanged in the market by using an exclusive electronic chat room and coded language to coordinate their trading

59 *Id.*

60 Anirban Nag, Foreign Exchange, the world's biggest market, is shrinking, Rueters (Feb. 11, 2016), http://www.reuters.com/article/us-global-fx-peaktrading-idUSKCN0VK1UD; CFTC Order Instituting Proceedings Against Citibank, N.A., CFTC Docket No. 15–03, http://www.cftc.gov/ucm/groups/public/@lrenforcementactions/documents/legalpleading/enfcitibankorder111114.pdf.

61 Simon Goodley, Tom Hayes, the Libor-rigging scandal's 'ringmaster,' The Guardian (Aug. 3, 2015), http://www.theguardian.com/business/2015/aug/03/libor-rigging-tom-hayes-sfo.

62 Jill Treanor, Two former Rabobank traders convicted in US Libor rigging trial, The Guardian (Nov. 5, 2015) http://www.theguardian.com/business/2015/nov/05/two-former-rabobank-traders-convicted-us-libor-rigging-trial.

63 Geoffrey Smith, U.S. makes its first convictions in Libor scandal, Fortune (Nov. 6, 2015), http://fortune.com/2015/11/06/u-s-makes-its-first-convictions-in-libor-scandal/.

64 James McBride, Counsil on Foreign Relations, Understanding the Libor Scandal (May 21, 2015), http://www.cfr.org/united-kingdom/understanding-libor-scandal/p28729.

65 *Id.*

66 Jennifer Koons, Libor Prosecutions a Priority, Justice Department says, Main Justice (Sept. 26, 2013), http://www.mainjustice.com/2013/09/26/libor-prosecutions-a-priority-justice-department-says/.

67 Evan Weinberger, London Jury Acquits 6th Trader of Libor Rigging, Law 360 (Jan. 28, 2016), http://www.law360.com/securities/articles/751908?nl_pk=f451a2d7-1c25-4ea1-bcdb-947ab53668ee&utm_source=newsletter&utm_medium=email&utm_campaign=securities0e0f9a23d050&utm_source=newsletter&utm_medium=email&utm_campaign=whitecollar.

68 James McBride, Council on Foreign Relations, Understanding the Libor Scandal (May 21, 2015), http://www.cfr.org/united-kingdom/understanding-libor-scandal/p28729.

69 Dunstan Prial, Five Major Banks Plead Guilty to Felony Charges Over Currency Rigging, FOX Business (May 20, 2015), http://www.foxbusiness.com/features/2015/05/20/five-major-banks-plead-guilty-to-felony-charges-over-currency-rigging.html.

of U.S. dollars and euros.[70] The fifth bank, UBS AG, pled guilty to LIBOR manipulation after the DOJ declared the bank in breach of its LIBOR non-prosecution agreement. UBS AG agreed to pay a criminal penalty of $203 million.[71] In total, the settlements require the banks to pay nearly $6 billion in both civil and criminal fines for their misconduct.[72]

The settlements were announced just six months after several of the banks agreed to pay $3.4 billion in fines in connection with the FX market manipulation to the CFTC, the FCA, and the Swiss Financial Market Supervisory Authority (FINMA).[73] In total, the new round of settlements brings the fines paid by the banks to U.S. and foreign regulators in connection with alleged Forex manipulation to over $9 billion.

In December 2015, FINMA temporarily banned six former UBS AG foreign exchange and metals traders from the securities industry because they repeatedly attempted to manipulate foreign exchange benchmarks.[74] Thus, despite the staggering amount of fines and penalties that have been amassed, the fallout from the FX market manipulation allegations appears likely to continue in 2016.

---

70 Press Release, Department of Justice, Five Major Banks Agree to Parent-Level Guilty Pleas (May 20, 2015), http://www.justice.gov/opa/pr/five-major-banks-agree-parent-level-guilty-pleas.

71 *Id.*

72 *Supra* note 69.

73 TrefisTeam, Taking Stock Of How Much Banks Have Paid For Settling Forex Manipulation Charges, Forbes (May 28, 2015), http://www.forbes.com/sites/greatspeculations/2015/05/28/taking-stock-of-how-much-banks-have-paid-for-settling-forex-manipulation-charges/#74816dbd6543.

74 Silke Koltrowitz, Six former UBS forex staff banned by Swiss watchdog, Reuters (Dec. 17, 2015), http://www.reuters.com/article/us-banks-forex-ubs-idUSKBN0U00T020151217.

II. Anti-Money Laundering, Racketeering, and Trade Sanctions

II. Anti-Money Laundering, Racketeering, and Trade Sanctions[75]

In 2015, the U.S. and other countries continued to coordinate their efforts in targeting large-scale frauds with intercontinental reach. Various countries are augmenting their regulatory frameworks to put pressure on international money launderers, and the widely publicized Liberty Bank investigation has culminated in a final guilty verdict. The global anti-corruption case against FIFA executives continues apace. And the U.S. government announced a half billion dollar forfeiture against Commerzbank for violating trade sanctions laws with Iran and Sudan. These developments, discussed below, highlight the increased prevalence of international cooperation in cross-border enforcement, anti-money laundering, racketeering, and trade sanction laws.

A. Anti-Money Laundering

1. Regulatory Updates

The emergence of ISIS in the Middle East and the January and November attacks in Paris, France, highlighted 2015's spike in global terrorism. This wave of terrorism has spurred regulators to pursue more aggressive anti-money laundering policies in a global effort to cut off the money supply that finances terrorist agendas. On May 20, 2015, the European Union adopted new rules to help fight money laundering and terrorist financing, a month after unveiling its European Security Agenda.[76] These rules aim to (i) facilitate the work of financial intelligence units from different member states to identify suspicious transfers of money; (ii) establish a coherent policy toward non-European Union countries that have deficient anti-money laundering and counter-terrorist-financing regimes; and (iii) ensure full traceability of funds transfers within, to, and from the European Union. On November 17, 2015, the European Union announced that implementation of these rules is on its way and that the European Commission will continue to assess the money laundering and terrorism financial risks that are caused by "supranational and cross-border dimensions," with the hope of providing "a clear picture of the threats and vulnerabilities of the financial system that can lead to terrorism financing risks."[77] The European Commission hopes to finalize this risk assessment by June 2017.

Similarly, on April 24, 2015, the Monetary Authority of Singapore issued guidelines for its anti-money laundering laws with a focus on preventing the financing of terrorism.[78] These guidelines stressed the importance of customer-based due diligence and the implementation of internal policies and controls to identify suspicious transactions accurately and quickly.

In the same vein, for the first time in a decade, on June 12, 2015 the U.S. Department of Treasury (Treasury) released a lengthy report that details the key money-laundering and terrorist-financing risks to the United States financial sector and analyzes the thousands of enforcement actions and regulatory proceedings that targeted these risks.[79] While the threats, vulnerabilities, and risks identified in this report are unchanged from the Treasury's last report in 2005, this report provides updated assessments that reflect the technological and industrial developments since that time, such as digital currencies.

Finally, it should be noted that consistent with the recent trends in financial regulation, regulators are targeting individuals at financial institutions to ensure that adequate anti-money laundering policies are in place. In February 2015, the New York Department of Financial Services (DFS) unveiled a plan to

75 For information about cross-border regulation and enforcement of the Foreign Corrupt Practices Act ("FCPA") and analogous anti-corruption laws in other countries, see BakerHostetler's Mid-Year FCPA Report, https://www.bakerlaw.com/files/uploads/Documents/FCPA/FCPA_2015_Mid-Year_Update_p11.pdf.

76 Press Release, European Commission, European Parliament backs stronger rules to combat money laundering and terrorism financing (May 20, 2015), http://europa.eu/rapid/press-release_IP-15-5001_en.htm.

77 European Commission – Fact Sheet, http://europa.eu/rapid/press-release_MEMO-15-6115_en.htm (last visited Jan. 27, 2016).

78 Monetary Authority of Singapore, Guidelines to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism (Apr. 24, 2015), http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Guidelines%20to%20MAS%20Notice%20626%20%20April%202015.pdf.

79 Report, Department of the Treasury, National Terrorist Financing Risk Assessment (June 12, 2015), http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20–%2006-12-2015.pdf.

require senior compliance officers to personally attest to the adequacy of their systems guarding against money laundering.[80] Months later, on December 1, 2015, the DFS and Governor Andrew Cuomo revealed new rule proposals that implemented their February plan.[81] The proposed rules make senior executives of financial institutions personally liable if their companies fail to establish and maintain adequate anti-money laundering controls, mirroring the Sarbanes-Oxley Act, which makes top executives personally liable for accounting fraud. But, unlike the Sarbanes-Oxley Act, these proposed rules require DFS-regulated institutions to submit to DFS by April 15 of each year certifications executed by each institution's chief compliance officer or the functional equivalent. Compliance officers who file false certifications may be subject to criminal penalties.

These proposed rules are the result of a four-year investigation by the DFS into terrorist financing and anti-money laundering compliance. According to the DFS, this investigation uncovered "serious shortcomings" by financial institutions and their senior executives. The DFS's proposed rules also apply anti-money laundering regulations to the digital currency industry, including Bitcoin. This recent regulatory activity regarding digital currencies is another example of how regulators are working to harmonize their regulations with the evolving technological practices of the financial sector.

Soon after the DFS's announcement, on March 18, 2015, the UK Treasury revealed its plans to apply anti-money laundering regulations to various exchanges trading digital currencies.[82]

2. Criminal Enforcement: Liberty Reserve

The global investigation into Liberty Reserve over its alleged role as one of the principal money transfer agents used by cybercriminals around the world to distribute, store, and launder the proceeds of illegal activity continued into 2015, with the sentencing of the company's former information technology manager in January 2015.[83] The 36-month sentence[84] was likely one of the last sentencings in a money-laundering investigation and prosecution that touched multiple countries – the U.S., Costa Rica, the Netherlands, Spain, Sweden and Switzerland, among others – and involved cooperation among various regulators. For example, Liberty Reserve's computer servers in the Netherlands showed that a significant portion of the company's users were from the U.S., which allowed U.S. authorities to demonstrate a substantial U.S.-connected money-laundering operation and pursue the case overseas.[85] Without the cooperation of the Dutch National High Tech Crime Unit, these servers probably would have been destroyed and the case against Liberty Reserve would not have been nearly as strong.

Many U.S. agencies – including the U.S. Secret Service, the Internal Revenue Service-Criminal Investigation, and the U.S. Immigration and Customs Enforcement's Homeland Security Investigations – took part in the Liberty Reserve investigation. In addition, Costa Rican officials were integral to the investigation and recovery of assets, seizing about $20 million of Liberty Reserve funds. Spanish authorities also contributed, facilitating the arrest by U.S. officials of Liberty Reserve's founder in 2013 during a layover in Spain. The Liberty Reserve case is truly global, and law enforcement's success was possible only with significant cross-border cooperation.

B. Racketeering: The FIFA Case

In May 2015, after collaborating in secret for months, the DOJ and the Office of the Attorney General of Switzerland (OAG) commenced criminal investigations of corruption, bribery, and mismanagement among high-ranking officials of the Fédération Internationale de Football Association (FIFA), the organization responsible for regulating and

80 New York State Department of Financial Services, Proposed Rules on Virtual Currencies (Feb. 4, 2015), http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf.

81 Press Release, New York Department of Financial Services, Governor Cuomo Announces Anti-Terrorism Regulation Requiring Senior Financial Executives to Certify Effectiveness of Anti-Money Laundering Systems (Dec. 1, 2015), http://www.dfs.ny.gov/about/press/pr1512011.htm.

82 Press Release, UK Treasury, Digital currencies: call for information (Mar. 18, 2015), https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information.

83 Press Release, Department of Justice, Former Liberty Reserve IT Manager Sentenced to 36 Months Prison (Jan. 30, 2015), http://www.justice.gov/opa/pr/former-liberty-reserve-it-manager-sentenced-36-months-prison.

84 *Id.*

85 See Jake Halpern, Bank of the Underworld, The Atlantic (May 2015), http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/.

promoting soccer worldwide.[86] Swiss authorities arrested seven of those officials on May 27, 2015,[87] and conducted raids at the head offices of FIFA and CONCACAF – the governing body for soccer in North America, Central America and the Caribbean – to secure relevant data and documents.[88] Although the arrests and document seizures were made in connection with two different criminal investigations that are being conducted separately by the DOJ and the OAG, the regulators have coordinated their efforts to prevent collusion and the possible destruction of relevant evidence.[89] Most recently, at the end of December 2015, Swiss authorities handed over bank documents related to the case to the DOJ to assist in its investigation.[90] News of the arrests was followed shortly by the unsealing of a 47-count indictment by the DOJ in the Eastern District of New York charging 14 defendants with racketeering, wire fraud and money laundering conspiracies, among other offenses, "in connection with the defendants' participation in a 24-year scheme to enrich themselves through the corruption of international soccer."[91] In addition to the indictment, the guilty pleas of four individual defendants and two corporate defendants were also unsealed by the DOJ. The same day, the OAG announced that it has opened criminal proceedings against persons unknown on suspicion of criminal mismanagement and money laundering in connection with the allocation of the 2018 and 2022 World Cups.[92]

In December 2015, after another morning raid in Zurich, Swiss police and U.S. prosecutors launched a second wave of arrests and indictments that more than doubled the number of defendants, and they announced the guilty pleas of eight additional defendants.[93] The DOJ's superseding, 92-count indictment charges an additional 16 defendants in connection with the alleged conspiracy, bringing to 41 the total number of individuals and entities charged.

The DOJ's investigation is focused on allegations relating to allocation of media, marketing, and sponsoring rights for soccer tournaments in the United States and Latin America. The DOJ alleges that over the past 24 years, the sports marketing executives allegedly paid more than $150 million in bribes and kickbacks to FIFA officials to secure broadcasting rights and sell them to broadcasters. Defendants named in the DOJ's indictments include FIFA officials, high-ranking officials of other soccer governing bodies that operate under the FIFA umbrella, sports marketing executives alleged to have made illegal payments, and a broadcaster who allegedly brokered payments between the FIFA officials and the sports marketing executives.

The focus of the OAG's parallel investigation relates to suspected irregularities surrounding FIFA's decision to award Russia and Qatar the 2018 and 2022 World Cups, respectively. Although the investigations will likely continue for years to come, 12 individuals and two sports marketing companies have already been convicted in the United States, and have agreed to forfeit more than $190 million.[94] In addition, more than $100 million has been restrained in the U.S. and abroad.[95]

C. U.S. Economic Sanctions Violations/Export Controls

On March 12, 2015, the DOJ announced that Commerzbank AG agreed to forfeit $563 million, pay a $79 million fine, and enter into a deferred prosecution agreement with the DOJ for violating the International Emergency Economic Powers Act (IEEPA), which authorizes the president to declare the existence of a threat and take certain actions to block transactions and freeze assets to deal with that threat, specifically with respect to threats that are foreign in nature, and with the Bank Secrecy Act

86 Press Release, Department of Justice, Nine FIFA Officials and Five Corporate Executives Indicted for Racketeering Conspiracy and Corruption (May 27, 2015), http://www.justice.gov/opa/pr/nine-fifa-officials-and-five-corporate-executives-indicted-racketeering-conspiracy-and.

87 *Id.*

88 *Id.*

89 Tom Peck, Fifa corruption arrests: Three things you need to know, Independent (May 17, 2015) http://www.independent.co.uk/news/world/europe/fifa-corruption-arrests-three-things-you-need-to-know-10278733.html

90 USA Today, Swiss hand over evidence to U.S. authorities in FIFA case (Dec. 30, 2015), http://www.usatoday.com/story/sports/soccer/2015/12/30/swiss-hand-over-evidence-to-us-authorities-in-fifa-case/78066836/.

91 *Supra* note 86.

92 Press Release, The Office of the Attorney General of Switzerland Seizes Documents at FIFA (May 27, 2015), https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-57391.html.

93 Matt Ford, FIFA in Double Trouble, The Atlantic (Dec. 3, 2015), http://www.theatlantic.com/international/archive/2015/12/fifa-indictments/418761/.

94 *Supra* note 86.

95 Press Release, Department of Justice, Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption (Dec. 3, 2015), http://www.justice.gov/usao-edny/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption

(BSA).[96] The DOJ had alleged Commerzbank concealed hundreds of millions of dollars in transactions on behalf of Iranian and Sudanese businesses that were prohibited by U.S. economic sanctions laws targeting Iran and Sudan, even though bank managers raised red flags about these illegal practices.

A key part of the case involved activity that took place in Commerzbank's Frankfurt, Germany back offices. Commerzbank designated a group of employees in the Frankfurt back office to review and amend Iranian payments so that the payments would not be stopped by U.S. sanctions filters. Commerzbank purposely omitted any reference to Iranian entities to avoid being stopped pursuant to U.S. sanctions.

In its press release, the DOJ emphasized that banks with a U.S. presence will be scrutinized for engaging in this type of activity: "Financial institutions must heed this message: banks that operate in the United States must comply with our laws, and banks that ignore the warnings of those charged with compliance will pay a very steep price." Importantly, the DOJ cited Commerzbank's failure to have an effective anti-money laundering program as a significant factor that led to the joint investigations into the bank's business activities.

On April 17, 2015, the U.S. Attorney's office for the Southern District of Texas unsealed a 24 count indictment charging four corporations (including Hosoda Taiwan Limited Corporation in Taiwan, Golsad Istanbul Trading Ltd. in Turkey and the Faratel Corporation in Iran) and five individuals with facilitating the illegal export of high-tech microelectronics, uninterruptible power supplies, and other commodities to Iran in violation of the IEEPA. The indictment alleges that, between 2010 and the present, the defendants were part of an Iranian procurement network in the United States that sent $24 million worth of micro-electronics used in a wide range of military systems to Iran via Turkey and Taiwan. If convicted, the corporate defendants face fines of up to $1 million for each violation of the IEEPA counts.[97]

On May 1, 2015, Paris-based BNP Paribas, S.A. was sentenced to a five-year term of probation, and ordered to forfeit $8,833,600,000 to the United States and pay a $140 million fine, for conspiring to violate the IEEPA and the Trading with the Enemy Act (TWEA) by processing billions of dollars' worth of transactions through the U.S. financial system on behalf of Sudanese, Iranian, and Cuban entities.[98] This represents the first time a financial institution has been sentenced for violations of U.S. economic sanctions, and the total financial penalty (the forfeiture together with the fine) was the largest financial penalty imposed in a criminal case to date.[99]

Meanwhile, in 2015 the United States Office of Foreign Assets Control (OFAC) levied significant fines against foreign banks and other corporations for violating a bevy of U.S. sanctions programs. In October 2015, Paris-based investment bank Crédit Agricole Corporate and Investment Bank paid over $300,000,000 to settle allegations that the bank committed 4,297 sanctions violations, primarily of the Sudanese Sanctions Regulations, 31 C.F.R. part 538 (SSR).[100] OFAC had alleged the bank omitted references to U.S.-sanctioned parties in U.S. SWIFT payment messages sent to the United States, which prevented U.S. financial institutions from appropriately reviewing and analyzing the transactions for compliance with OFAC regulations. The settlement was part of a global settlement among OFAC, the DOJ, the New York County District Attorney's Office, the Federal Reserve Board of Governors, and the DFS.[101]

96 Press Release, Department of Justice, Commerzbank AG Admits to Sanctions and Bank Secrecy Violations, Agrees to Forfeit $563 Million and Pay $79 Million Fine (Mar. 12, 2015), http://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and.

97 Press Release, U.S. Department of Justice, Four Companies and Five Individuals Indicted for Illegally Exporting Technology to Iran (Apr. 17, 2015), available at http://www.justice.gov/opa/pr/four-companies-and-five-individuals-indicted-illegally-exporting-technology-iran.

98 Press Release, U.S. Department of Justice, BNP Paribas Sentenced for Conspiring to Violate the International Emergency Economic Powers Act and the Trading with the Enemy Act (May 1, 2015), http://www.justice.gov/opa/pr/bnp-paribas-sentenced-conspiring-violate-international-emergency-economic-powers-act-and.

99 *Id.*

100 United States Department of Treasury, Enforcement Information for October 20, 2015, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20151020_cacib.pdf. (last visited Feb. 15, 2016).

101 Press Release, U.S. Department of Justice, Crédit Agricole Corporate and Investment Bank Admits to Sanctions Violations, Agrees to Forfeit $312 Million (Oct. 20, 2015), https://www.fbi.gov/newyork/press-releases/2015/credit-agricole-corporate-and-investment-bank-admits-to-sanctions-violations-agrees-to-forfeit-312-million.

III. Accounting Fraud

III. Accounting Fraud

In 2015, there were major developments in SEC cross-border enforcement relating to accounting fraud. Most notably, the SEC reached overseas to enforce violations of the securities laws relating to the Olympus Corp. alleged accounting fraud that was uncovered in October 2011.

In February 2015, Japanese banker Hajime "Jim" Sagawa settled civil charges with the SEC relating to his role the accounting scandal at Olympus Corp., a Japanese camera and medical device manufacturer. Among other things, the settlement alleges that Sagawa violated Sections 17(a)(91) and 17(a)(3) of the Securities Act, which prohibit fraudulent conduct in the offer and sale of securities.[102] According to the SEC, Olympus conducted a decades-long scheme to obscure losses it incurred during the 1990s by, among other things, transferring funds to a "secret web" of offshore entities that were used to purchase failed investments using bank loans.[103] Olympus hired a brokerage firm owned in part by Sagawa to advise them on how to repay the loans, with Sagawa accepting a "disproportionate financial advisory fee" that he then transferred to the offshore firms for repayment to the banks. Sagawa's brokerage firm also advised Olympus on a $2 billion takeover of a British medical instruments company, receiving $687 million in advisory fees and preference shares that he then transferred to Olympus's offshore creditors. Although Sagawa was not required to pay a penalty, the SEC has barred him from working in the securities industry.[104]

The settlement follows the 2013 withdrawal of charges against Olympus by the UK's Serious Fraud Office, after a British judge ruled that English law does not criminalize the misleading of auditors by the company under audit.[105] Olympus has not been able to escape prosecution in Japan, however. In 2013, Tokyo prosecutors fined the company approximately 700 million yen and obtained guilty pleas from both Olympus itself and three of the company's executives in connection with the accounting fraud.[106]

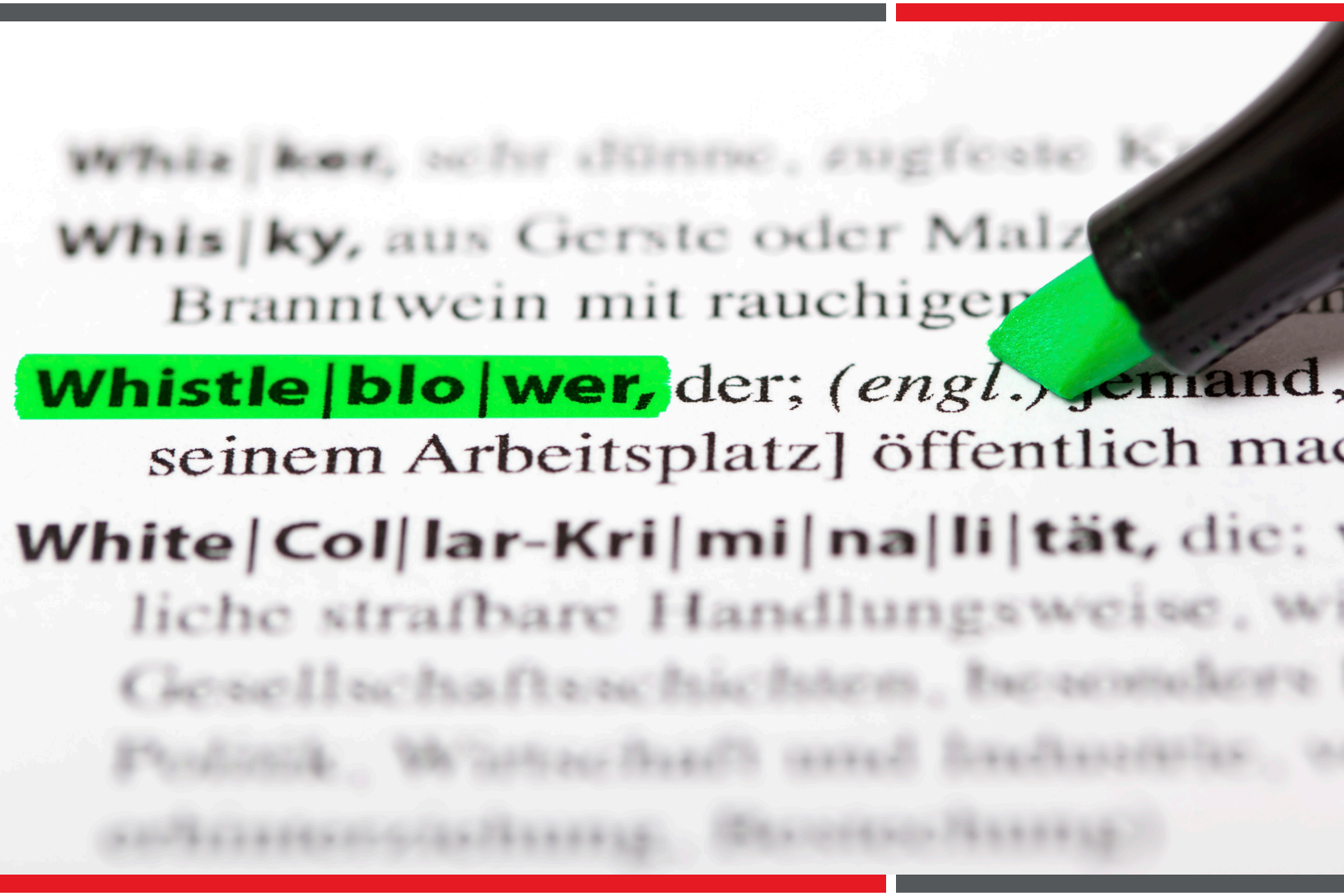
102 In the Matter of Hajime Sagawa, Administrative Proceeding No. 3-16412 (Feb. 27, 2015), http://www.sec.gov/litigation/admin/2015/33-9733.pdf.

103 Sarah Lynch, Banker tied to Olympus accounting scandal settles with U.S. SEC, Reuters (Feb. 27, 2015), http://www.reuters.com/article/sec-olympus-case-idUSL1N0W11ME20150227

104 Sarah Lynch, Banker tied to Olympus accounting scandal settles with U.S. SEC, Reuters (Feb. 27, 2015), http://www.reuters.com/article/sec-olympus-case-idUSL1N0W11ME20150227

105 *Id.*

106 *Id.*



IV. Whistleblower Programs

IV. Whistleblower Programs

A. Foreign Whistleblowers Under The SEC Whistleblower Program[107]

The SEC continues to see an uptick in both the quantity and quality of tips under the whistleblower program instituted in 2010 under Dodd-Frank.[108] And those tips have increasingly come from individuals outside the U.S.; during the 2015 fiscal year, approximately 10 percent of the tips received by the SEC originated from individuals in foreign countries, including the United Kingdom (72), Canada (49), China (43), India (33), and Australia (29).[109] Overall, in 2015 the SEC received whistleblower tips from 65 different countries.[110]

The largest-ever whistleblower award – more than $30 million – was issued in September 2014 and paid in early 2015 to a whistleblower in a foreign country, the fourth such award to a whistleblower living outside the U.S.[111] According to Sean McKessy, the chief of the SEC's Office of the Whistleblower:

107 For more information about the SEC and CFTC whistleblower programs see the Baker 2015 Mid-Year Securities Litigation and Enforcement Highlights Report, http://www.bakerlaw.com/alerts/2015-mid-year-securities-litigation-and-enforcement-highlights.

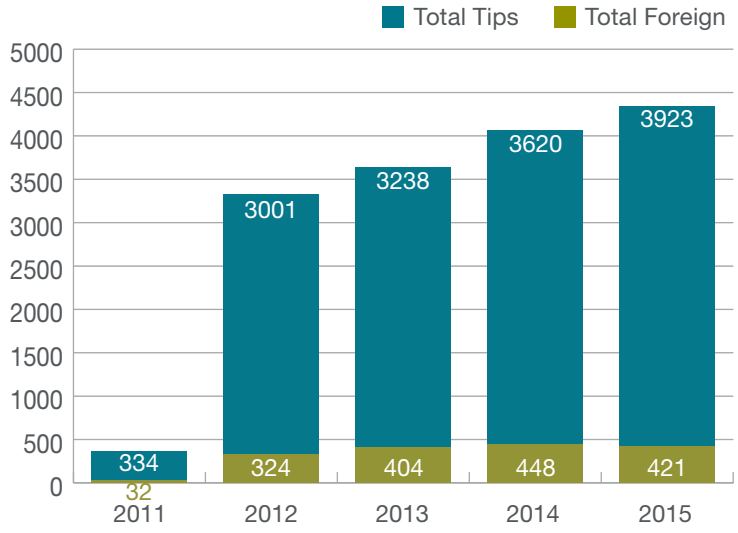
108 Speech, SEC, The SEC as the Whistleblower's Advocate (Apr. 30, 2015), http://www.sec.gov/news/speech/chair-white-remarks-at-garrett-institute.html.

109 SEC, 2015 Annual Report to Congress on the Dodd-Frank Whistleblower Program, http://www.sec.gov/whistleblower/reportspubs/annual-reports/owb-annual-report-2015.pdf.

110 *Id.*

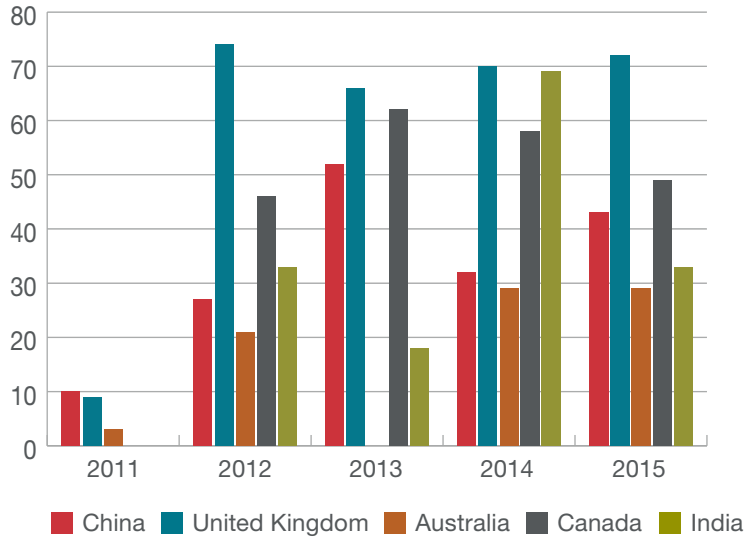
111 Press Release, SEC, SEC Announces Largest-Ever Whistleblower Award (Sep. 22, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543011290.

Number of Foreign Tips vs. Total Tips: 2011-2015



Source: Securities and Exchange Commission, Annual Reports to Congress on the Dodd-Frank Whistleblower Program (2011-2015), https://www.sec.gov/about/offices/owb/owb-resources.shtml#reports.

Number of Tips Originating From China, UK, Australia, Canada and India: 2011-2015



Source: Securities and Exchange Commission, Annual Reports to Congress on the Dodd-Frank Whistleblower Program (2011-2015), https://www.sec.gov/about/offices/owb/owb-resources.shtml#reports.

This award of more than $30 million shows the international breadth of our whistleblower program as we effectively utilize valuable tips from anyone, anywhere to bring wrongdoers to justice. Whistleblowers from all over the world should feel similarly incentivized to come forward with credible information about potential violations of the U.S. securities laws.[112]

Also in September 2015, the SEC issued an award of 20 percent to two foreign nationals who jointly reported information that enabled the SEC to open an investigation into the underlying activity.[113]

These awards continue despite litigation concerning the programs' international reach. In 2014, the Second Circuit held in *Liu v. Siemans AG*, 763 F.3d 175 (2d Cir. 2014), that foreign whistleblowers are not protected by the anti-retaliation provisions of Dodd-Frank when the conduct is entirely foreign. In that case, a Chinese employee of a U.S.-listed German company reported violations of the Foreign Corruption Practices Act to the SEC and subsequently suffered retaliation for his actions. The court held that to provide the whistleblower protection outlined in Dodd-Frank would be an impermissible extraterritorial application of the statute.

Nonetheless, the SEC has maintained the position that while the anti-retaliation provisions of Dodd-Frank may not apply to foreign whistleblowers, *Liu* is not controlling with respect to the bounty provisions of the act, as Dodd-Frank's bounty provisions "have a different Congressional focus than the anti-retaliation provisions."[114]

B. Whistleblower Programs in Other Jurisdictions

The success and international reach of the SEC whistleblower program appears to be calling other countries into action. In China, for example, whistleblower laws issued by the China's Supreme People's Procuratorate (the government agency responsible for prosecution and investigation) were strengthened with China's enactment of the "Regulations on Whistleblowing Work by the People's Procuratorate," effective September 30, 2014. The new regulations require that the procuratorate take a more proactive approach, including a protection plan designed to both prevent and punish retaliation. The protections will go into effect once the whistleblower so requests, and they can even lead to police protection in emergency situations.[115]

That pattern, however, was put into perspective by a September 2014 survey of whistleblower protection laws in G20 countries,[116] which suggested that whistleblower protection has a way to go – especially in terms of retaliation. Comprehensive laws covering private sector corporations, for example, are lacking. According to the report, anonymity, internal disclosure procedures, and external reporting channels remain the topics most in need of substantive development. Notably, of all the G20 countries, the United States scored the highest marks for protecting the anonymity of whistleblowers.

And despite the apparent success of the SEC whistleblower program, some jurisdictions remain unconvinced that US-style whistleblower programs are effective tools to combat wrongdoing. In July 2014, the FCA and the Bank of England Prudential Regulation Authority reviewed certain recommendations of the Parliamentary Committee on Banking Standards about whistleblowing; specifically whether or not they should undertake a financial incentive scheme to encourage reports of wrongdoing, similar to the U.S. system.[117] The regulatory bodies ultimately refused to create such incentives, finding that the costs associated with them, including legal costs, far outweighed the benefits, which they believe were ultimately realized by only a small portion of whistleblowers whose evidence directly led to certain convictions. The report further noted that protection for whistleblowers against retaliation in the UK already exists through the Public Interest Disclosure Act of 1998.

112 *Id.*

113 Duxes 2015: Year of the Whistleblower Report, http://www.duxes.cn/eNewsletter/Industry_AC_8/AC%20Interview%EF%BC%9A2015%20Year%20of%20the%20Whistleblower%20EN.pdf

114 In the Matter of the Claim for Award in connection with [Redacted], Whistleblower Award Proceeding No. 2014-10 (Sep. 22, 2014), https://www.sec.gov/rules/other/2014/34-73174.pdf.

115 *Supra* note 111.

116 Transparency International Australia, Final Report, Whistleblower Protection Laws in G20 Countries: Priorities for Action (Sept. 2014), https://www.transparency.de/fileadmin/pdfs/Themen/Hinweisgebersysteme/Whistleblower-Protection-Laws-in-G20-Countries-Priorities-for-Action.pdf.

117 FCA, Financial Incentives for Whistleblowers (July 2014), http://www.kkc.com/wp-content/uploads/2014/12/Bank-of-England-2014.pdf.

V. Corporate Liability

V. Corporate Liability

In the area of corporate liability, the U.S. and the UK are increasing their focus on prosecuting corporate executives in addition to companies themselves. The UK has taken a page out of the U.S. playbook with the relatively recent introduction of deferred prosecution agreements.

A. Executive Accountability

Recently, the U.S. (and foreign jurisdictions) have pursued increased enforcement against corporate executives to further deter corporate wrongdoing. On September 9, 2015, Sally Quillian Yates, the U.S. deputy attorney general, issued a memorandum announcing the DOJ's new guidelines regarding its intensifying focus on individual wrongdoers in the context of corporate misconduct (Yates Memo).[118] The Yates Memo is the latest in a line of pronouncements by the DOJ concerning the framework federal prosecutors must use in determining whether and how to charge corporations and their employees in criminal cases. It is particularly significant for corporate officers and employees who may be subject to DOJ investigations. As Ms. Yates explained in a September 10, 2015 speech at New York University's program on corporate compliance and enforcement, the new guidelines "are institutional policy shifts that change the way we investigate, charge, and resolve cases."[119]

Six directives comprise the core of the Yates Memo, which applies to both criminal and civil matters: (i) to be eligible for any cooperation credit, corporations must provide the DOJ with all relevant facts about the individuals involved in corporate misconduct; (ii) both criminal and civil corporate investigations should focus on individuals from the inception of the investigation; (iii) criminal and civil attorneys handling corporate investigations should communicate routinely with one another; (iv) absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals; (v) corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires, and declinations as to individuals in such cases must be memorialized; and (vi) civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.

While a number of the above directives relate to the manner in which DOJ personnel communicate and interact with one another (for example, criminal and civil DOJ attorneys must now promptly and routinely consult with each other concerning pending investigations), the directives focusing on cooperation credit and corporate settlements are the most important. The Yates Memo effectively codifies prior public statements by DOJ officials that they intend to take a tougher stance on prosecuting all levels of corporate employees. As Ms. Yates explained, "We cannot allow the flesh-and-blood people responsible for misconduct to walk away, while leaving only the company's employees and shareholders to pay the price."[120]

Critically, to receive any cooperation credit under the new guidance, corporations must disclose all relevant facts concerning individual misconduct. This is an important shift from the fourth factor – "the corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents" – stated in the April 2008 "Principles of Federal Prosecution of Business Organizations" issued by then-Deputy Attorney General Mark Filip and since incorporated into the U.S. Attorney's Manual.[121] Previously, corporations could receive "partial" credit even if disclosures regarding individual misconduct were incomplete. Cooperation is now an all-or-nothing proposition.

Importantly, Ms. Yates made it clear that corporations cannot plead ignorance. "If they don't know who is responsible, they will need to find out. If they want any cooperation credit, they will need to investigate and identify the responsible parties,

118 Memorandum from Sally Quillian Yates, United States deputy attorney general, Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), http://www.justice.gov/dag/file/769036/download.

119 Speech, U.S. Department of Justice, deputy attorney general Sally Quillian Yates Delivers Remarks at New York University School of Law Announcing New Policy on Individual Liberty in Matters of Corporate Wrongdoing (Sept. 10, 2015), http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

120 *Id.*

121 Memorandum from Mark Filip, United States deputy attorney general, Principles of Federal Prosecution of Business Organizations (Aug. 28, 2008), http://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf.

then provide all non-privileged evidence implicating those individuals."[122] This cooperation requirement will be ongoing, as Ms. Yates explained, "Corporate plea agreements and settlement agreements will include a provision that requires the companies to continue providing relevant information to the government about any individuals implicated in the wrongdoing. A company's failure to continue cooperating against individuals will be considered a material breach of the agreement and grounds for revocation or stipulated penalties."[123]

The Yates Memo includes additional guidelines on the interplay between corporate settlements and individual liability. According to the new guidelines, before finalizing a settlement with a company during an ongoing investigation into individual liability, DOJ attorneys must provide a memorandum to their supervisors that details potentially liable individuals, the current status of the investigation regarding their conduct, and a plan to bring the matter to resolution prior to the end of any statute of limitations period. The assistant attorney general or U.S. attorney whose office handled the investigation, or their designees, must approve any declinations. In addition, absent "extraordinary circumstances," corporate settlements may not include agreements to dismiss charges or release claims against, or provide immunity for, individual officers or employees. The guidelines articulated in the Yates Memo show the seriousness of the U.S. government's intentions to prosecute those individuals it believes are responsible for white-collar crimes.

Meanwhile, in the UK, there have been key changes to civil securities enforcement standards to address the goal of holding more corporate executives responsible for corporate misconduct. Starting in March 2016, the FCA will implement the "Senior Managers Regime" (SMR).[124] The SMR will require certain mangers at banks to file a "statement of responsibilities." The statement will allow the FCA to pinpoint the responsible individual or individuals when regulations are violated. A key component of the SMR is the type of liability it places on responsible individuals; essentially, executives will be guilty until proven innocent. Executives will be presumed liable unless they can prove they took the necessary remedial steps when a regulatory breach occurs.

B. Use of Deferred Prosecution Agreements

While U.S. regulators frequently use deferred prosecution agreements (DPAs) as a means of resolving actions against organizations, this law enforcement tool had not taken root abroad until February 2014, when UK prosecutors were permitted to use DPAs against organizations in cases of economic crime.[125] Under the new UK DPA settlement system, prosecutors can charge a company "with a criminal offence but proceedings are automatically suspended."[126] The company is required to agree to certain conditions, such as financial penalties and cooperation with prosecutors; if the company does not honor the conditions, the proceedings may resume.

The first apparent use of DPAs in the UK against organizations came in May 2015, when Ben Morgan, the joint head of bribery corruption in the UK's Serious Fraud Office (SFO), issued the first "invitation letters" giving corporations the opportunity to begin DPA negotiations.[127] Concerning the DPA program, Morgan stated:

> *A DPA responds to criminal liability—as I said, no cozy deals—so don't be under any illusion. In a process scrutinized by a Crown Court judge, criminal proceedings will be commenced against the organization but immediately suspended pending compliance with the terms of the agreement. Those terms can pack a hefty punch too—a fine, compensation, remedial*

122 Speech, U.S. Department of Justice, deputy attorney general Sally Quillian Yates Delivers Remarks at New York University School of Law Announcing New Policy on Individual Liberty in Matters of Corporate Wrongdoing (Sept. 10, 2015), http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school.

123 *Id.*

124 See Bank of England, Senior Managers Regime – Forms, http://www.bankofengland.co.uk/pra/Pages/authorisations/smr/default.aspx (last visited Feb. 11, 2016).

125 Press Release, UK Serious Fraud Office, Deferred Prosecution Agreements: New Guidance for Prosecutors (Feb. 14, 2014), https://www.sfo.gov.uk/2014/02/14/deferred-prosecution-agreements-new-guidance-prosecutors/.

126 Press Release, UK Serious Fraud Office, Deferred Prosecution Agreements: Consultation on Draft Code of Practice (June 27, 2013), https://www.sfo.gov.uk/2013/06/27/deferred-prosecution-agreements-consultation-draft-code-practice/.

127 News Release, UK Serious Fraud Office, Ben Morgan: Compliance and Cooperation (May 20, 2015), https://www.sfo.gov.uk/2015/05/20/compliance-and-cooperation.

measures, in some cases a monitor and other possible terms. But it has a lot going for it too—speed and certainty, as I have said; a level of compatibility that enables us to get a bit closer to that hallowed ground of a global resolution for conduct that crosses borders, as I suspect much of the activity in your sector inevitably would; and also the chance to really live your corporate values—integrity around facing up to what's gone wrong and putting it right rather than being on the back foot, having to be defensive.[128]

On November 30, 2015, the SFO announced the first approval of an application for a DPA with Standard Bank Plc (Standard Bank).[129] Standard Bank was the subject of an indictment alleging failure to prevent bribery in violation of Section 7 of the UK Bribery Act 2010 related to an alleged $6 million bribery payment. The SFO alleged that the bribery payment was directed to members of the government of Tanzania. Under the DPA, Standard Bank agreed to pay a fine of $25.2 million, in addition to paying the government of Tanzania $7 million and the SFO £330,000 to cover the costs related to the investigation. Standard Bank also agreed to fully cooperate with the SFO, conduct a review of existing anti-bribery and corruption controls, and implement recommendations of an independent reviewer.

The end result of the Standard Bank case somewhat tempers previous concerns over suggestions by SFO officials that waiver of privilege would be required for successful DPA negotiations. It does not appear that the SFO required Standard Bank to waive privilege in this instance, and the Standard Bank DPA may be an indicator of how DPAs will be used in the future. This newly available tool for UK prosecutors – which they appear eager to use – provides corporations with an incentive to cooperate and resolve criminal liability in the UK.

128 *Id.*

129 Press Release, UK Serious Fraud Office, SFO Agrees First UK DPA with Standard Bank (Nov. 30, 2015) https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank.

VI. U.S. Government's Authority to Seize Data Stored Overseas

VI. U.S. Government's Authority to Seize Data Stored Overseas

As cybercrime takes on an increasingly international flavor, the United States has accelerated efforts to seize data evidence located overseas. Traditionally, law enforcement has employed mutual legal assistance treaties (MLATs) – agreements between two or more countries that facilitate cross-governmental collaboration in criminal investigations and prosecutions – to obtain evidence located abroad, but the MLAT process is viewed as complicated, time-consuming, and ill-equipped to handle 21st-century data storage and privacy issues. In 2015, the U.S. government continued its efforts – through litigation and proposed amendments to the Federal Rules of Criminal Procedure – to sidestep the MLAT process and gain quick access to such evidence.

A. The Microsoft Ireland Case

There were developments in 2015 in *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, 14-2985-cv (2d Cir. 2014) (hereinafter "*Microsoft-Ireland*"). In December 2013, on application from the U.S. government, a federal magistrate judge in New York issued a warrant under the Stored Communications Act, 18 U.S.C. §§ 2701–2712, directing Microsoft to disclose all emails and other private information associated with a certain email account in Microsoft's possession, custody, or control. When Microsoft determined that the target account was hosted in Dublin, Ireland, and that the data content was stored there, it filed a motion to quash the warrant, arguing the information was beyond the U.S. government's reach.

The magistrate judge denied Microsoft's motion to quash the subpoena in April 2014, and U.S. District Court Judge Preska adopted the magistrate's ruling in August 2014. Judge Preska agreed with the magistrate that it was a "question of control, not a question of . . . location" of the sought-after information. Because Microsoft could easily access the data and no U.S. law enforcement official would step foot in Irish territory, producing the information was "not an intrusion on the foreign sovereign."

Microsoft appealed to the Court of Appeals for the Second Circuit, where a number of technology companies including Amazon, Cisco, Apple, and AT&T filed amicus briefs. Both Microsoft and the government made further submissions in advance of the hearing of Microsoft's appeal in September 2015. The central issue was whether the government can compel Microsoft and other Internet service providers to produce emails or other private communications stored in a foreign nation.

Oral argument in *Microsoft-Ireland* took place on September 9, 2015, and the parties have since filed letters with the court debating the implications of a recent ruling by the European Court of Justice. *Schrems v. Data Protection Commissioner*, Case C-362/14. *Schrems* invalidated a "safe harbor" provision in the EU Data Protection Directive that would have prohibited a European Facebook user from lodging a complaint about the adequacy of the U.S.'s data protection regime. Microsoft has argued that the decision "underscores that the subject of cross-border data transfers is fraught and easily gives rise to international discord[,]" but the government insists that *Schrems* has no impact on data transfers between the European Union and the U.S. pursuant to a judicially issued warrant. Whether the Second Circuit affords any weight to the *Schrems* decision remains to be seen.

B. Proposed Amendments to Federal Rule of Criminal Procedure 41

In 2015, the government also continued efforts to reach data overseas through proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure. The proposal, originally submitted in 2013 with revisions in August 2014, would allow the Government to execute search warrants via remote access when the physical location of the place to be searched is unknown – potentially expanding the extraterritorial reach of government search warrants.

The proposed amendments would facilitate the government's ability to obtain a remote search warrant in situations where criminals use sophisticated anonymizing technologies to obscure a user's IP address or use multiple computers in many districts simultaneously as part of complex criminal schemes.[130] First, the amendment would authorize a court in a district where "activities related to a crime"

130 See Letter from the Department of Justice (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf.

have occurred to issue a warrant to use remote access to search electronic storage media, and to seize or copy electronically stored information located within or outside that district, where (A) "the district where the media or information is located has been concealed through technological means," or (B) "in an investigation of a violation of 18 U.S.C. § 1030(a)(5) [concerning computer fraud and related activity], the media are protected computers that have been damaged without authorization and are located in five or more districts."[131]

The proposals are now the subject of vigorous criticism and opposition. The period for public comment, which ended on February 17, 2015, saw a number of high-profile submissions from technology leaders and privacy rights advocates. Google, for example, submitted comments in February 2015 arguing that the proposed amendment would impermissibly expand the extraterritorial reach of Rule 41 since it would in many cases end up authorizing the government to conduct searches outside the United States. Google urged the Criminal Rules Advisory Committee to reject the proposed amendment and leave the matter to Congress.[132]

The committee held meetings in March and September 2015 to debate the proposed amendments. The proposal next goes to the standing committee, which may elect to make changes, then to the Judicial Conference and subsequently to the United States Supreme Court for final approval.

C. LEADS Act

In 2015, various draft bills[133] were introduced that would amend the antiquated Electronic Communications Privacy Act (ECPA) by enhancing protections for private electronic communications. One such bill, the Law Enforcement Access to Data Stored Abroad (LEADS) Act, which garnered broad support from technology companies, business organizations, and privacy and civil liberties advocacy groups, is designed to both clarify the scope of the U.S. government's authority to search and seize electronically stored information outside the United States and to strengthen and enhance the MLAT process. The LEADS Act would update the ECPA with two primary improvements:

- Recognizing that U.S. law enforcement may not use warrants to compel the disclosure of customer content stored outside the United States unless the account holder is a U.S. person;
- Strengthening the MLAT process through increased accessibility and transparency, by requiring an online intake form and docketing system where foreign governments could both submit MLAT requests electronically and track the status of those requests. It would seek to provide accountability by requiring the DOJ to annually publish statistics on the number of MLAT requests it receives and completes, as well as their average processing time.[134]

On September 16, 2015, the Senate Judiciary Committee held a hearing on a similar bill, S.356 – the Electronic Communications Privacy Act Amendments Act of 2015.[135] That proposal is also designed to enhance protection for cloud-based private data. It would, among other things, prohibit cloud service providers from knowingly divulging the contents of private electronic communications to a governmental entity and require the government to obtain a warrant before requiring providers to disclose the content of such communications.

131 Fed. R. Crim. P. 41(b)(6), 10-11 (Preliminary Draft 2014), https://www.justsecurity.org/wp-content/uploads/2014/09/preliminary-draft-proposed-amendments.pdf.

132 Comment from Richard Salgado, Google Inc. (submitted Feb. 13, 2015), http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0029.

133 See, e.g., Law Enforcement Access to Data Stored Abroad Act, H.R. 1174 – 114th Congress (Feb. 27, 2015); Electronic Communications Privacy Act Amendments Act of 2015, H.R. 283 – 11th Congress (Jan. 12, 2015).

134 Law Enforcement Access to Data Stored Abroad Act, S. 512 – 114th Congress (Feb. 12, 2015).

135 United States Senate Committee on the Judiciary, Reforming the Electronic Communications Privacy Act (Sept. 16, 2015), http://www.judiciary.senate.gov/meetings/reforming-the-electronic-communications-privacy-act.

VII. 2016 and Beyond

VII. 2016 and Beyond

Any company concerned about finding itself in the crosshairs of a regulatory investigation or enforcement action should take stock of the current state of play in cross-border regulation and enforcement: with increasing frequency, governments of multiple countries are seeking to regulate and remedy the same types of misconduct, often working in parallel and sometimes even directly coordinating efforts. The U.S. government has also shown increased vigor in applying U.S. law to conduct by foreign nationals and entities overseas. Pressure on companies engaging in even the slightest cross-border conduct can therefore be extreme. It is thus crucial for companies to consult with their counsel to understand the regulatory and policy agendas of U.S. and foreign authorities and to develop adequate procedures to ensure compliance with any foreign laws to which a company might be subject. As we move further into 2016, we expect a continued rise in the international character of the regulatory and enforcement environment. Readers should stay tuned for BakerHostetler's next Cross-Border Government Investigations and Regulatory Enforcement Review, which will highlight key cross-border regulation and enforcement developments in the first half of 2016.

For more information about cross-border government investigations and regulatory enforcement law, or if you have questions about how these matters may impact your business, please contact the following BakerHostetler attorneys or visit our website.

John J. Carney

jcarney@bakerlaw.com
212.589.4255

Steven M. Dettelbach

sdettelbach@bakerlaw.com

Cleveland
216.861.7177

Washington, D.C.
202.861.1621

George A. Stamboulidis

gstamboulidis@bakerlaw.com
212.589.4211

bakerlaw.com

Celebrating the 100th anniversary of its founding this year, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation, and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.