



JULY 2017 • VOL 1, ISSUE 2

# White Collar Watch

INSIDE

## THIS ISSUE

- 1** A Note from the Editors
- 2** The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications
- 4** At the Intersection of Cybersecurity and White Collar
- 6** Mark M. Lee Joins Blank Rome as Partner in White Collar Defense & Investigations Group
- 8** FCPA under the New Administration
- 10** *Chambers USA 2017* Recognizes Blank Rome White Collar Defense & Investigations Attorneys
- 11** The Sessions Memo: A Significant Reversal of Policy?
- 11** *Who's Who Legal 2017* Recognizes Blank Rome White Collar Defense & Investigations Attorneys
- 12** Record-Setting Prosecutions in the Money Transmitting Business: Ways to Avoid Compliance Violations
- 13** Recent Speaking Engagements
- 14** Jane F. Barrett Joins Blank Rome as Of Counsel in White Collar Defense & Investigations Group
- 15** Overview of IRS Penalties for Individuals with Foreign Bank Accounts and Investments
- 17** Blowing the Whistle: Employers Must Properly Respond to Employee Allegations of Wrongdoing

## A NOTE FROM THE EDITORS

Welcome to the summer edition of Blank Rome's **White Collar Watch**. In a world that seems to bring new challenges daily—such as the global cybersecurity attacks that were launched in late June—this newsletter is designed to provide content that we hope will assist you in areas of continuing and growing importance.

This edition of *White Collar Watch* includes articles about cybersecurity, changes in whistleblower laws, the Foreign Corrupt Practices Act ("FCPA") under the Trump administration, enforcement actions against FinTech companies, and an overview of IRS penalties for individuals with foreign bank accounts. We also are pleased to introduce you to two new attorneys who have joined our practice—Mark M. Lee and Jane F. Barrett—who bring a wide range of experience in white collar matters, including criminal defense, environmental issues, and corporate investigations.

Blank Rome's white collar defense & investigations practice group is comprised of seasoned, nationally recognized attorneys who represent companies and individuals facing criminal and regulatory investigations, congressional inquiries, whistleblower accusations, and self-discovered misconduct. This newsletter will continue to discuss key industry topics and provide insightful analysis on a wide range of issues potentially impacting companies and individuals within numerous industries. We welcome your feedback, as well as any suggestions for articles in areas that may impact your business, and encourage you to share this newsletter with friends and colleagues. We are here to be of service to you, and your companies, in every way possible.

Our team wishes you and your families a happy and healthy summer!



JOSEPH G. POLUKA

PARTNER



INBAL P. GARRITY



WILLIAM B. SHIELDS

OF COUNSEL

EDITORS, *WHITE COLLAR WATCH*

## The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications

BY ARIEL S. GLASNER AND BRIDGET MAYER BRIGGS



ARIEL S. GLASNER BRIDGET MAYER BRIGGS

ASSOCIATE

ASSOCIATE

***This is the second installment in a series of articles. For an understanding of FinTech products and services and how they are disrupting the financial services industry, please read our first article in this series, [An Introduction to Financial Technology](#).***

As law enforcement authorities and government regulators have developed a greater understanding of the FinTech industry, various government agencies have brought enforcement actions against FinTech companies in an effort to protect the integrity of our financial system. This article surveys these actions and discusses the implications that they may have on the FinTech industry as a whole. Notably, cryptocurrencies such as bitcoin have dominated regulators' focus relative to other FinTech products and services. For this reason, it is useful to separate out enforcement actions involving cryptocurrencies from enforcement actions involving other areas of FinTech.

### Enforcement Actions Concerning the Use, Exchange, and Marketing of Cryptocurrencies

A number of well-publicized criminal prosecutions have been pursued by the U.S. Department of Justice ("DOJ") against companies and individuals seeking to use bitcoin or other cryptocurrencies for illicit purposes. Perhaps most notoriously, the founders of Silk Road and Silk Road 2.0 were charged with money laundering, computer hacking, trafficking narcotics, and trafficking fraudulent identification documents after it was determined that these websites promoted a black market for illegal drugs and other illicit goods and services by having users anonymously conduct

transactions in bitcoin.<sup>1</sup> The DOJ also charged several individuals associated with Coin.mx, a bitcoin exchange service that offered, for a fee, to exchange cash for bitcoins for cyberattack victims paying bitcoin ransoms to individuals hijacking their computers. The defendants in this case were charged with operating an unlicensed money transmitting firm, making corrupt payments, wire fraud, and money laundering.<sup>2</sup>

Other agencies also have pursued actions against companies using cryptocurrencies in an unlawful manner. For example, the Securities and Exchange Commission ("SEC") has brought enforcement actions against a number of companies offering virtual currency investment opportunities that did not properly register security offerings.<sup>3</sup> Likewise, the Commodity Futures Trading Commission ("CFTC") brought an enforcement action against Coinflip, a service connecting buyers and sellers of bitcoin operation contracts, for failure to meet regulatory requirements and failure to register as a swap execution facility.<sup>4</sup> Finally, the Financial Crimes Enforcement Network ("FinCEN") assessed a civil penalty against Ripple Labs, a digital currency operator, based upon its failure to register as a money services business and to implement a suitable anti-money laundering program prior to beginning sales.<sup>5</sup>

- Government agencies are still in the early stages of determining how to address the challenges presented by FinTech. While certain agencies, such as the DOJ, have pursued enforcement actions to punish and deter conduct that is clearly unlawful, other agencies such as the IRS, FinCEN, and the CFPB have sought to establish their authority to regulate this space by initiating test cases.

Most recently, the Internal Revenue Service ("IRS") has sought to investigate the use of cryptocurrencies to facilitate tax evasion. In November 2016, the IRS requested, and received, permission to serve a "John Doe" summons on Coinbase, a cryptocurrency exchange, seeking information on all users who transferred virtual currency from 2013 to 2015. If the summons is upheld, the IRS will be able to mine the data that is produced under the summons to identify tax evaders and bring enforcement actions accordingly.<sup>6</sup>

## Enforcement Actions Brought in Connection with Other FinTech Services

Though perhaps subject to less scrutiny than businesses involving cryptocurrencies, other services that fall under the FinTech umbrella have not been immune from regulatory enforcement actions. In 2013, the DOJ shut down Liberty Reserve, an online payment processor and digital currency system, for facilitating drug trafficking and child pornography, because it did not require users to validate their identification information. The company and seven of its principals were charged with conspiracy to commit money laundering and operating an unlicensed money transmitting business.<sup>7</sup> In March 2015, the Office of Foreign Asset Control ("OFAC") entered into a settlement agreement with PayPal based upon allegations that PayPal did not implement sufficient compliance procedures to identify and prevent transactions violating U.S. sanctions programs.<sup>8</sup>

The Consumer Financial Protection Bureau ("CFPB") also has pursued

enforcement actions against FinTech enterprises. In 2016, it entered into a consent order with LendUp, an online lending company that advertised its loan programs as allowing consumers to build up their credit over time. The CFPB determined that LendUp engaged in unfair and deceptive practices in violation of the Consumer Financial Protection Act, because it failed to provide consumers with several of the advertised benefits of the program and it had no written policies or procedures in place related to credit reporting.<sup>9</sup> Also in 2016, the CFPB brought an enforcement



action against Dwolla, Inc., an online payment provider, on the grounds that Dwolla falsely represented the strength of its data security practices, in violation of the Dodd-Frank Wall Street Reform and Consumer Protection Act.<sup>10</sup>

## Implications for the FinTech Industry

Government agencies are still in the early stages of determining how to address the challenges presented by FinTech. While certain agencies, such as the DOJ, have pursued enforcement actions to punish and deter conduct that is clearly unlawful, other agencies such as the IRS, FinCEN, and the CFPB have sought to establish their authority to regulate this space by initiating test cases. Certain enforcement actions also indicate that government agencies are prepared to punish FinTech companies for failing to "know their customers" because they, like banks, often serve as gatekeepers to the financial system.

The enforcement actions that have been pursued thus far are reflective of the broad range of laws and regulations that the FinTech industry implicates. The evolving and innovative nature of this industry also means, however,

that legal requirements can be murky and that the industry is vulnerable to individuals and entities seeking to exploit the industry for fraudulent and illegal activity. We will return to these issues in future issues of *White Collar Watch*. Nevertheless, FinTech companies are well-served to understand the types of enforcement actions that already have been brought, so that they can evaluate applicable legal requirements and ensure that compliance procedures are properly implemented as early as possible. □ – ©2017 BLANK ROME LLP

1. *United States v. Ulbricht*, 1:14-cr-00068 (S.D.N.Y.); *United States v. Benthall*, 1:14-2427 (S.D.N.Y.).

2. *United States v. Murgio et al.*, 1:15-769 (S.D.N.Y.).

3. *In the Matter of Erik T. Voorhees*, File No. 3-15902 (SEC June 3, 2014) (involving failure to register securities offerings in violation of the Securities Act); *In the Matter of BTC Trading Corp. and Ethan Burnside*, File No. 3-16307 (SEC Dec. 8, 2014) (involving the operation of unregistered virtual securities exchanges); *In the Matter of Sand Hill Exchange et al.*, File No. 3-16598 (SEC June 17, 2015) (involving violations of Dodd-Frank Act by company offering investments in financial derivatives through its website rather than on a national securities exchange in violation of the Dodd-Frank Act).

4. *In the Matter of Coinflip*, CFTC Docket No. 15-29 (Sept. 17, 2015).

5. *In the Matter of Ripple Labs Inc. and XRP II, LLC*, Financial Crimes Enforcement Network, Order Number 2015-05 (May 5, 2015).

6. See Case No. 3:16-cv-06658-JSC (N.D. Cal.).

7. *United States v. Liberty Reserve, et al.*, 13-368 (S.D.N.Y.).

8. Settlement Agreement Between OFAC and PayPal, Inc., MUL-762365.

9. *In the Matter of Flurish d/b/a Lendup*, File No. 2016-CFPB-0023 (Sept. 27, 2016).

10. *In re Dwolla, Inc.*, File No. 2016-CFPB-0007 (Mar. 2, 2016).

## At the Intersection of Cybersecurity and White Collar

BY INBAL P. GARRITY AND NICHOLAS R. TAMBONE



INBAL P. GARRITY



NICHOLAS R. TAMBONE

PARTNER

ASSOCIATE

### The global “ransomware” cyberattack in early May 2017

resulted in tens of thousands of computer systems being taken hostage by hackers and, in the instances involving hospitals, put lives at risk.<sup>1</sup> Companies that suffered breaches are exposed to liability, and many of the breaches reportedly could have been solved with an act as simple as downloading the latest updates to Windows operating systems.<sup>2</sup>

By now, everyone knows—even as they hope to be spared—that cyberattacks are a big problem. One recent estimate projected that cybercrimes cost the global economy \$445 billion in 2016 alone.<sup>3</sup> Other projections anticipate that the cost of cybercrimes will be close to two trillion dollars globally by 2019.<sup>4</sup> Beyond the integrity of an employee’s office computer, industry leaders recently spoke about the serious cybersecurity risks created by the “Internet of Things”—that is, the dissemination of Internet-connected “smart devices,” now present in everything from cars to thermostats and healthcare equipment.<sup>5</sup> And, as the May 2017 ransomware attacks demonstrated, no individual or entity is immune to a cyberattack.

The New York Department of Financial Services (“DFS”) already has implemented a regulatory scheme for the imposition of penalties on businesses that do not comply with cybersecurity guidelines. As of March 1, 2017, New York financial institutions subject to DFS oversight have been required to comply with new cybersecurity rules, or face stiff penalties. And, the Securities

and Exchange Commission (“SEC”) has recently cautioned that companies with deficient cybersecurity disclosures may soon face SEC enforcement actions. What is clear is that cybersecurity is an issue that no business can afford to ignore—regardless of industry.

### The New Cybersecurity Regulations Implemented by DFS Introduce Measures That Exceed Existing Guidance

The new DFS cybersecurity regulations require New York financial institutions to, among other things, adopt a cybersecurity program, implement and maintain a cybersecurity policy, and designate a qualified chief information security officer. These new measures are a “sea change in how government approaches cybersecurity.”<sup>6</sup> Indeed, in a press release announcing the implementation of the new rules, Governor Andrew Cuomo characterized the measures as “the first-in-the-nation cybersecurity regulation.”<sup>7</sup> According to some reports, the new measures well exceed current general practices among financial institutions.<sup>8</sup> For instance, the new regulations will require data encryption measures, enhanced multi-factor authentication, annual certification, and incident reporting. Deadlines for

compliance are coming as soon as August 28, 2017. All of this means that businesses should start taking steps to comply with these measures now.

### Although the SEC Has Not yet Brought a Cybersecurity-Related Enforcement Action, It Soon May

It is not only financial institutions doing business in New York that need to be aware of regulators’ focus on cybersecurity. In response to questions, the SEC’s Acting

Enforcement Director, Stephanie Avakian, recently stated that, under the right circumstances, the SEC “absolutely” would bring an enforcement action against a company with inadequate cybersecurity disclosures.<sup>9</sup> Although the SEC has not yet brought an enforcement action based on insufficient cybersecurity disclosures, it appears ready to do so. And, arguably, with an increasing number of front page stories on devastating cyberattacks, the pressure is mounting for the SEC to act. This means that public companies and securities firms, in addition to banks and other financial institutions subject to the oversight of New York’s DFS, must ensure that their cybersecurity measures, and disclosures about those measures, are robust.

- Regardless of industry, it is critical that companies assess and address data security risks and ensure compliance with applicable regulations, particularly in light of increased focus by regulators. Implementing robust cybersecurity protocols should be at the forefront in 2017.

## The Government Is Taking More Aggressive Steps to Prevent Cyberattacks, Both Offensive and Defensive

The U.S. Senate Committee on Homeland Security and Governmental Affairs recently heard testimony that the government is not doing enough to stop cyberattacks, both by private hacker groups and by other nation-states.<sup>10</sup> One view is that the government's strategy of shining a spotlight on companies that suffer cyberattacks, without also seeking to prosecute the offenders who committed the cyberattacks, was akin to blaming the victim. Another view is that the government should focus its energy on doing the things that corporate America cannot do—such as filing criminal charges or retaliating against foreign powers that sponsor hackers.

Also, President Trump recently signed an executive order designed to fortify the cybersecurity of the federal government by mandating that the government's information technology follow the "Framework for Improving Critical Infrastructure Cybersecurity," which was developed by the National Institute of Standards and Technology.<sup>11</sup> While the order applies only to the federal executive branch, some consider it to be a positive first step for more robust cybersecurity technology.<sup>12</sup> But, the new measures in the executive order are already being criticized for

being insufficient.<sup>13</sup> The takeaway is that, although the federal government is improving its own cybersecurity, even those measures may not be enough, and the measures do not extend to the private sector. It remains to be seen whether the government changes its strategy as to investigating and prosecuting cybercriminals in its effort to protect businesses.

## Companies Need to Take Action Now

While the federal government is making overtures toward protecting companies, financial institutions, and individuals from cyberattacks, any new measures will take time to implement and prove effective. Thus, the onus remains on companies and employees to work with their internal information security team, outside counsel, and security consultants to ensure that they are not only in compliance with governing regulations, but that they have also put themselves in the best position to defend against a cyberattack and respond if they find themselves the victim of one.

Regardless of industry, it is critical that companies assess and address data security risks and ensure compliance with applicable regulations, particularly in light of increased focus by regulators. Implementing robust cybersecurity protocols should be at the forefront in 2017. □ — ©2017 BLANK ROME LLP

1. Allison Grande, "Global Cyberattack Exposes Big Liabilities for Simple Fixes," *Law360* (May 14, 2017, 4:55 PM), <http://www.law360.com/privacy/articles/923818/global-cyberattack-exposes-big-liabilities-for-simple-fixes>.
2. *Id.*
3. Harriet Taylor, "An Inside Look at What's Driving the Hacking Economy," *CNBC* (Feb. 5, 2016, 10:02 AM), <http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html>.
4. Steve Morgan, "Cyber Crime Costs Projected to Reach \$2 Trillion by 2019," *Forbes* (Jan. 17, 2016, 11:01 AM), <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#23a224e3bb0c>.
5. Jimmy Hoover, "AT&T, Cisco Leaders Warn of Privacy, Safety Threats," *Law360* (Apr. 27, 2017, 1:49 PM), <http://www.law360.com/technology/articles/918076/at-t-cisco-leaders-warn-of-privacy-safety-threats>.
6. James E. Lee, "Will New Cybersecurity Legislation Offer Better Protection for Consumers?", *Infosecurity Magazine* (May 9, 2017), <http://www.infosecurity-magazine.com/opinions/will-new-cybersecurity-legislation/>.
7. Press Release, *Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions From Cyber-Attacks to Take Effect March 1*, Department of Financial Services (Feb. 16, 2017), <http://www.dfs.ny.gov/about/press/pr1702161.htm>.
8. See, e.g., Clarke Cummings, et al., "Cyber: New York Regulator Moves the Goalposts," *Financial Crimes Observer* (Sept. 2016), <http://www.pwc.com/us/en/financial-services-financial-crimes/publications/assets/NY-DFS-proposes-cybersecurity-regulations.pdf>.
9. Jimmy Hoover, "SEC Suits over Cyber Reporting Could Be on Horizon," *Law360* (Apr. 20, 2017, 1:25 PM), <http://www.law360.com/privacy/articles/915377/sec-suits-over-cyber-reporting-could-be-on-horizon>.
10. Allison Grande, "Feds Need to Dial up Cyberattack Responses, Senate Told," *Law360* (May 10, 2017, 10:22 PM), <http://www.law360.com/privacy/articles/922140/feds-need-to-dial-up-cyberattack-responses-senate-told>.
11. Alfred Ng, "Trump's Cybersecurity Order: Out with 'Antiquated Systems,'" *CNet* (May 11, 2017, 1:11 PM), <http://www.cnet.com/news/president-trump-signs-cybersecurity-executive-order/>.
12. Bob Ackerman, "Trump's Cybersecurity Executive Order is a Good First Step," *TechCrunch* (May 13, 2017), <http://techcrunch.com/2017/05/13/trumps-cybersecurity-executive-order-is-a-good-first-step/>.
13. *Id.*

JUNE 27, 2017

## PRESS RELEASE

### **Mark M. Lee Joins Blank Rome as Partner in White Collar Defense & Investigations Group**

Blank Rome LLP is pleased to announce that [Mark M. Lee](#) has joined the Firm as a Partner in the White Collar Defense & Investigations practice in the Philadelphia office. He joins from Schnader Harrison Segal & Lewis LLP where he was chair of the firm's white collar defense and corporate investigations practice group.

Formerly an Assistant United States Attorney ("AUSA") for the District of Delaware, Mr. Lee has a traditional white collar defense practice, counseling his clients on everything from pre-indictment negotiations to plea negotiations and trials. He assists both private and public sector entities in internal investigations, and offers them compliance counseling. Mr. Lee regularly acts as an interface between his clients—both businesses and individuals—and the government agencies with which they come into contact.

"We are very excited to welcome Mark to the Firm," said [Alan J. Hoffman](#), Chairman and Managing Partner. "Mark has built a highly regarded practice and he is well-respected in the legal and business communities. Several of us at Blank Rome have known Mark for a number of years and I'm confident that his approachability and eagerness to collaborate across practices will further enhance our white collar group."

As an AUSA, Mr. Lee organized and directed complex investigations. He has managed federal grand jury investigations and white collar criminal prosecutions in a wide variety of matters, including money laundering, public corruption, tax evasion, financial institution and mortgage fraud, and theft of identity, ERISA, and government funds. He has tried cases before the United States District Court for the District of Delaware and the United States District Court for the Eastern District of Pennsylvania, and has successfully filed nine appellate briefs before the Third Circuit Court of Appeals. Notably, Mr. Lee recently defended a sitting U.S. congressman on multiple criminal charges, such as RICO, bank fraud, wire fraud, bribery, obstruction of justice, and money laundering.



**Mark M. Lee**  
**Partner**

One Logan Square  
130 North 18th Street  
Philadelphia, PA 19103-6998  
v. +1.215.569.5536  
f. +1.215.754.4316

[MMLee@BlankRome.com](mailto:MMLee@BlankRome.com)  
[Download VCard](#)  
[View web profile](#)

*(continued on page 7)*

**Mark M. Lee Joins Blank Rome as Partner in  
White Collar Defense & Investigations Group (continued)**

Additionally, Mr. Lee has directed several federal investigations involving various technologies, including peer-to-peer software applications, social networking websites, and wireless and mobile networks and devices. His background also includes digital and computer forensic investigations.

"At his core, Mark is a problem solver," said [Shawn M. Wright](#), Co-Chair of the White Collar Defense & Investigations practice. "Whether at trial or in negotiations, Mark is a relentless advocate for clients, consulting with the respective agency or prosecutorial authority and resolving compliance issues under government scrutiny. Our group and our clients will undoubtedly benefit from Mark's experience and perspective. We're thrilled to have him on the team."

In addition to his white collar practice, Mr. Lee also advises clients on matters concerning cybersecurity and data privacy, including assessments of policies and procedures, data breach preparation, and breach response and remediation.

"Blank Rome's white collar defense & investigations practice group has a deep bench of exceptional attorneys," said Mr. Lee. "I look forward to collaborating with attorneys across the Firm's practices and offices to service my existing clients and strategically expand my practice. This is a perfect fit."

Outside of his legal practice, Mr. Lee is a mentor to the youth in his community and serves on the Board of Directors of the National Black Child Development Institute. Mr. Lee's pro bono and community investment activities center on education. For example, during his time as an AUSA, Mr. Lee coached a high school mock trial team in Delaware.

Mr. Lee earned his J.D. from Temple University Beasley School of Law, and his B.A. from the University of North Carolina at Chapel Hill.



## FCPA under the New Administration

BY MAYLING C. BLANCO, CARLOS F. ORTIZ, SHAWN M. WRIGHT,  
AND ARIEL S. GLASNER



**The single most frequently asked question** by our international clients over the past several months is whether there will be changes in white collar prosecution priorities under the new administration, specifically with respect to the Foreign Corrupt Practices Act (“FCPA”). The FCPA, which criminalizes the payment of bribes to foreign officials around the world, has been subject to enforcement trends and scrutiny during its 40-year history. Prior to 2005, there were few notable prosecutions. However, over the past 12 years, the law has garnered much attention given the unparalleled increase in the number of prosecutions and the headline-grabbing monetary amounts of the settlements. This trend has straddled administrations from both sides of the aisle.

Of course, it is nearly impossible to answer the question posed directly with any degree of certainty. Venturing to do so would require reading tea leaves. However, there are certain indicia and reasoning that can guide our understanding of the direction that the new administration may be heading in.

### The Tone from the Top

For months, many doubted whether the new Attorney General for the Department of Justice (“DOJ” or the “Department”), Jeff Sessions, would abandon the prosecution of white collar crimes, such as the FCPA, in favor of other crimes—drugs, immigration, violent crimes—that formed a central role in the election rhetoric. This public perception was not lost on the attorney general, and he laid that fear to rest with his remarks at the Ethics and Compliance Initiative’s Annual

Conference on April 24, 2017. Attorney General Sessions stated that he wanted “to make clear ... that under [his] leadership, the Department of Justice remain[ed] committed to enforcing all the laws. That includes laws regarding corporate misconduct, fraud, foreign corruption, and other types of white-collar crime.” He acknowledged that this would be the case, despite his efforts to strengthen the DOJ’s focus on traditional crimes.

The attorney general went on to specifically identify FCPA enforcement efforts as “critical” to the Department. He recognized that corruption in the form of bribes to foreign officials “harms free competition, distorts prices, and often leads to substandard products and services coming into this country.” He further noted that it “increases the cost of doing business, and hurts honest companies that don’t pay these bribes.” He stated that he “wants to create an even playing field for law-abiding companies[,]” which “should succeed because they provide superior products and services, not because they have paid off the right people.” To this end, he declared that the DOJ “will continue to strongly enforce the FCPA and other anti-corruption laws.”

The attorney general also made clear that the prosecutorial approach in pursuing FCPA matters would not deviate in any major way with that of his predecessors, in at least two respects.



First, the DOJ will continue to emphasize the importance of holding individuals accountable for misconduct. In other words, prosecutors will continue adhering to what is commonly known as the “Yates Memo” and, towards that end, will continue to work with international law enforcement to prosecute individuals.

Second, the DOJ will continue to consider some of the same previously identified factors when making charging decisions. These factors include evaluating the quality of a company's compliance program and valuing companies that choose to do the right thing on their own accord. In determining the appropriate fines to impose, these factors include taking into account the company's efforts to self-disclose, cooperate, and accept responsibility. In all, Attorney General Sessions confirmed that there would be no major departures from the way the prior administration pursued FCPA matters. Indeed, it will be interesting to see how prosecutors will apply the recently issued "Sessions Memo"—requiring prosecutors to pursue the most "readily provable" offense—to FCPA matters. (For more information, see [article](#) on page 11.)

Any doubts of the DOJ's commitment should have been dispelled by the statements of the Acting Principal Deputy Assistant Attorney General, Trevor N. McFadden. At two compliance-related events, he made efforts to "dispel [the] myth" surrounding white collar prosecuting priorities. McFadden unequivocally

- Finally, the DOJ has publicized that international law enforcement cooperation is increasing. Not only does this cooperation make it more likely that wrongful conduct will come to the attention of U.S. authorities, but it also facilitates investigations and prosecutions. FCPA violations are becoming low-hanging fruit for the DOJ.

declared that the Department "continues to vigorously enforce the FCPA...motivated as ever by the importance of ensuring a fair playing field for honest corporations."

The appointment of Jay Clayton to head the Securities and Exchange Commission ("SEC") has not yet resulted in as clear a mandate. Mr. Clayton is a well-respected Wall Street lawyer and is no stranger to the FCPA. In 2010, he was involved in representing ENI, S.p.A., an Italian oil group, in settling a FCPA matter with the SEC.<sup>1</sup> On the other hand, Mr. Clayton also publicly expressed reservations on the law. In 2011, he assisted in drafting an article for the New York City Bar Association, "The FCPA and Its Impact on International Business Transactions: Should Anything Be Done to Minimize the Consequences of the U.S.'s Unique Position on Combating Offshore Corruption?" The article noted

that companies have become increasingly wary of purchasing businesses with potential costly liabilities due to FCPA violations. The article further noted that companies not subject to the law's reach have reservations about entering into transactions that would bring the company within the FCPA's jurisdictional reach. Mr. Clayton has not made any recent public statements regarding the FCPA, and it is difficult to say how these six-year-old views may impact his policies as chairman.

### Money Talks and Pro-America

Last year was a near record-setting year for the FCPA, both in terms of number of actions brought and total dollar amounts secured through settlements. In 2016, there were 29 SEC and 25 DOJ enforcement actions.<sup>2</sup> Only 2010 was more prolific, with 33 DOJ and 23 SEC enforcement matters.<sup>3</sup> Also in 2016, over \$2.4 billion was paid in fines and penalties for FCPA violations.<sup>4</sup> The total amount of sanctions recovered was slightly greater, at \$2.6 billion, in 2008.<sup>5</sup> Numbers like these are difficult for anyone to ignore.

The FCPA also may be more aligned in certain respects with the new administration's agenda. The law has a broad jurisdictional reach, and businesses, including foreign businesses, that fall within its jurisdiction must conduct business by the same ethical standards as U.S. companies. Indeed, all but one of the top FCPA settlements have been with non-U.S. corporations.<sup>6</sup> FCPA penalties paid by foreign companies have been significantly higher than those paid by U.S. companies.<sup>7</sup> This data suggests that foreign companies bear a higher FCPA-enforcement burden than their American counterparts.

### Wheels Set in Motion

Over the past few years, the DOJ has taken steps that will continue to encourage and increase FCPA prosecutions. First, the Fraud Section's one-year "Pilot Program" has been extended. (See our previous Blank Rome white collar advisory on this program [here](#).) The program is intended to motivate companies and individuals to voluntarily disclose their FCPA violations. McFadden has announced that the "program will continue in full force" pending "a final decision regarding its permanence."

Second, the size of the FCPA Unit has significantly increased in the past several years. After the announcement of the Pilot Program, in April 2016, the Fraud Unit doubled the size of its FCPA-dedicated prosecutors and created teams of special FBI agents focused solely on FCPA matters. Those agents, McFadden

confirmed, are working on “numerous significant investigations.” Additional resources are provided by the U.S. Attorney’s Offices across the country, which are actively working on these cases alongside the Fraud Unit.

Third, more so now than ever before, FCPA enforcement has led to a growing, global wave of anti-corruption laws. Mexico and France have recently instituted anti-bribery systems and have pledged to root out offenders. Even though some of these countries’ laws and enforcement systems are in their infancy, international cooperation among foreign prosecutorial authorities makes it more likely that corrupt activity will come to the attention of U.S. prosecutors.

Finally, the DOJ has publicized that international law enforcement

cooperation is increasing. Not only does this cooperation make it more likely that wrongful conduct will come to the attention of U.S. authorities, but it also facilitates investigations and prosecutions. FCPA violations are becoming low-hanging fruit for the DOJ.

### More Than Tea Leaves

Despite the new administration’s focus on prosecution of domestic crime, the DOJ remains heavily invested in the aggressive prosecution of FCPA violations on both the corporate and individual levels, and corporations must ensure that their compliance programs and measures are active and effective. □ — ©2017 BLANK ROME LLP

1. See <http://www.marketwatch.com/story/new-sec-chief-may-have-interest-in-reforming-foreign-bribery-enforcement-2017-01-04>.
2. See <http://fcpa.stanford.edu/statistics-analytics.html>.
3. *Id.*
4. See <http://fcpa.stanford.edu/chart-penalties.html>.
5. *Id.*
6. See <http://fcpa.stanford.edu/statistics-top-ten.html>.
7. See <http://www.fcpablog.com/blog/2015/1/23/paper-the-fcpa-is-a-new-international-business-tax-on-non-us.html>.



### Chambers USA 2017 Recognizes Blank Rome White Collar Defense & Investigations Attorneys



BARRY W. LEVINE

PARTNER



CARLOS F. ORTIZ

PARTNER



HENRY F. SCHUELKE III

PARTNER

**Blank Rome is pleased to announce** that *Chambers USA* 2017 recognized the following members of the Firm’s white collar defense and investigations group as “leaders in their fields” in the area of “Litigation: White Collar Crime and Government Investigations.”

In addition to Blank Rome’s white collar defense and investigations attorneys, the Firm and its attorneys were proud to receive numerous high-level rankings in a number of practice areas.

To view all of Blank Rome’s *Chambers USA* 2017 rankings, please visit [www.blankrome.com/chambersusa2017](http://www.blankrome.com/chambersusa2017).

Chambers USA assesses its annual rankings according to technical legal ability, professional conduct, client service, commercial astuteness, diligence, commitment, and other qualities most valued by clients.

## The Sessions Memo: A Significant Reversal of Policy?

BY NICHOLAS C. HARBIST AND MELISSA FUNDORA MURPHY



In May 2017, Attorney General Jeff Sessions issued a memorandum to U.S. attorneys, ordering all federal prosecutors to “charge and pursue the most serious, readily provable offense” as a “core principle” of charging and sentencing policy. The memorandum defines the most serious offenses as “those that carry the most substantial guidelines sentence, including mandatory minimum sentences.”

This policy represents a significant reversal of the comparatively lenient stance established by Eric Holder, one of Sessions’ predecessors under President Barack Obama, who had ordered federal prosecutors in 2013 to refrain from charging defendants with certain offenses that could see long mandatory minimum sentences.

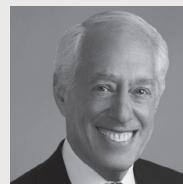
Prosecutors will now be expected to recommend a sentence within federal guidelines when before a federal judge, and must disclose to the sentencing court all of the facts that impact the sentencing guidelines or mandatory minimum sentences. Recommendations outside of the guidelines will require a documented explanation, as well as approval from a U.S. attorney, assistant attorney general, or a designated supervisor. Deviations from the “core principle” of pursuing the most serious offenses will only be granted if “justified by unusual facts.”

Attorney General Sessions made it clear that he wants this shift in policy to be immediate, noting that “[a]ny inconsistent previous policy of the Department of Justice relating to these matters is rescinded, effective today.” □ — ©2017 BLANK ROME LLP



### Who's Who Legal 2017 Recognizes Blank Rome White Collar & Investigations Attorneys

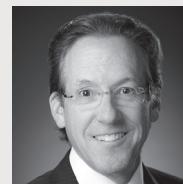
Blank Rome is pleased to announce that Who's Who Legal 2017 recognized the following Blank Rome white collar defense and investigations attorneys in the area of “Business Crime Defence.”



BARRY W. LEVINE  
 PARTNER



HENRY F. SCHUELKE III  
 PARTNER



LAURENCE S. SHTASEL  
 PARTNER



LAWRENCE H. WECHSLER  
 PARTNER

In addition to the Firm’s white collar defense and investigations attorney rankings, numerous other Blank Rome attorneys in eight practice areas were recognized by Who's Who Legal.

To view all of Blank Rome’s Who's Who Legal 2017 rankings, please click [here](#).

Nominees were selected by Who's Who Legal based upon comprehensive, independent survey work with both general counsel and private practice lawyers worldwide. Only professionals who have met independent international research criteria are listed in the annual survey.

## Record-Setting Prosecutions in the Money Transmitting Business: Ways to Avoid Compliance Violations

BY MAYLING C. BLANCO AND D. MORGAN BARRY



MAYLING C. BLANCO

D. MORGAN BARRY

PARTNER

ASSOCIATE

**In the first several months of 2017, we have seen significant** anti-money laundering settlements and penalties in the money transmitting business arising from lax compliance programs, including the record-setting Western Union settlement and the various individuals facing personal exposure. From each of these there are lessons to be drawn.

### The \$586M Western Union Settlement

On January 19, 2017, Western Union agreed to a \$586 million forfeiture, the largest ever imposed on a money services business.

According to the deferred prosecution agreement,<sup>1</sup> Western Union violated reporting and compliance obligations mandated by the Bank Secrecy Act ("BSA"), which is sometimes referred to as an anti-money laundering law ("AML") or jointly as "BSA/AML." 31 U.S.C. §§ 5311-30. The steep penalty for compliance and reporting lapses may be attributable to the fact that, as Acting Assistant Attorney General David Bitkower observed, "Wiring money can be the fastest way to send it—directly into the pockets of criminals and scam artists."<sup>2</sup>

Specifically, Western Union violated BSA/AML provisions requiring all domestic financial institutions to implement an effective anti-money laundering compliance program. Part of the required compliance includes the mandatory submission of certain reports, such as Currency Transaction Reports for transactions over \$10,000 (or multiple transactions that amount to over \$10,000) and Suspicious Activity Reports ("SARs") for transactions that may violate a law or regulation.

Western Union's failure to maintain sufficient anti-money laundering measures enabled its agents to defraud thousands of U.S. residents between 2004 and 2012. The various fraudulent

schemes induced victims to wire money through false promises of lottery winnings or large cash prizes; sham offerings of "high-ticket" items at greatly discounted prices; fake employment opportunities, such as "secret shoppers"; and fictitious relatives in need of money. The fraudulent and unlawful activities reached into the company's international operations, most notably in the United Kingdom and China. According to the Department of Justice ("DOJ"), a substantial portion of this money had ties to human smugglers.

While Western Union's Corporate Security Department recommended guidelines for countering money laundering, Western Union failed to implement these proposed guidelines. According to the DOJ, execution of the proposed guidelines would have "prevented significant fraud losses to victims and would have resulted in corrective action against more than 2,000 agents worldwide between 2004 and 2012."

### Inadequate BSA/AML Compliance Results in Individual Liability

Similar to the circumstances surrounding the Western Union settlement, MoneyGram International Inc. entered into a deferred prosecution agreement in late 2012, forfeiting \$100 million. Four-and-a-half years later, penalties from MoneyGram's inadequate anti-money laundering compliance are still materializing, most recently with the guilty plea of one of its and Western Union's former agents. This could be at least in part because of the DOJ's mandate, commonly known as the Yates Memo, to hold individuals and not just corporations accountable.

On May 9, 2017, the former agent pled guilty to defrauding thousands of victims out of approximately \$4.4 million through mass-marketing fraud schemes.<sup>3</sup> According to the indictment, the former agent conspired with a group of complicit agents. These former agents engaged in mass-marketing fraud by processing fraudulently induced money transfers, while allowing themselves to retain up to 10 percent for their role in the schemes.

The former agent faces imprisonment of up to 20 years for each count and a \$250,000 fine for his role in the schemes.

### Six Ways to Reduce Exposure

These cases present examples of how important it is for financial institutions to understand their areas of risk and have real and fully executed compliance programs that address and combat these risks. At the outset, companies involved in any way in the transmission of currency should familiarize themselves with the expansive definition of "financial institutions" under the BSA/AML,

which, while including traditional entities such as commercial banks, also may include less conventional entities, such as pawnbrokers, travel agencies, travelers check cashiers, jewel dealers, and car dealerships.

Businesses whose cash transactions may have a high degree of usefulness in criminal, tax, or regulatory matters should contemplate the following suggestions as ways to assist in reducing the risk of violations:

- consider whether their business has been designated as one that is subject to the BSA/AML;
- ensure that they have executed a compliance program that appropriately takes into consideration the business' risk areas;

- understand the triggering obligations for filing SARs and have systems in place to help expose transactions structured in a manner to evade detection;
- designate personnel responsible for day-to-day compliance and to stay abreast of any suspicious activity report trends;
- provide regular training for appropriate personnel, including agents where appropriate; and
- create a hotline for the reporting of suspicious activity.

These measures can assist in avoiding serious violations and in mitigating the potentially hefty fines, should a violation be uncovered. □ —©2017 BLANK ROME LLP

1. Western Union's deferred prosecution agreement can be accessed through the DOJ's website: <http://www.justice.gov/opa/press-release/file/938371/download>.
2. Press Release, *Western Union Admits Anti-Money Laundering and Consumer Fraud Violations, Forfeits \$586 Million in Settlement with Justice Department and Federal Trade Commission*, Department of Justice (Jan. 19, 2017), available at <http://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million>.
3. Press Release, *Former Canadian MoneyGram and Western Union Agent Pleads Guilty to \$4.4 Million Fraud Scheme*, Department of Justice (May 9, 2017), available at <http://www.justice.gov/usao-mdpa/pr/former-canadian-moneygram-and-western-union-agent-pleads-guilty-44-million-fraud-scheme>.

## Recent Speaking Engagements



**NICHOLAS C. HARBIST**  
PARTNER

**Nicholas C. Harbist:** The Perils of Dealing with Whistleblowers under the False Claims Act at the Seton Hall Law U.S. Healthcare Compliance Certification Program, June 12, 2017, in Newark, NJ.



**JOSEPH G. POLUKA**  
PARTNER

**Joseph G. Poluka and Jed M. Silversmith:** AML, KYC, and Conflict Minerals: Current Issues at the International Precious Metals Institute's Annual Conference, June 12, 2017, in Orlando, FL.



**SHAWN M. WRIGHT**  
PARTNER

**Shawn M. Wright:** Yes! You Can Have It All at the Prince George's County Economic Development Corporation Women's Excellence & Leadership Luncheon, June 8, 2017, in Oxon Hill, MD.



**JED M. SILVERSMITH**  
OF COUNSEL

JULY 10, 2017

## PRESS RELEASE

### Jane F. Barrett Joins Blank Rome as Of Counsel in White Collar Defense & Investigations Group

Blank Rome LLP is pleased to announce that [Jane F. Barrett](#) has rejoined the Firm's Washington, D.C., office as Of Counsel in the [White Collar Defense & Investigations](#) group, which recently [welcomed](#) Partner [Mark M. Lee](#) to the Firm's Philadelphia office.

Ms. Barrett rejoins Blank Rome after serving as a professor and the director of the Environmental Law Clinic at the University of Maryland Carey School of Law. She taught students administrative and environmental law, ethics, civil procedure, and trial and appellate advocacy through clinical casework. She was also actively engaged with the Maryland NGO community on a wide variety of environmental policy issues while focusing her research on environmental and worker safety enforcement.

We are very excited to have Jane rejoin our white collar practice group and the Firm," stated [Shawn M. Wright](#) and [Carlos F. Ortiz](#), Partners and Chairs of the White Collar Defense & Investigations group. "She is a highly respected white collar practitioner, and we look forward to her immediate contribution to the significant work we do for our clients.

At Blank Rome, Ms. Barrett provides strategic advice to clients confronted by government investigations, whistleblower allegations, and other legal crises in a range of substantive areas. A former federal and state prosecutor, she has extensive criminal jury trial experience and has successfully argued numerous appellate cases. Her private practice clients include companies and individuals throughout the United States involving diverse industries and legal issues. Her experience includes representing clients in federal and state criminal cases involving environmental crimes, securities fraud, bribery, racketeering, kickbacks, healthcare fraud, and government contract and program fraud.

Ms. Barret first joined Blank Rome in 2003 as part of the Firm's notable combination with Dyer Ellis & Joseph, where she served as chair of the firm's white collar and government investigations group, a role that she continued at Blank Rome. Her practice focused on complex criminal and civil litigation and corporate internal investigations, and she worked extensively with clients in the oil and gas, chemical, financial services, and maritime industries. Prior to her private practice, Ms. Barrett served for 11 years as an assistant U.S. attorney ("AUSA") in Maryland where she prosecuted high-profile fraud, public corruption, bribery, racketeering, and environmental criminal cases. She was also an assistant attorney general for the State of Maryland where she was responsible for developing and supervising the prosecution of criminal violations of state environmental laws. Her environmental experience began as an attorney-adviser for the U.S. Environmental Protection Agency's Office of Water Enforcement.

Admitted to practice in Maryland, Ms. Barrett received her J.D. from the University of Maryland School of Law, and her B.A. in Political Science from Loyola College. She is a member of many professional associations, including the American Bar Association, Federal Bar Association for the District of Maryland, Women's Criminal Defense Association, National Association of Women Lawyers, and National Association of Criminal Defense Lawyers. Ms. Barrett is a prolific author, speaker, and adviser on environmental crimes, corporate accountability, and compliance, as well as clinical legal education issues.



**Jane F. Barrett**  
Of Counsel

1825 Eye Street NW  
Washington, DC 20006  
v. +1.202.420.2570  
f. +1.202.379.9316

[JBarrett@BlankRome.com](mailto:JBarrett@BlankRome.com)  
[Download VCard](#)  
[View web profile](#)

## Overview of IRS Penalties for Individuals with Foreign Bank Accounts and Investments

BY JEFFREY M. ROSENFELD AND JED M. SILVERSMITH



JEFFREY M. ROSENFELD

JED M. SILVERSMITH

ASSOCIATE

OF COUNSEL

### Earlier this spring, the Internal Revenue Service (“IRS”) Large Business and International Division

identified several “campaigns” or areas where it plans to focus its audit resources. One campaign involved taxpayers who opted out of the Offshore Voluntary Disclosure Program (“OVDP”).

### IRS Campaign Background

The OVDP is a program whereby U.S. persons who have offshore assets may voluntarily disclose unreported income and/or offshore assets to the IRS. Under the program, taxpayers apply for pre-clearance, meaning that the IRS will cross-check applicants' names with a list of individuals who are under audit, subjects of criminal investigations, or in other situations. Applicants for whom the cross-checks reveal that there are no such open audits, criminal investigations, or other situations are then pre-cleared to make a voluntary disclosure, while applicants who are the subject of an open audit, criminal investigation, or other situations are denied pre-clearance. Taxpayers who receive pre-clearance then file, among other documents (which may be voluminous), amended tax returns (or original tax returns); pay the requisite tax, interest, and accuracy-related penalties; and in addition, pay a miscellaneous penalty equal to 27.5 percent (or in some cases, 50 percent) of the balance of the undisclosed offshore assets. Taxpayers who do not have unreported income and do not owe back taxes may enter into other compliance programs with less significant penalties.

In some cases, taxpayers, after being accepted into the OVDP, have second thoughts about resolving their matter through such a program, and instead withdraw from the OVDP. In such a case, the taxpayer is simply attempting to resolve their outstanding tax issues outside of the OVDP (which typically involves a formal audit). The IRS campaign suggests that these individuals, as well as individuals who are denied pre-clearance from the outset, will be subject to heightened scrutiny.

### IRS Forms and Penalties Likely to Be the Focus of the IRS Campaign

As part of the campaign, it is likely that the IRS will be focusing on the assertion of penalties for failing to file certain information returns with respect to foreign assets, including the forms that are set forth below. An audit that focuses on the failure to file, or incomplete filing, of these returns can result in draconian civil and criminal penalties. Further, the IRS may be able to assert that the statute of limitations with respect to a tax return (*i.e.*, the period of time during which the IRS is legally permitted to assess additional tax or assert penalties with respect to a filed tax return) continues to remain open until these forms are filed.

- ▶ An audit that focuses on the failure to file, or incomplete filing, of these returns can result in draconian civil and criminal penalties.

Here are some of the most common forms likely to be the subject of the IRS campaign, a description of the taxpayers required to file them, and a general overview of the penalties that may be asserted.

- **FinCEN Form 114. *Foreign Bank Account Report (“FBAR”)*** *Form.* U.S. persons are required to file a FinCEN Form 114 if (1) the U.S. person had a financial interest in or signature authority over at least one financial account located outside of the United States; and (2) the aggregate value of all foreign financial accounts exceeded \$10,000 at any time during the calendar year reported. The term “financial account” includes bank accounts such as savings accounts, checking accounts, and time deposits; securities accounts such as brokerage accounts; commodity futures accounts; insurance policies with a cash value (such as a whole life insurance policy); and mutual funds or similar pooled funds. “Financial interest” includes the owner of record, as well as agents, nominees, closely held corporations, and “owners” of trusts. Thus, if an individual has a power of attorney over a foreign account held in the name of a parent, that individual would have a FBAR filing requirement. Similarly, the FinCEN Form requires that an individual with a 50-percent ownership in an entity report that company’s foreign bank accounts.

The penalty for failure to file a FBAR is \$10,000, if the failure to file was non-willful. However, if the IRS deems the taxpayer's failure to file to be willful, it may impose a penalty of up to 50 percent of the balance of the account (or, if higher, \$100,000 for such an account).

■ **IRS Form 8938.** *Statement of Specified Foreign Financial Assets.* The IRS requires that "specified individuals" who file tax returns also file a Form 8938, if they have foreign assets with an aggregate balance of more than \$50,000. The Form 8938 is filed in addition to the FinCEN Form 114, even though both forms collect similar (or, in many cases, identical) information.

The Form 8938 looks at a broader category of assets, including foreign stock and partnership interests. However, the taxpayer does not need to report bank accounts for which he simply possesses signatory authority. The penalty for failing to file a Form 8938 is up to \$10,000, with an additional \$10,000 for each 30 days of non-filing after the IRS notice, for a potential maximum penalty of \$60,000. But, perhaps most importantly, the taxpayer's entire tax return remains subject to audit, irrespective of any statute of limitations, until a Form 8938 is filed—only then does the three-year statute of limitations begin to run.

■ **IRS Forms 3520 and 3520-A.** *Annual Return to Report Transactions with Foreign Trusts and Receipt of Certain Foreign Gifts and Annual Information Return of Foreign Trust with a U.S. Owner.* These forms generally apply to taxpayers who receive foreign gifts or who have an interest in an offshore trust. First, the Form 3520 must be filed by any U.S. person who receives either \$100,000 from a foreign individual or a foreign trust, or a gift from a foreign corporation or partnership over \$15,671. A Form 3520 must be filed even if the gifts are not taxable. Failure to file the form can trigger a penalty of up to 35 percent of the value of the transfer. If a U.S. person is deemed to be the owner of a foreign trust, then the foreign trust must file a Form 3520-A. If the foreign trust fails to file the Form 3520-A, then the IRS can assess a penalty of up to five percent of the value of the

foreign trust's corpus. There is no statute of limitations for the IRS to assess penalties on unfiled Forms 3520 and 3520-A. Thus, a trust that has not filed for many years could be assessed with multiple five-percent penalties.

■ **IRS Form 5471.** *Information Return of U.S. Persons with Respect to Certain Foreign Corporations.* There are a number of scenarios in which a U.S. person is required to file this return. Generally, the filing requirement is triggered if the U.S. person owns 10 percent or more of stock in a foreign company. The form is required to be filed irrespective of any tax liability. The penalty regime is the same as the Form



8938. The taxpayer's entire tax return potentially remains subject to audit, irrespective of any statute of limitations, until a Form 5471 is filed—only then does the three-year statute of limitations begin to run.

## Conclusion

The aforementioned forms are just a sample of some of the most commonly filed forms for reporting foreign assets, but there are several others that may be applicable, depending on the facts and circumstances. Often, due to the complexity of the foreign reporting rules, there will be situations where either a taxpayer is non-compliant with respect to foreign asset reporting or needs an analysis as to the scope of the full reporting requirement related to a particular foreign asset or transaction. In these cases, sophisticated counsel should be retained in order to navigate this complex area of the tax law. Blank Rome has handled hundreds of matters concerning foreign asset reporting and has [significant experience](#) in this area. □ — ©2017 BLANK ROME LLP

## Blowing the Whistle: Employers Must Properly Respond to Employee Allegations of Wrongdoing

BY NICHOLAS C. HARBIST AND LAUREN E. O'DONNELL



NICHOLAS C. HARBIST

LAUREN E. O'DONNELL

PARTNER

ASSOCIATE

The Occupational Safety and Health Administration's ("OSHA") Whistleblower Protection Program enforces the whistleblower provisions of 22 statutes protecting employees who report violations of various federal laws.

Examples of the types of conduct that these laws protect include (1) participating in safety and health activities; (2) reporting a work-related injury or fatality; or (3) reporting a statutory violation. Employers are prohibited from discriminating against their employees for exercising such rights, and the prohibited conduct is retaliation against the employee for engaging in protected whistleblowing activity.<sup>1</sup>

Similarly, under the False Claims Act, any employee who is discharged, demoted, harassed, or otherwise discriminated against because of lawful acts in furtherance of an action under the act, is entitled to all relief necessary to make the employee whole, which may include reinstatement, double back pay, and compensation for special damages like litigation costs and attorneys' fees.<sup>2</sup>



### Recent OSHA Developments and Activities

Earlier this year, OSHA issued an advisory, *Recommended Practices for Anti-Retaliation Programs*, for public and private sector employers covered by the 22 whistleblower protection laws that it enforces. It outlines five elements of an effective anti-retaliation program: (1) management leadership, commitment, and accountability; (2) a system for listening to and resolving employees' concerns; (3) a system for receiving and responding to reports of retaliation; (4) anti-retaliation training; and (5) program oversight.

Employees who believe in good faith that they have been retaliated against can file a complaint with the secretary of labor to request an OSHA investigation. OSHA also reviews settlement agreements between complainants and their employers to ensure that they are knowing, voluntary, fair, and in the public interest. In August 2016, OSHA issued updated criteria to evaluate whether settlement agreements impermissibly restrict or discourage protected activity. OSHA advised that it reserves the right not

to approve settlements with liquidated damages provisions.<sup>3</sup> Also, OSHA will not approve a "gag" provision that prohibits, restricts, or discourages protected activity, such as filing a complaint with a government agency, participating in an investigation, testifying in proceedings, or otherwise providing information to the government. In addition to the OSHA criteria, criminal statutes would likely prohibit such "gag" provisions, such as the Federal Blackmail Statute, 18 U.S.C. § 873, and New Jersey's prohibition against Compounding, N.J. STAT. ANN. § 2C:29-4.

In the past six months, OSHA has engaged in a number of whistleblower protection enforcement activities that should caution employers about how to respond to a whistleblower complaint.

Recently, in an April 2017 Sarbanes-Oxley Act ("SOX") whistleblower case, OSHA ordered Wells Fargo Bank N.A. to reinstate a whistleblower and compensate him approximately \$5.4 million in back pay, compensatory damages, and attorneys' fees. The whistleblower is a former bank manager who lost his job after reporting suspected fraudulent behavior. OSHA concluded that the former manager's whistleblower activity was protected under SOX (one of the 22 statutes that OSHA enforces) and was a contributing factor in his termination.

### Compliance Policies and Recommendations

To avoid costly enforcement actions, companies should have clear compliance policies requiring employees to report, in good faith, violations of law or policy, and companies must be prepared for whistleblower and retaliation complaints before any such complaints are received. Companies should consider using anonymous complaint and retaliation hotlines, as well as having written policies and procedures outlining the proper reporting chains for whistleblower complaints and allegations of retaliation. This will help route whistleblower and retaliation complaints to the appropriate individual(s) within a company to ensure that such allegations are handled properly.

Companies also should have clear policies in place explaining that employees will not be retaliated against for making good faith whistleblower complaints or engaging in any protected activity.

Anti-retaliation training should be conducted regularly. Further, companies should have a system to protect the employment status of a whistleblower or employee who engages in any protected activity from demotion, pay decreases, or termination until the complaint is fully investigated and found to be without merit.

- To avoid costly enforcement actions, companies should have clear compliance policies requiring employees to report, in good faith, violations of law or policy, and companies must be prepared for whistleblower and retaliation complaints before any such complaints are received.

Once a whistleblower complaint is received, employers must carefully investigate the complaint to mitigate the risk of enforcement action. Upon receipt of such a complaint, companies should begin an investigation into the merits of the complaint. Companies should seek legal advice and, if appropriate, hire independent outside counsel to conduct the investigation.

Given OSHA's recent focus on protecting whistleblowers and the costs that companies incur when faced with OSHA enforcement action, companies should promptly reevaluate their compliance policies and procedures for handling such protected activity. □

— ©2017 BLANK ROME LLP

1. States also have whistleblower protection laws. For example, the New Jersey Conscientious Employee Protection Act, N.J. STAT. ANN. §§ 34:19-1 – 34:19-8 ("CEPA"), prohibits all public and private employers from retaliating against employees who disclose, object to, or refuse to participate in certain actions that the employees reasonably believe are either illegal or in violation of public policy.
2. See 31 USC § 3730(h).
3. Liquidated damages are damages in a predetermined sum that the parties designate during the formation of a contract for the injured party to collect as compensation upon a specific breach.