BLANK ROME LLP
COUNSELORS AT LAW

DECEMBER 2017 • VOL 1, ISSUE 3

White Collar Watch

INSIDE

THIS ISSUE

A Note From The Editors

Welcome to the holiday edition of our *White Collar Watch*. This edition includes an article discussing IRS audit priorities, the third installment in our series on FCPA investigations, an article on new compliance requirements for UK businesses, and a new FinTech series article that discusses blockchain's impact on federal regulatory enforcement.

It has been a year of change in many ways, as we adjust to the new administration and new technologies that impact many of our clients' industries. 2018 likely promises yet more dramatic developments, and we will be ready to assist you in responding.

As we head into the final days of 2017, we want to wish all of you, and your families, the happiest and healthiest of holiday seasons.

JOSEPH G. POLUKA

PARTNER

INBAL P. GARRITY

PARTNER

WILLIAM B. SHIELDS

OF COUNSEL

EDITORS, *WHITE COLLAR WATCH*

The FinTech Revolution: The Impact of Blockchain Technology on Regulatory Enforcement

BY MICHELLE ANN GITLITZ, ARIEL S. GLASNER, AND BRIDGET MAYER BRIGGS



MICHELLE ANN GITLITZ — PARTNER
ARIEL S. GLASNER — ASSOCIATE
BRIDGET MAYER BRIGGS — ASSOCIATE

***This is the third installment in a series of articles. For more background on this topic, please read our first article in the series,* An Introduction to Financial Technology, *and our second article,* The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications.**

A bedrock of the FinTech revolution is blockchain technology—a digital, decentralized ledger of all transactions that take place across a peer-to-peer network of computers. The ledger is visible to anyone within the network, and permanently and securely records, in "blocks," the history of exchanges that takes place between the peers in the network. All the completed and authenticated transaction blocks are connected and "chained" from the beginning of the chain to the most current block—hence the name "blockchain." Most importantly, there is no need for a central authority to manage the blockchain because the blockchain records all transactions and the records are considered virtually impossible to modify or delete once entered.

This article considers the potential impact of blockchain technology on regulatory enforcement by examining its application in two different contexts: 1) as a verification tool, and 2) as the vehicle for cryptocurrencies. Whereas the former application promotes regulatory compliance and has the potential to *dramatically* reduce the costs of regulatory enforcement, the nature of cryptocurrencies and their capacity for preserving investors' anonymity greatly complicate regulators' ability to protect against unlawful conduct.

Blockchain Technology as a Promoter of Regulatory Compliance

Because blockchain technology offers the ability to preserve historical records and transactions, it has numerous applications in, among other areas: trade reporting, clearing, and confirmation; record keeping; financial and/or records auditing; due diligence; supply chain management; and contracting. For instance, the technology can be used to preserve records about an individual or company, including individuals' professional or medical records or individuals'/companies' financial records. Once the information has been preserved on a blockchain, the information can be automatically downloaded each time a computer, or "node," joins the network on which this information has been stored.

Blockchain technology also offers the ability for parties to enter into "smart contracts," which employ coding on a blockchain to define contract terms and execute automatically when specific terms or product deliveries are met. Likewise, blockchain technology can facilitate due diligence in connection with mergers, acquisitions, and third-party business arrangements. Thus, it could, for example, permit U.S. companies working with third-party vendors abroad to easily obtain certifications of compliance with provisions of the Foreign Corrupt Practices Act ("FCPA").

When used as a tool to preserve records, ensure compliance with contract terms, or to facilitate due diligence, blockchain technology has the potential to greatly improve regulatory efficiency by lowering costs and expediting the time that regulators or law enforcement authorities invest in ensuring legal compliance. Thus, regulators could use blockchain technology quickly and accurately to verify companies' fulfillment of applicable licensing or reporting requirements. Likewise, in cases where smart contract coding has been used to implement corporate compliance programs by automating certain events if compliance objectives are achieved (or violated), regulators/law enforcement authorities may have an improved ability to monitor the programs and assess their strength.

Cryptocurrencies and Initial Coin Offerings

Another principal application of blockchain technology is as the vehicle for cryptocurrencies. In contrast to fiat currencies, cryptocurrencies have no physical form, and all transactions are recorded in the blockchain. As such, they are not backed by any government or central bank. Moreover, the holders of cryptocurrencies—including those who transact in cryptocurrencies—maintain their anonymity through the blockchain network and by securing access to their cryptocurrency "wallet" through a private "key."

Preservation of cryptocurrency users' anonymity naturally heightens the risk of fraudulent transactions and greatly complicates the role of regulators seeking to identify perpetrators of unlawful conduct. Indeed, when individuals' identities are concealed, digital currency exchanges cannot comply with anti-money laundering ("AML") and know-your-customer ("KYC") reporting

requirements. In the United States, there has been conflicting guidance as to whether offerors of digital currency are subject to the federal Bank Secrecy Act ("BSA"), which sets forth AML and KYC reporting requirements. Nevertheless, the U.S. Treasury's Financial Crimes Enforcement Network ("FinCEN") has pursued civil enforcement actions against digital currency exchanges that it alleged failed to comply with the BSA as required.[1]

► There is no need for a central authority to manage the blockchain because the blockchain records all transactions and the records are considered virtually impossible to modify or delete once entered.

The issues facing cryptocurrency exchanges also extend to the sale of digital "tokens" or coins through Initial Coin Offerings ("ICOs"), which likewise take place on blockchain networks. ICOs permit companies to raise funds through the sale of tokens that can be redeemed for goods or services, or that can be resold for profit on a token exchange. While ICO issuers typically have access to investors' identifying information, they are not always subject to AML regulation. However, if an ICO qualifies as a security under the test set forth in *SEC v. W.J. Howey,* 328 U.S. 293 (1946), the issuer is subject to SEC (and AML) oversight. Other countries have sought to mitigate the risk of fraudulent transactions in connection with ICOs in different ways. For example, in September, the British Crown dependency of the Isle of Man announced the creation of the first-ever regulatory framework, the Isle of Man Registered Designated Business ICO, to enable companies issuing ICOs to comply with AML oversight.

Piercing cryptocurrency holders' identities in order to identify perpetrators of unlawful conduct has also proven to be difficult and costly. In November 2016, the Internal Revenue Service ("IRS") served a "John Doe" summons on Coinbase, a cryptocurrency exchange, seeking information on all users who transferred virtual currency from 2013 to 2015, in an effort to identify potential tax evaders. This effort, however, has led to protracted litigation concerning the scope and reach of the IRS subpoena.

Lastly, the "virtual" nature of cryptocurrencies makes it difficult for law enforcement authorities to consider them "assets" and subject them to forfeiture and seizure. Judicial authorities in the Netherlands have tackled this issue by ruling that cryptocurrencies qualify as assets and permitting prosecutors to access suspects' computers so that they can identify the key to their cryptocurrency wallets. By contrast, law enforcement authorities in the United Kingdom are considering whether to classify cryptocurrencies as a form of cash so that they can be more easily seized.[2] In the United States, the IRS issued a formal ruling in 2014 stating that "virtual currency is treated as property."[3] Likewise, U.S. courts have authorized the forfeiture of virtual currency in connection with criminal proceedings.[4] Notwithstanding these rulings, efforts to forfeit or seize virtual currency face significant obstacles due to the difficulty in tracing transactions.

Conclusion

When employed as a mechanism for verification and record keeping, blockchain technology has the potential to significantly reduce both the costs and time associated with regulatory compliance and enforcement. In order to realize this prospect, companies and governments must work in tandem to address regulatory concerns and root out illegal financial transactions. ◘

1. *See, e.g., In the Matter of Ripple Labs Inc. and XRP II, LLC,* No. 2015-05; *In the Matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik,* No. 2017-03.
2. N8 Policing Research Partnership, "Policing Bitcoin: Investigating, Evidencing and Prosecuting Crimes Involving Cryptocurrency," available at http://n8prp.org.uk/small_grants/.
3. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, 2014 WL 1224474 (March 2014).
4. *See United States v. 50.44 Bitcoins,* No. CV ELH-15-3692, 2016 WL 3049166, at *2 (D. Md. May 31, 2016); *United States v. Carl Mark Force IV,* Case No. 15-0319 (N.D. Cal. Nov. 3, 2015), Dkt. Entry 88; *United States v. Sean Roberson,* Case No. 14-565 (D.N.J. Feb 9, 2016), Dkt. Entry 39; *United States v. Ross William Ulbricht,* Case No. 13-06919 (S.D.N.Y.) (the docket for this case is sealed; however, the U.S. Attorney's office's press release related to the forfeiture can be found at www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins); *United States v. 178.95842915 Bitcoins stored in MultiBit wallet XXXX4XDAd,* Case No. 16-07009 (E.D. Wash. Sept. 29, 2017), ECF 46.

IRS Focuses Its Audit Priorities on Captive Insurance

BY JED M. SILVERSMITH

JED M. SILVERSMITH
OF COUNSEL

The terms "captive insurance" and "federal income tax code" are anything but captivating. Yet, captive insurance has captivated the attention of the Internal Revenue Service ("IRS"), which has placed captive insurance on its list of the "Dirty Dozen Tax Scams"—an annual list of the most abusive positions taken by taxpayers.[1] The IRS's aggressive stance on captive insurance has become more focused after the IRS's victory in *Avrahami v. Commissioner,* 149 T.C. No. 7 (Aug. 21, 2017).

What is "Captive Insurance"?

Savvy tax promoters will recommend that their clients create a captive or microcaptive insurance company that sells the taxpayer insurance for its business. Thus, the taxpayer (or a related party) owns his insurer. Once the newly established insurance company is created, it obtains the opinion of an underwriter who helps prepare new policies, which the taxpayer then uses to supplement or replace his pre-existing insurance. The taxpayer (or a related party), however, owns the insurance company and is therefore selling himself insurance.

The shelter aspect of the transaction lies in the fact that Section 831(b) of the Internal Revenue Code permits insurance companies to make certain elections and exclude up to $1.2 million in net premiums from their income. Thus, the taxpayer gets the benefit of a deduction for insurance premiums, and the captive insurance company does not pay income tax on the first $1.2 million in premiums. The captive insurer may invest the money, and in some cases return the money to the taxpayer in the form of loans or dividends. Instantly, through the creation of a wholly owned insurance company, the taxpayer has obtained a $1.2 million tax deduction.

Year after year, the tax benefits add up quickly. Not surprisingly, shelter promoters use captive insurance companies as part of an overall structure that can provide additional tax benefits. For example, the captive insurer could be owned by the taxpayer's Roth IRA, thereby ensuring that the investment profits of the captive insurer are never subject to federal income tax. Other captive insurance companies may be owned by the taxpayer's children, thereby avoiding potential gift and estate tax liabilities.

What Has the IRS Done?

1) Recent Policy Announcements

The IRS has listed captive insurance as one of its "Dirty Dozen" abusive transactions for the last three years. This list identifies some of the IRS's top audit priorities. In 2016, the IRS also listed microcaptive insurance companies as transactions of interest, meaning that taxpayers involved in these transactions must disclose these transactions when they file their tax returns.[2]

2) *Avrahami*

In August 2017, the Tax Court handed down a 105-page decision in *Avrahami,* disallowing the deductions from a captive insurance program. The Avrahamis were Arizona-based jewelers who entered into a captive insurance shelter. The court noted that, as a result of the Avrahamis' participation in this program, their annual insurance bills (and deductions) soared from $150,000 per year to $1,100,000. Some of the additional line items were even more suspect—such as the increase from $1,500 to $360,000 for terrorism risk insurance premiums paid by the taxpayers.

In disallowing the deductions, the court also noted, among other things, that the Avrahamis' company did not have a sufficient "number of risk exposures to achieve risk distribution," because the only entities that the Avrahamis insured were their companies. The court was also critical of a reinsurance program that the Avrahamis used to meet their risk distribution requirements. Risk distribution is a prerequisite for a transaction to be deemed as insurance. The court determined that the reinsurance company was not a bona fide insurer, because the funds paid by the Avrahamis (and the promoters' other clients) were simply funneled back to the clients each year. For example, during their two years under audit, the Avrahamis paid $720,000, which was ultimately returned to other entities under their control.

> ► For example, the captive insurer could be owned by the taxpayer's Roth IRA, thereby ensuring that the investment profits of the captive insurer are never subject to federal income tax.

The Avrahamis returned all of the money from the captive insurance company to a U.S.-based partnership called Belly Button Center, LLC, which owned real estate in Arizona. The funds were returned in the form of loans, which were never paid back.

Critically, although the IRS disallowed the premium deductions and treated the loans as income, it only assessed an accuracy-related penalty (*i.e.,* a negligence penalty) on the decision to disregard the loans. The Tax Court did not impose the fraud penalty. Furthermore, the far more substantial deduction for the premiums paid to the captive insurance company were not subject to any penalty. The court found that the Avrahamis relied in good faith on their tax advisers—who created this structure—and should not be required to pay a negligence penalty.

What Does *Avrahami* Mean?

The *Avrahami* decision will provide a guidepost for future audits. Taxpayers who use captive insurance may be subject to audit and substantial adjustments. While the Avrahamis avoided most of the accuracy-related penalties, other taxpayers may not be as fortunate. Taxpayers who have used captive insurance should seek an independent review of their specific structure to evaluate their options in light of the IRS's recent victory. ◘

1. www.irs.gov/newsroom/irs-warns-of-abusive-tax-shelters-on-2017-dirty-dozen-list-of-tax-scams
2. www.irs.gov/irb/2016-47_IRB

Blank Rome Named "Best Place to Work for LGBTQ Equality" by Human Rights Campaign in 2018 Corporate Equality Index

Blank Rome LLP received a perfect score of 100 percent on the 2018 Corporate Equality Index ("CEI"), a national benchmarking survey and report on corporate policies and practices related to LGBTQ workplace equality, administered by the Human Rights Campaign Foundation ("HRC").

With this score, Blank Rome has been designated for the third year in a row as a "Best Place to Work for LGBTQ Equality" by the HRC, and joins the ranks of 609 major U.S. businesses that earned top marks this year.

The 2018 CEI rated 947 businesses in the report, which evaluates LGBTQ-related policies and practices including non-discrimination workplace protections, domestic partner benefits, transgender-inclusive health care benefits, competency programs, and public engagement with the LGBTQ community. Blank Rome's efforts in satisfying all of the CEI's criteria results in a 100 percent ranking and the designation as a "Best Place to Work for LGBTQ Equality."

The Criminal Finances Act of 2017: New Compliance Requirements for UK Businesses

BY MARK M. LEE AND NAOMI ZWILLENBERG


MARK M. LEE
PARTNER

NAOMI ZWILLENBERG
ASSOCIATE

On April 27, 2017, the United Kingdom enacted the Criminal Finances Act 2017 (the "Act"), which provides that companies and partnerships ("relevant bodies") are criminally liable if they fail to implement adequate procedures to prevent economic crime and fraud (*e.g.,* tax evasion) by employees or agents, even when the company was not aware of the crime.[1]

Background

In April 2016, the British government published an Action Plan for anti-money laundering and counter-terrorist financing[2] that established procedures to reduce risks of money laundering and terrorist financing that were identified by the government in October 2015.[3]

Goal

The Act strengthens the government's ability to confiscate the proceeds of crime, to improve the international reach of enforcement and to enforce the Terrorism Act 2000.

Corporate Criminal Offenses

The Act is the most significant change to the anti-money laundering and terrorist finance regime in the United Kingdom since the enactment of the Proceeds of Crime Act in 2012, and will significantly affect the investigation and enforcement of corporate crime. The Act creates two new corporate criminal offenses for the failure to prevent the facilitation of tax evasion.

The government's draft guidance for these new corporate offenses for the failure to prevent tax evasion demonstrates that the aim of the legislation is to hold a "relevant body" criminally liable when it fails to prevent its employees and agents from committing or facilitating tax evasion.[4] The new law does not radically alter *what* is criminal; it focuses on *who* is held to account for the criminal conduct.[5] The draft guidance defines a "relevant body" as an incorporated body (typically a company) or partnership that does not include natural persons.[6] The guidance further explains that the previous structure required prosecutors to prove that senior members of the organization participated in the illegal activity, which had the perverse effect of making prosecutions more difficult and rewarded companies that failed to implement effective corporate governance and preventative procedures.

The guidance lists six principles that organizations should adopt:

1) risk assessment,
2) proportionality of risk-based prevention procedures,
3) top level commitment,
4) due diligence,
5) communication (including training), and
6) monitoring and review.

Defenses

A business can avoid criminal liability by implementing procedures to prevent someone acting on its behalf from facilitating tax evasion in the United Kingdom or in a foreign country. For a relevant body to benefit from the "prevention procedures" defense under the Act, it must prove that it had "such prevention procedures as it was reasonable in all the circumstances to expect … or [that] it was not reasonable in all the circumstances to expect [the company] to have any."

What UK Businesses Should Do

Businesses need to review their current procedures, minimize risks, and establish appropriate monitoring and training. Effective measures will depend on the size of the business and its complexity. At the least, smaller business acting in low-risk industries should prohibit the illegal activities, train staff, and implement clear reporting and whistleblowing procedures. It's important to note, however, that compliance with the guidance will NOT automatically immunize the company from prosecution. ◻

1. Criminal Finances Act 2017 (Commencement No. 1) Regulations 2017. http://services.parliament.uk/bills/2016-17/criminalfinances.html
2. www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering_web_.pdf
3. www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf
4. www.gov.uk/government/uploads/system/uploads/attachment_data/file/560120/Tackling_tax_evasion_-_Draft_government_guidance_for_the_corporate_offence_of_failure_to_prevent_the_criminal_facilitation_of_tax_evasion.pdf
5. UK Nexus: The foreign tax offense can only be committed by a relevant body incorporated under UK law (*e.g.,* a limited company incorporated under UK law or carrying on a business or part of a business in the UK; a company incorporated in France, but operating in Manchester; or a company-associated person located within the UK who facilitates the evasion of the overseas tax—for example, a company incorporated under German law whose employee helps another person commit a foreign tax evasion offence in London). *Id.*
6. www.gov.uk/government/uploads/system/uploads/attachment_data/file/560120/Tackling_tax_evasion_-_Draft_government_guidance_for_the_corporate_offence_of_failure_to_prevent_the_criminal_facilitation_of_tax_evasion.pdf
7. www.gov.uk/government/uploads/system/uploads/attachment_data/file/560120/Tackling_tax_evasion_-_Draft_government_guidance_for_the_corporate_offence_of_failure_to_prevent_the_criminal_facilitation_of_tax_evasion.pdf

Blank Rome Honored for Advancing Women in the Legal Industry in 2017

2017 has been a banner year for Blank Rome's Women's Forum and diversity initiatives, with the Firm receiving significant recognition from *Bloomberg, Working Mother,* and the *Philadelphia Business Journal* for its efforts in advancing women in the legal industry and beyond. Additionally, the Firm hosted its inaugural Women's Leadership Summit and Hackathon in September 2017 and expanded its participation in Diversity Lab initiatives by joining the Mansfield Rule pilot program, continuing the OnRamp Fellowship program, and participating in the Women in Law Hackathon Alliance, following the Firm's participation in the 2016 Women in Law Hackathon. □

Blank Rome Receives 2017 Advancing Women Company Award by *Philadelphia Business Journal*

LISA CASEY SPANIEL
PARTNER

Blank Rome received the 2017 Advancing Women Company Award by the *Philadelphia Business Journal* and was honored at a reception in November, along with 30 women honorees who received the "Women of Distinction" award based on their career accomplishments and community service.

Blank Rome Partner Lisa Casey Spaniel, who serves as chair of the Firm's Women's Forum, as well as Partner Sophia Lee, who leads various diversity and inclusion initiatives for the Firm's Philadelphia office, accepted the award on behalf of the Firm.

"It's truly an honor to be a part of such an inclusive, forward-thinking firm, and to be recognized for our role in advancing women in the legal industry," said Ms. Spaniel. "As our Women's Forum continues to grow and evolve, we look forward to expanding on our current initiatives in this space, as well as exploring additional opportunities to advance and retain women in the workforce." □

Blank Rome Named a 2017 "Best Law Firm for Women" by *Working Mother*

ALAN J. HOFFMAN
CHAIRMAN AND MANAGING PARTNER

Blank Rome was named one of the 2017 Best Law Firms for Women by *Working Mother* magazine, marking the second year that the Firm has been recognized for its commitment to creating one of the best women-friendly workplaces in the United States. *Working Mother's* annual list honors 50 U.S. law firms for their policies in the advancement of women, notably with regards to key factors such as female representation, flexibility, paid-time off and leaves of absence, leadership, and compensation and advancement, as well as the development and retention of women.

"Blank Rome has a longstanding history of commitment to diversity and inclusion, and has been at the forefront of leading the legal industry with developing and promoting policies and programs aimed at advancing women in the workforce," said Alan J. Hoffman, Blank Rome Chairman and Managing Partner. "Through our affinity groups such as the Women's Forum, diversity programs, industry initiatives, and professional and personal development offerings—including mentoring opportunities and alternative work arrangements—we are actively engaged in fostering the next generation of female leaders at our Firm, and are proud of their achievements and successes as they grow within Blank Rome and our local communities." □

The Benefits of Corporate Anti-Corruption Programs: No Charges

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

CARLOS F. ORTIZ — PARTNER
SHAWN M. WRIGHT — PARTNER
MAYLING C. BLANCO — PARTNER
ARIEL S. GLASNER — ASSOCIATE

The U.S. Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC") issued 15 declination letters in 2017 notifying companies of their decision not to pursue charges in connection with alleged violations of the Foreign Corrupt Practices Act ("FCPA"). These declinations are a strong signal to companies that they should have strong anti-corruption systems in place, and that when they find themselves facing a potential violation, how they choose to respond can have a far-reaching impact on the outcome of any government investigation. Companies are much more likely to avoid facing charges with respect to the alleged unlawful conduct if they have a robust compliance program, conduct a thorough investigation when allegations of misconduct are raised internally, cooperate through voluntary self-disclosure, and, in certain cases, disgorge ill-gotten gains.

Declinations are the most favorable mechanism for resolving FCPA matters, followed by non-prosecution agreements ("NPAs") and deferred prosecution agreements ("DPAs"). NPAs typically require companies to commit to ongoing obligations, including engaging corporate monitors for a period of years and conducting annual anti-corruption reviews followed by reports to the government setting forth their findings and continuing remedial efforts. DPAs are a less-favored type of resolution, because they also involve the filing of a public pleading that is held in abeyance while the company works to satisfy the conditions set forth in the agreement. Most notably, NPAs and DPAs involve the payment of harsh fines, penalties, and the disgorgement of ill-gotten gains in most instances. By contrast, while certain declinations—specifically those granted under the DOJ's Pilot Program—require companies to disgorge their ill-gotten gains, they involve no other penalties, no continuing obligations, and no finding of guilt by the court or admission of guilt. Declinations result in the total avoidance of criminal charges in connection with the alleged conduct.

In an October 2017 policy speech, DOJ Deputy Attorney General ("DAG") Rod Rosenstein announced that the DOJ "is working to incentivize, reward, and even partner with companies that demonstrate a commitment to combating corporate fraud." This message was reinforced when DAG Rosenstein announced in November 2017 that the principles behind the DOJ's Pilot Program, which commenced in April 2016 and offers companies incentives to self-disclose FCPA violations, cooperate with the government, remediate unlawful conduct, and disgorge any profits that resulted from the violations, would be made permanent through incorporation into the U.S. Attorneys' Manual. The declinations that have been issued to date offer an example of the policies that the DOJ is implementing. Specifically, they reflect decisions not to pursue criminal charges against companies that have anti-corruption programs in place and adopt a cooperative stance vis-à-vis the government's investigation into alleged FCPA misconduct.

> ► Compared to 2016, when 14 declinations, including five under the Pilot Program, were issued, the total number of declinations increased in 2017.

DOJ's Pilot Program—"Declinations with Disgorgement"

In 2017, two declinations were issued under the Pilot Program. In declining to pursue charges, the DOJ cited the following factors: 1) voluntary self-disclosure; 2) thorough and comprehensive internal investigation; 3) full cooperation; 4) full disgorgement; 5) continuing enhancements to the company's compliance program and internal controls; and 6) full remediation, including the termination of or disciplinary action against the executives and other employees involved in the misconduct. These factors echoed the reasons cited by the DOJ in the five declinations granted under the Pilot Program in 2016. These declinations of charges also continued the DOJ's practice under the Pilot Program of requiring companies to disgorge profits to secure a declination. Per DAG Rosenstein's November 2017 policy announcement, this practice will now be incorporated into the U.S. Attorneys' Manual.

"Traditional" Declinations

In addition to the two declination letters sent under the Pilot Program in 2017, 13 public companies, including Merck & Co. and IBM, announced that they received declination letters from the DOJ and/or the SEC.[1] Unlike Pilot Program declinations, these "traditional" declinations did not involve disgorgement of profits.

Whereas a stated objective of the Pilot Program is to increase transparency regarding FCPA enforcement, including what companies must do in order to receive a declination letter or a criminal penalty below that recommended under the U.S. Sentencing Guidelines, "traditional" declinations offer no such transparency. Moreover, as companies make "traditional" declinations public only through general statements, usually in required securities filings,[2] specific information is not readily available about the declinations.

Notwithstanding the absence of stated criteria, certain factors that likely contribute to the DOJ's decision to issue a "traditional" declination mirror the bases for obtaining a declination under the Pilot Program. These factors include: 1) the existence of a strong compliance program; 2) the completion of a comprehensive internal investigation; and 3) remedial measures. The overlap of these factors with those required under the Pilot Program highlights that the two types of declinations both require a proactive approach by the subject companies.

Conclusion

Compared to 2016, when 14 declinations, including five under the Pilot Program, were issued, the total number of declinations increased in 2017.[3] A key takeaway of the Pilot Program that has now been made permanent is that disgorgement is an integral part of both the DOJ's and SEC's strategy against global corruption. Regarding declinations more broadly—both in and out of the Pilot Program—companies with a potential FCPA violation are well-served to be mindful of the huge benefits of implementing a timely and effective compliance and remediation program.

1. *See, e.g.,* press release issued by Orthofix International, *Orthofix Announces Resolution of SEC Investigations,* Jan. 18, 2017, available at http://ir.orthofix.com/releasedetail.cfm?ReleaseID=1008341; Press release issued by Cobalt International Energy, *Cobalt Announces Closing of DOJ Investigation,* Feb. 9, 2017, available at www.cobaltintl.com/newsroom/cobalt-announces-closing-of-doj-investigation; Merck & Co., Form 10-K (filed Feb. 28, 2017), at 103; Crawford and Company, Form 10-K (filed Feb. 27, 2017), at 97; and Innodata Inc., Form 10-K (filed March 16, 2017), at 29.
2. By contrast, Pilot Program declinations are publicized by DOJ on the agency's website and in public letters issued to the target companies.
3. www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html; www.justice.gov/criminal-fraud/pilot-program/declinations.

Blank Rome Joins the 2017 Global 100

Blank Rome LLP is pleased to announce that the Firm has been ranked in the 2017 Global 100, joining as one of five new entrants to *The American Lawyer* report.

Using Am Law 100 data, the Global 100 annually recognizes the world's largest law firms in the categories of gross revenue, attorney head count, and profits per equity partner. This year, Blank Rome ranked 96th for gross revenue and tied in 97th place for highest profit per equity partner.

Additionally, in May 2017, the Firm ranked 78th in the 2017 Am Law 100, rising 16 places from last year. Blank Rome also had the largest change in revenue for Philadelphia-based firms and the second largest change in revenue nationally.