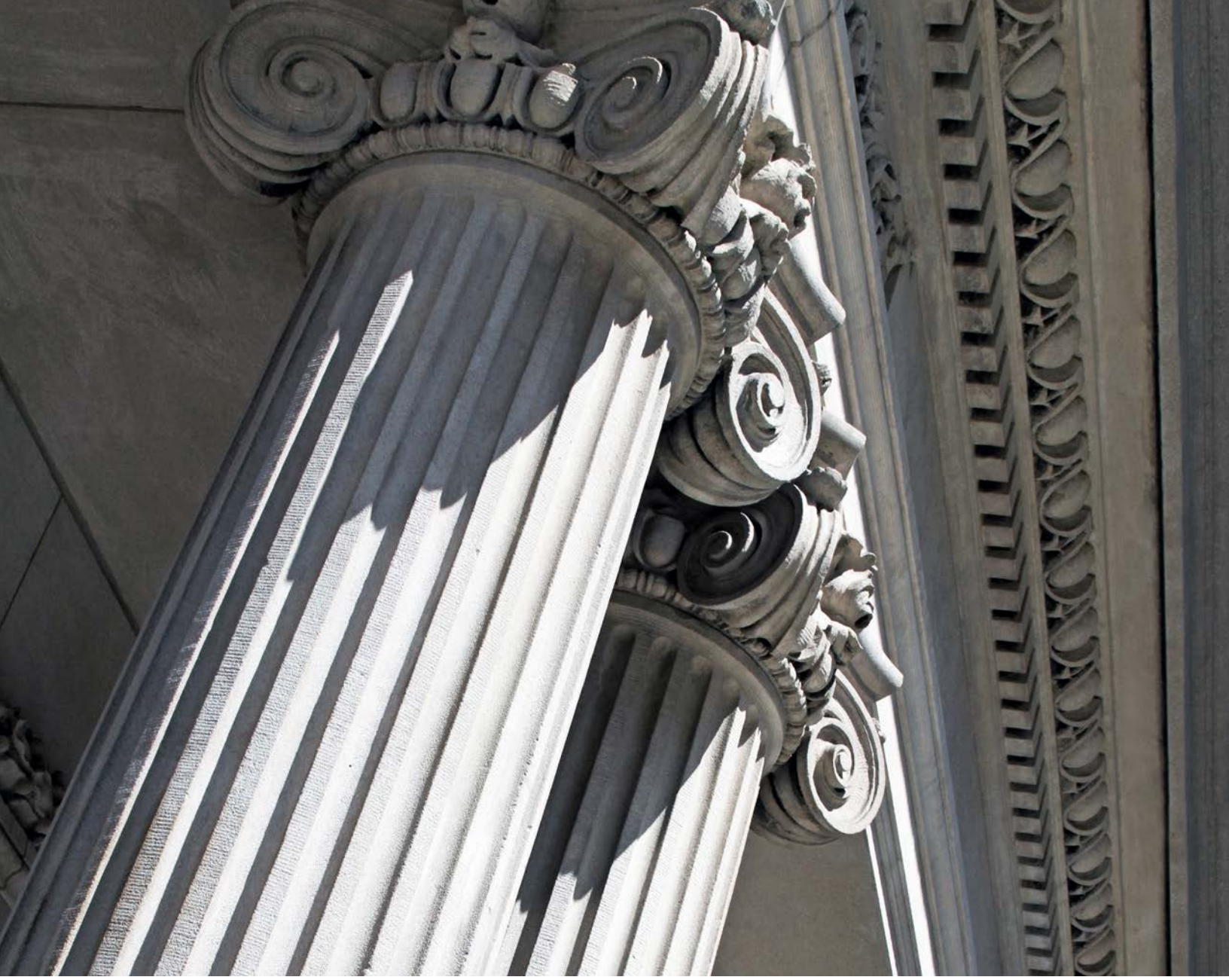


WHITE COLLAR WATCH

BLANKROME

SEPTEMBER 2018 • NO. 2

CONTENTS

Note from the Editors

Welcome to the September 2018 edition of Blank Rome's *White Collar Watch.* As we head into the last days of summer, this edition covers some of the hottest white collar issues in the areas of finance, data security, and international business.

On the finance front, we explore the buzz phrase "Initial Coin Offering" ("ICO") and the potential tax penalties to which many individuals may now be exposed due to undeclared capital gains on coin investments. Regarding the always-important and evolving issue of data security, we continue our "FinTech Revolution" series and discuss how data breaches can result in regulatory enforcement actions.

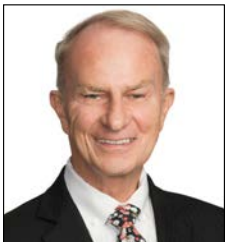
From an international perspective, we provide important updates from the ever-expanding world of the Foreign Corrupt Practices Act, taking a look at its enforcement under the Trump administration, and we also discuss new U.S. Treasury regulations that impact foreign individuals with interests in the United States.

We wish you and yours a healthy and happy remainder of your summer and beginning of autumn! Please reach out if you have any questions about the topics discussed in the enclosed newsletter, or if you have suggestions for future *White Collar Watch* editions. It is our pleasure to be a resource to you.

With warm regards,

JOSEPH G. POLUKA
PARTNER

INBAL P. GARRITY
PARTNER



WILLIAM B. SHIELDS
OF COUNSEL

EDITORS, *WHITE COLLAR WATCH*

FCPA Enforcement under the Trump Administration: No "Piling On," but Otherwise Business as Usual

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

CARLOS F. ORTIZ
PARTNER

SHAWN M. WRIGHT
PARTNER

MAYLING C. BLANCO
PARTNER

In 2012, Donald Trump called the Foreign Corrupt Practices Act ("FCPA") "ridiculous" and a "horrible law" that made it more difficult for U.S. companies to compete abroad.[1] While President Trump's private thoughts on the FCPA may not have changed, reportedly telling then-Secretary of State Rex Tillerson in February 2017 that the FCPA unfairly penalizes American businesses,[2] his administration has continued to enforce it at rates comparable to the Obama administration and has provided incentives for companies to comply with the FCPA. Thus, as the numbers below demonstrate, companies doing business outside of the United States should not expect any relief from the Department of Justice's ("DOJ") and the Securities and Exchange Commission's ("SEC") vigorous enforcement efforts as a result of the president's reported personal views.

Enforcement under the Trump Administration

In 2017, the first year of Trump's presidency, the DOJ brought 27 FCPA enforcement actions and the SEC brought eight.[3] So far, in 2018, the DOJ has brought nine such actions, while the SEC has brought four. *Id.* While the number of SEC actions brought in 2017 and anticipated for 2018 is far below the number brought during the final year of the Obama administration, it is comparable to the number brought in 2014 and 2015 (eight and 11, respectively). *Id.* Furthermore, the 27 actions brought by Trump's DOJ in 2017 matches the 27 brought by Obama's DOJ in 2016. *Id.* Even if the DOJ is on pace to bring fewer enforcement actions this year, it likely will still bring more than it did in 2014 and 2015 under President Obama. *Id.* Furthermore, in 2018, the DOJ and SEC already have settled FCPA enforcement actions for more than $923 million, compared to the $934 million in fines collected during the entirety of 2017. *Id.* In sum, the Trump administration has continued to enforce the FCPA at a rate comparable to the Obama administration.

DOJ's New "Anti-Piling On" Policy to Encourage Corporate Compliance with the FCPA

In early May 2018, Deputy Attorney General Rod Rosenstein announced a new internal DOJ policy aimed at coordinating with other enforcement agencies to prevent imposing multiple penalties for the same conduct.[4] One of the policy's goals is to provide "greater transparency and consistency in corporate enforcement." *Id.* In announcing the new "anti-piling on" policy, Rosenstein stated that the DOJ "want[s] companies and their counsel to promptly report suspected crimes, and…want[s] them to expeditiously negotiate reasonable resolutions." *Id.*

There are four aspects to the policy. First, DOJ attorneys cannot invoke the threat of criminal prosecution solely to gain leverage in negotiating a settlement in a civil enforcement action. *Id.*

> While the Trump administration has established new policies aimed at increasing FCPA compliance, such as the new "anti-piling on" policy and the FCPA Corporate Enforcement Policy, it has not hesitated to bring enforcement actions when necessary.

Second, DOJ attorneys are directed to coordinate with one another to avoid disproportionate punishment, which may involve "crediting and apportionment of financial fines, forfeitures, and penalties." *Id.* Third, DOJ attorneys are encouraged to coordinate with other federal, state, local, or foreign enforcement authorities seeking to resolve a case with a company for the same misconduct. *Id.* Finally, DOJ attorneys should look at the following factors in determining whether multiple penalties serve the interests of justice: the egregiousness of the wrongdoing, statutory requirements regarding penalties, the risk of delay in finalizing a resolution, and the adequacy and timeliness of a company's disclosures and cooperation with the DOJ. *Id.*

Overall, while the Trump administration has established new policies aimed at increasing FCPA compliance, such as the new "anti-piling on" policy and the FCPA Corporate Enforcement Policy,[5] it has not hesitated to bring enforcement actions when necessary. ◻ –

1. Jim Zarroli, "Trump Used to Disparage an Anti-Bribery Law; Will He Enforce It Now?," *NPR* (Nov. 8, 2017), available at npr.org/2017/11/08/561059555/trump-used-to-disparage-an-anti-bribery-law-will-he-enforce-it-now.
2. Dexter Filkins, "Rex Tillerson at the Breaking Point: Will Donald Trump Let the Secretary of State Do His Job?," *The New Yorker* (Oct. 16, 2017), available at newyorker.com/magazine/2017/10/16/rex-tillerson-at-the-breaking-point.
3. Victoria Graham, "Anti-Bribery Enforcement Remains Steady Under Trump," *Bloomberg Law* (June 20, 2018).
4. Rod J. Rosenstein, Deputy Attorney General, Department of Justice, Remarks at the American Conference Institute's 20th Anniversary New York Conference on the Foreign Corrupt Practices Act (May 9, 2018), available at justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institutes.
5. "DOJ Incorporates FCPA Pilot Program into U.S. Attorneys' Manual Providing Permanent Incentives for Strong FCPA Compliance," Blank Rome Alert (Dec. 2017), available at blankrome.com/publications/doj-incorporates-fcpa-pilot-program-us-attorneys-manual-providing-permanent-incentives.

The FinTech Revolution: How Data Breaches Can Result in Regulatory Enforcement Actions

BY BRIDGET MAYER BRIGGS AND ARIEL S. GLASNER

BRIDGET MAYER BRIGGS
ASSOCIATE

ARIEL S. GLASNER
ASSOCIATE

This is the fifth 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; our second article, The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications; our third article, The FinTech Revolution: The Impact of Blockchain Technology on Regulatory Enforcement; and our fourth article, The FinTech Revolution: Complying with Anti-Money Laundering Laws to Avoid Regulatory Enforcement Actions.

As news reports of corporate data breaches have become commonplace, companies must be proactive in preventing security breaches and prepared to take appropriate action in the event one occurs. This mantra is particularly true for FinTech companies that, by the very nature of their business, regularly collect customers' personally identifiable information ("PII") and other sensitive data. A failure to adequately protect this information, or to disclose the occurrence of a data breach, exposes companies to the very real possibility of government enforcement action.

> When a company becomes aware of a cybersecurity incident or risk that would be material to its investors, the SEC expects it to make appropriate disclosures prior to the offer and sale of securities.

We have noted previously that a FinTech company that falsely represents its data security practices is subject to an enforcement action by the Consumer Financial Protection Bureau for violation of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[1] In addition, FinTech companies that sell securities—whether publicly or in a private placement—must comply with applicable securities regulations when it comes to data breaches and their attendant disclosure.

Disclosure Requirements under the Securities Exchange Act

Section 10(b) of the Securities Exchange Act of 1934—the antifraud provision of the Exchange Act—and the Securities and Exchange Commission ("SEC") Rule promulgated under this section, Rule 10b-5, broadly prohibit fraud in connection with the sale of securities.[2] Rule 10b-5 specifically forbids using any "device, scheme, or artifice to defraud," making any misstatement or omission of a "material fact," or engaging in "any act, practice or course of business which operates…as a fraud or deceit upon any person," in connection with the sale of any securities. Any company engaged in the sale of securities, whether public or private, is subject to this rule.[3]

A FinTech company that sells securities must disclose material information about cybersecurity risks and cyber incidents to prevent a misleading statement or omission about a material fact. For example, if a company expects to incur substantial costs as a result of a data breach that would be material for its financial condition or results of operations, it would need to disclose the breach and the risk of its adverse impact on the company's financial position to avoid misleading investors about the company's future financial performance.

Importantly, there is no bright-line rule for when information is considered "material," such that it must be disclosed. Based on case law guidance, information is considered material if there is a substantial likelihood that a reasonable investor would view the information important in making an investment decision or if the information would significantly alter the "total mix" of the information available about a security.[4] In 2011, the SEC issued guidance on "disclosure obligations related to cybersecurity risks and cyber incidents." Although it principally applied to public company disclosure obligations, this guidance also offers useful best practices information for private entities involved in the sale of securities. In particular, the guidance provides general examples of what might constitute a material fact in certain circumstances, such as when the risk of cyber incidents is "among the most significant factors that make an investment in the company speculative or risky."[5] Again, the analysis is fact-specific and can be subjective.

Earlier this year, the SEC published additional guidance to further assist public companies in preparing SEC filings about cybersecurity risks and incidents.[6] Besides reinforcing the 2011 guidance, the recent publication emphasized, among other things, the importance of implementing a framework of policies and procedures to address cybersecurity risks and incidents, and the obligations of public companies and their insiders to "refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents."[7]

The 2018 guidance also provided a helpful framework for analyzing the materiality of cyber incidents and risk. In determining disclosure obligations regarding cybersecurity risks and incidents, companies should generally "weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations."[8] The SEC also clarified that the materiality of cybersecurity risks or incidents depends upon their "nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations," as well as "the range of harm that such incidents could cause," which could include "harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions."[9]

The SEC made it clear that it does not expect companies to disclose "specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident." However, when a company becomes aware of a cybersecurity incident or risk that would be material to its investors, the SEC expects it to make appropriate disclosures prior to the offer and sale of securities.[10] Although the SEC understands that a company may require time to "discern the implications of a cybersecurity incident," the SEC guidance makes it clear that "an ongoing internal or external investigation … would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."[11]

Penalties for Failure to Comply with Rule 10b-5

The penalties for failure to comply with Rule 10b-5 are onerous. Companies or individuals that engage in a "willful" violation of Rule 10b-5 are subject to criminal prosecution by the U.S. Department of Justice. A resulting conviction carries with it a fine of up to $25 million for companies, and a period of incarceration of up to 20 years and a fine of up to five million dollars for individuals.[12] In addition to seeking disgorgement of ill-gotten gains, the SEC also has the authority to impose a range of civil monetary penalties for "each act or omission" resulting in a violation of the securities laws, of up to $775,000 per act or omission by a company and up to $160,000 per act or omission by an individual.[13] Importantly, each investor to whom a misleading statement or report was made constitutes a separate "act or omission." The amount of the maximum fine the SEC may seek to impose is thus multiplied by the number of separate acts or omissions that have occurred, thereby exposing companies to substantial fines.

Conclusion

FinTech companies that fail to take seriously the proliferation of threats to data privacy and security operate at their own peril. In addition to taking steps to implement comprehensive data protection systems and policies, companies must be aware of their obligations to disclose material cyber risks and data breaches. FinTech companies should consult further with legal counsel to understand these obligations, so that they are fully equipped to confront risks to their data protection systems, to respond appropriately to the possibility of a data breach, and to avoid the risk of failure to comply with applicable laws and regulations. ◘ –

1. *See In re Dwolla, Inc.*, File No. 2016-CFPB-0007 (Mar. 2, 2016).
2. *See* 15 U.S.C. § 78j; 17 C.F.R. § 240.10b-5.
3. *See, e.g., SEC v. Stiefel Laboratories, Inc.,* Case No. 1:11-cv-24438 (S.D. Fla. Dec. 12, 2011) (private company).
4. *Matrixx Initiatives, Inc. v. Siracusano,* 563 U.S. 27, 43 (2011).
5. Division of Corporation Finance SEC, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), available at sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
6. Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 26, 2018), available at sec.gov/rules/interp/2018/33-10459.pdf.
7. *Id.* at 7.
8. *Id.* at 10–11.
9. *Id.* at 11.
10. *See id.*
11. *Id.* at 12.
12. 15 U.S.C. § 78ff.
13. 15 U.S.C. §§ 77h-1(g), 78u-2(b), 80a-9(d), 80b-3(i).

Recent Announcements & Recognitions

Chambers USA 2018 Ranks Blank Rome White Collar Attorneys

Congratulations to the following partners who were ranked in *Chambers USA 2018* for their work in the category of Litigation: White Collar Crime and Government Investigations.

Barry Wm. Levine (Band Four – District of Columbia). *Chambers USA* states: "'Barry Levine is smart, defense-minded and has a lot of trial experience' according to impressed interviewees, who also add that 'he is terrific in the courtroom as he is so charismatic.' His clients further attest: 'He stands out because of his responsiveness, technical abilities and his courtroom success.' He has a wealth of experience defending individual clients in white-collar criminal cases, counting bankers, executives and high-level public officials among his varied client list."

Carlos F. Ortiz (Band Three – New Jersey). *Chambers USA* states: "Carlos Ortiz is an experienced trial lawyer specializing in white-collar criminal defense work and government investigations. He also represents clients in cases concerning violations of the TCPA."

Henry F. Schuelke III (Senior Statesperson – District of Columbia). *Chambers USA* states: "Henry Schuelke has a wealth of experience representing boards of directors and major corporations facing a variety of white-collar criminal allegations. His areas of expertise include FCPA violations, environmental crimes and accounting fraud, among other matters."

To view Blank Rome's full *Chambers USA 2018* rankings, please click here.

Attorneys Honored for Their Commitment to Pro Bono

Congratulations to our Blank Rome attorneys who practice white collar defense & investigations law on receiving Blank Rome Pro Bono Awards in recognition of completing 65 or more pro bono hours in 2017.

Rither Alabre, Associate, NY
Mayling C. Blanco, Partner, NY
Bridget Mayer Briggs, Associate, PA
Kiersten L. Carlson, Associate, D.C.
Negar M. Kordestani, Associate, D.C.
Courtney M. O'Brien, Associate, PA
Stephen M. Orlofsky, Partner, NJ
Victoria Ortega, Associate, D.C.
Carlos F. Ortiz, Partner, NJ
Joseph G. Poluka, Partner, PA
Ann E. Querns, Associate, PA
Laurence S. Shtasel, Partner, PA
Henry F. Schuelke, III, Partner, D.C.
Nicholas R. Tambone, Associate, NY

Ariel Glasner Elected to D.C. Bar's Attorney/Client Arbitration Board

Congratulations to Blank Rome Associate Ariel S. Glasner on being elected to serve a three-year term on the Attorney/Client Arbitration Board ("ACAB") of the D.C. Bar. The ACAB is elected by the D.C. Bar Board of Governors to oversee an efficient fee arbitration service for D.C. Bar members and their clients to resolve disputes about legal fees. For more information on the ACAB, please click here.

Cryptocurrency: The Tax Man Cometh Again

BY CARLOS F. ORTIZ, MAYLING C. BLANCO, AND D. MORGAN BARRY

CARLOS F. ORTIZ
PARTNER

MAYLING C. BLANCO
PARTNER

D. MORGAN BARRY
ASSOCIATE

In the wake of the success of its "Swiss Bank Program," the U.S. Department of Justice ("DOJ") Tax Division and the Internal Revenue Service ("IRS") Criminal Investigation Division are gearing up for a similar initiative aimed at taxpayers using virtual currency to evade taxes. In public statements, key officials at the DOJ and IRS have made no secret of their intention to crack down on the use of cryptocurrency to evade taxes. They also appear to be following the same blueprint they used successfully in prosecuting taxpayers using offshore accounts. If history repeats itself, it is likely they will prosecute those who facilitate or in any way assist taxpayers in these efforts.

> Taxpayers and cryptocurrency platforms should prepare for the application of the highly effective, but relatively inexpensive, tools utilized in the Swiss Bank Program to bring those involved in virtual currency transactions into reporting compliance.

Swiss Bank Program Resulted in Billions in Fines and Settlements with over 80 Swiss Banks

In 2008, the IRS started the Swiss Bank Program by issuing John Doe subpoenas[1] to Swiss banks to uncover then-unknown tax evaders. Following this initial step, the DOJ and IRS utilized further investigative tools, such as treaty requests and subsequent subpoenas, enabling the prosecution of individuals and, ultimately, the investigation of and settlements with financial institutions in Switzerland. In exchange for non-prosecution agreements and monetary penalties, Swiss banks disclosed their cross-border activities and provided information about U.S. taxpayer accounts and other banks into which individuals transferred funds. Over 80 Swiss banks cooperated in civil and criminal proceedings, and penalties exceeding $1.36 billion were collected. This was an unprecedented success for the DOJ and IRS in their long-running efforts to address an area of significant noncompliance that was thought by many to be an undetectable means to evade taxes.

The Offshore Voluntary Disclosure Program ("OVDP") played a significant part in the IRS's efforts to attack offshore tax evasion by encouraging and enabling taxpayers to come forward and disclose their offshore tax liabilities in exchange for the guarantee of non-prosecution. The OVDP resulted in over 54,000 self-disclosures and collected more than eight billion dollars in taxes and penalties. This program also led to the discovery of much useful intelligence, as each participant was required to provide information regarding the banks used and the individuals involved. This information then was available to the government in its prosecution of the financial institutions.

Upon the conclusion of the Swiss Bank Program in 2016, the then-Principal Deputy Assistant Attorney General warned that the Tax Division remained committed to holding individual taxpayers accountable for their respective roles in concealing foreign accounts and assets and evading U.S. tax obligations. At numerous conferences since, the DOJ has made clear that it intends to replicate this enforcement formula in other parts of the world, as it tracks funds transferred out of the Swiss banks.

The IRS and DOJ *Are* Targeting Cryptocurrency Transactions

There currently exists a perceived anonymity for virtual currency transactions similar to that which existed for transactions in offshore accounts before the Swiss Bank Program. Indeed, many believe that the anonymity of virtual currency transactions provides a comparable opportunity to obtain tax-free gains for cryptocurrency investments. The fact that the identity of the coin owners are encrypted, combined

with the uncertainty among taxpayers of their reporting obligations for cryptocurrency transactions, present a fertile area for potential noncompliance, as well as an enforcement challenge.

As an initial step to address this problem, in 2014, the IRS issued public Notice 2014-21 to provide guidance for the tax treatment of transactions involving virtual currency. The IRS

confirmed that virtual currency that can be converted into traditional currency constitutes property for tax purposes. Thus, a gain or loss realized by the sale of cryptocurrency must be reported on a taxpayer's returns.

Additionally, the receipt of units of cryptocurrency for services similarly must be reported as income at the time of its receipt at the fair market value of the unit. Nevertheless, out of approximately 120 million individual electronic tax returns filed annually between 2013 and 2015, less than 900 taxpayers in each of the relevant years reported a virtual currency transaction. During this time frame, Coinbase, one of the largest cryptocurrency exchange platforms, serviced approximately 5.9 million customers, and more than 14,000 Coinbase users either bought, sold, sent, or received at least $20,000 worth of cryptocurrency in a given year.[2] The numbers clearly do not add up.

In 2016, the IRS took a significant step to address this issue, and, following its playbook from the Swiss Bank Program, issued a John Doe summons to Coinbase seeking expansive information regarding U.S. taxpayers' use of this platform. The request included transaction logs, records of payments processed, and account statements. Following Coinbase's legal challenges, the summons was narrowed to accounts with a transaction of at least $20,000 between 2013 and 2015. As of February 23, 2018, approximately 13,000 Coinbase customers were informed that their records would be turned over to the IRS.

On July 2, 2018, the IRS stepped up its efforts and announced a focus on virtual currency as part of a new tax enforcement campaign. The IRS has reportedly assigned elite veteran criminal agents to investigate whether bitcoin and other cryptocurrencies are being used to evade taxes. Chief of IRS Criminal Investigation Don Fort stated that it is possible to use bitcoin and other cryptocurrencies in the same fashion as foreign bank accounts to facilitate tax evasion and that, while the agency has yet to charge anyone, the cases will come.

Based on this newest campaign, the IRS's enforcement efforts are likely to focus on:

- individuals who redeem, transfer, or exchange virtual currency;
- companies that pay individuals for personal services in virtual currency; and
- individuals who receive compensation in the form of virtual currency for providing personal services.

This sequence of investigative tools implemented by the DOJ and the IRS is strikingly similar to the measures utilized in the Swiss Bank Program.

Importance of Taking Action Now

There is no question that the IRS is prioritizing the enforcement of cryptocurrency reporting. Accordingly, taxpayers and cryptocurrency platforms should prepare for the application of the highly effective, but relatively inexpensive, tools utilized in the Swiss Bank Program to bring those involved in virtual currency transactions into reporting compliance.

Cryptocurrency platforms should be mindful of potential criminal liability for facilitating tax evasion. If the penalties imposed on the non-compliant Swiss banks are indicative of the future treatment of cryptocurrency, then facilitating platforms determined to be complicit in tax evasion can expect to turn over up to 50 percent of the maximum aggregate of all non-compliant accounts. Likewise, taxpayers who intentionally fail to report virtual currency transactions could face severe criminal penalties, such as fines up to $250,000 and imprisonment.[3]

There are measures that cryptocurrency exchange platforms can implement now to avoid or reduce their potential exposure, such as developing corporate compliance programs to ensure their platforms are not being used to facilitate tax evasion. These include policies and procedures, as well as internal controls, to prevent the individuals from intentionally circumventing U.S. laws.

Likewise, individuals who use virtual currency and have concerns that they are not correctly reporting these transactions should seek advice from an attorney or certified public accountant. If the unreported transactions are substantial, the IRS has a voluntary disclosure program that permits individuals and companies who have failed to report substantial amounts of taxes to amend prior tax returns and potentially receive penalty abatements (or at least mitigated penalties) in exchange for coming forward. Individuals considering entering the IRS voluntary disclosure program should seek legal counsel immediately. The program is not open to individuals or companies who are already selected for audit.

The tax man is coming again, and individuals and exchange platforms who do not take action now risk being swept up into the next enforcement wave and likely will face penalties similar to those imposed in the Swiss Bank Program. The risk of detection is high, because the DOJ and the IRS now have a blueprint for successful prosecutions that they are plainly implementing.

1. Internal Revenue Code § 7609(f). A John Doe summons or subpoena does not list the name of the taxpayer under investigation, as the taxpayer is unknown to the IRS.
2. *United States v. Coinbase, Inc.,* No. 17-CV-01431-JSC, 2017 WL 5890052, at *4 (N.D. Cal. Nov. 28, 2017).
3. Willful tax evasion can result in imprisonment and fines up to $250,000. 26 U.S.C. §§ 7201, 7203, 7206. However, if signs of fraud are absent, the IRS may fine the taxpayer a penalty of 20 percent of the underpayment. 1 I.R.M. Abr. & Ann. § 4.10.6.5.

New Treasury Regulations Impose Conflicting Requirements on Foreign Persons with U.S. Interests

BY JED M. SILVERSMITH AND JEFFREY M. ROSENFELD

JED SILVERSMITH
OF COUNSEL

JEFFREY M. ROSENFELD
ASSOCIATE

Few Americans consider the United States to be a money laundering haven, but it is. Earlier this year, the European Parliament wrote:

> The USA is seen as an emerging leading tax and secrecy haven for rich foreigners, when in parallel it has reprimanded other countries for helping rich Americans hide their money offshore. It is difficult to estimate how much revenue the United States loses from tax avoidance and evasion, but some have suggested that the annual cost of offshore tax abuses may be around US $100 billion per year.[1]

To combat U.S. money laundering by foreign citizens, the Internal Revenue Service ("IRS") and the U.S. Department of Treasury Financial Crimes Enforcement Network ("FinCEN") implemented new and strengthened existing reporting requirements for foreign individuals who have financial interests in the United States. Although these regulations are applied broadly, there has been very little discussion about their implementation in the United States. Presumably, there has been even less discussion abroad.

This article focuses on two new, wide-ranging regulatory requirements: 1) the requirement that foreign-owned entities, treated as "disregarded entities" for U.S. federal income tax purposes, file an IRS Form 5472, *Information Return of a 25 Percent Foreign-Owned U.S. Corporation or a Foreign Corporation Engaged in a U.S. Trade or Business;* and 2) the requirement that all entities report beneficial ownership when opening a bank account. Failure to comply with these requirements may subject foreign nationals and U.S. individuals who do business with them to civil and criminal sanctions.

IRS Form 5472 Filing Requirements: Old and New

As has always been the case, an IRS Form 5472 is required to be filed:

> If, at any time during a taxable year, a corporation…
> (1) is a domestic corporation…, and
> (2) is 25-percent foreign-owned.[2]

The IRS Form 5472 has always been intended to be a mechanism for the IRS to obtain information on transactions between a domestic corporation and their foreign owners. The requirements for transactions that trigger an IRS Form 5472 filing are described on the form and are broad. They include most monetary transactions (rent, royalties, payments for services, sale of property, etc.), and also include transactions in which less than full consideration is paid.

The IRS Form 5472 collects the following information: 1) name; 2) principal place of business; 3) nature of the business; and 4) country or countries in which each related party—with any transaction with the reporting corporation—is organized or resides.[3] The form requires that the taxpayer report gratuitous transfers (*i.e.,* gifts).[4] The IRS also has attribution rules, so if a company's shares are owned by close family members, their ownership may be attributed to one person.[5] For example, a domestic corporation, whose members include a father and son who are both foreign persons and both have a 15 percent ownership interest, must file an IRS Form 5472.

While the IRS Form 5472 filing requirements described above are not new, recently enacted Treasury regulations expanded the application of the IRS Form 5472 from domestic corporations to both domestic corporations and entities that are disregarded for U.S. federal income tax purposes ("DE").[6] This is a dramatic change. The transactions that must be reported by a DE are arguably broader than that of a domestic corporation and include:

> any sale, assignment, lease, license, loan, advance, contribution, or any other transfer of any interest in or a right to use any property (whether tangible or intangible, real or personal) or money, however such transaction is effected, and whether or not the terms of such transaction are formally documented. A transaction also includes the performance of any services for the benefit of, or on behalf of, another taxpayer.[7]

A limited liability company formed in the United States and wholly owned by a foreign person will be subject to the reporting requirements of Section 6038A.[8]

How does a DE file an IRS Form 5472 (which is required to be attached to a U.S. tax return) when a DE does not have a U.S. tax return filing obligation to begin with? The Treasury Regulations cross-reference the instructions to IRS Form 5472, which require that all DEs file a *pro forma* tax return on IRS Form 1120 and attach the IRS Form 5472 to the IRS Form 1120.[9] The only information required on an IRS Form 1120 filed by a DE is its name and address, its employer identification number, and Box E of the IRS Form 1120. "Foreign-owned U.S. DE" should be written across the top of the Form 1120 with Form 5472 attached, and it may be faxed or mailed to the IRS.

For example, suppose a Canadian citizen purchases a winter home in South Florida. As is the case with many individuals who may want to make a real estate purchase with some level of anonymity, he/she can title the property in the name of a LLC. This LLC, historically, would never have had any U.S. tax filings obligations. Under the new Treasury regulations described above, the LLC must now must file a Form 5472 every year (along with a *pro forma* IRS Form 1120) because a reportable transaction includes a right to use property granted by a DE (*i.e.,* the LLC) to a foreign-related party.[10]

These rules discussed above are in addition to the long-standing reporting requirements imposed on foreign corporations that are engaged in a U.S. trade or business in the United States during a taxable year.[11] The IRS requires that any foreign corporation engaged in a U.S. trade or business file an IRS Form 5472. Foreign corporations are corporations that incorporated offshore.[12] Thus, a corporation can be foreign even if its shareholders are U.S. persons.

An IRS Form 5472 is generally due on the successive March 15 for that calendar year (*e.g.,* the 2017 form was due on March 15, 2018). It must be filed with an IRS Form 1120—corporate tax return—even if the entity does not pay U.S. taxes, and in the case of a DE, it must be filed with a *pro forma* IRS Form 1120.

Failure to file the IRS Form 5472 subjects the entity to a $25,000 penalty.[13] The penalty is continuing, meaning that additional $25,000 penalties accrue each month after the taxpayer is placed on notice that it is not in compliance.[14] The penalty is not subject to regular audit deficiency procedures, and the taxpayer may waive his right to present evidence at any hearing if he does not respond to the IRS at the first opportunity, which differs from typical procedures where the IRS gives the taxpayers multiple opportunities to comply.[15]

Effective May 11, 2018, All Legal Entities Must Disclose Any Natural Person with Control of *and* a 25 Percent or Greater Interest in the Entity to Financial Institutions

Separate and apart from the new IRS filing requirement imposed on DEs, effective May 11, 2018, any legal entity (domestic or foreign) opening an account at specified financial institutions (*i.e.,* bank accounts, securities accounts, and futures trading accounts) must verify the identity of:

1) each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer; and
2) a single individual with significant responsibility to control, manage, or direct a legal entity customer, including:
   i) an executive officer or senior manager (*e.g.,* a chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president, or treasurer); or
   ii) any other individual who regularly performs similar functions.[16]

These FinCEN regulations apply to any entity opening an account, including limited liability companies, corporations, and trusts. FinCEN's rule differs from the IRS Form

5472 rules, so one needs to carefully consider the separate requirements for both rules. In particular, the Form 5472 rules focus exclusively on ownership, not control, whereas

> Failure to comply with these requirements may subject foreign nationals and U.S. individuals who do business with them to civil and criminal sanctions.

FinCEN's rules require that covered financial institutions identify a controlling person with less than a 25 percent ownership stake as well individuals with a 25 percent or greater interest. The IRS Form 5472 also requires an attribution analysis. Consequently, multiple family members are considered to be one person for IRS purposes, but not when disclosing their identity to a financial institution. Thus, a family-owned business might be required to file an IRS Form 5472 listing individual family members but not identify family members to U.S. financial institutions where the entity has a U.S. bank or trading account.[17]

The FinCEN rules are prospective and financial institution are not required to verify the ownership interest in current accounts:

> The obligation to obtain or update beneficial ownership information on legal entity customers with accounts established before May 11, 2018, is triggered when a financial institution becomes aware of information about the customer during the course of normal monitoring relevant to assessing or reassessing the risk posed by the customer, and such information indicates a possible change of beneficial ownership.[18]

However, when an account holder opens a new account or takes other action such as renewing a loan or rolling over a certificate of deposit, FinCEN requires the entity to provide evidence of the identity of the natural person who has a beneficial interest via a driver's license or passport. Financial institutions may use non-documentary methods of verification such as contacting the natural person or references with other financial institutions.

Individuals who submit false or misleading information to financial institutions are subject to criminal prosecution under the bank fraud and money laundering statutes. Banks that are skeptical of the information furnished by the customer may close the account, file a suspicious activity report, or both.

In light of the interest in financial transparency, expect vigorous enforcement of these new statutes and regulations. Foreign citizens and companies with U.S. financial interests should consult with U.S. counsel to determine if they are complying with these regulations. ◘

1. *EU-US Trade and Investment Relations: Effects on Tax Evasion, Money Laundering and Tax Transparency,* p. 6, (Mar. 2017), available at europarl.europa.eu/RegData/etudes/IDAN/2017/598602/EPRS_IDA(2017)598602_EN.pdf.
2. Section 6038A of the Internal Revenue Code of 1986, as amended (the "Code").
3. A copy of the form can be found here: irs.gov/pub/irs-pdf/f5472.pdf.
4. 26 C.F.R. § 1.6038A-2(b)(4).
5. 26 C.F.R. § 1.6038A-1(e) (citing 26 U.S.C. § 318).
6. 26 C.F.R. § 1.6038A-1(c)(1).
7. *See* 26 C.F.R. § 1.482-1(i)(7) and IRS Form 5472, Filing Instructions, Part V ("You must check the box in Part V if you are a foreign-owned DE that had any other transaction as defined by Regulations section 1.482-1(i)(7) not already entered in Part IV. These transactions include amounts paid or received in connection with the formation, dissolution, acquisition and disposition of the entity, including contributions to and distributions from the entity.").
8. Note that in order to file an IRS Form 5472, one must obtain a taxpayer identification number by filing a Form SS-4, which will identify a responsible party.
9. *See* IRS Form 5472, Filing Instructions, When and Where to File.
10. *See* IRS Form 5472 instructions, Part V. *See also* 26 C.F.R. § 1.482-1(i)(7).
11. *See* U.S.C. § 6038C.
12. *See* 26 U.S.C. § 7701(a)(5).
13. Congress raised the penalty from $10,000 to $25,000 in 2017. However, the regulations have not been amended and still reflect the lower amount. 26 C.F.R. § 1.6038A-4. An argument can be made that the lower amount should apply. *See United States v. Colliot,* AU-16-CA-01281-SS, 2018 WL 2271381 (W.D. Tex. May 16, 2018).
14. 26 C.F.R. § 1.6038A-4(a)(3). Separate penalties may be assessed for failing to comply with the requirement to produce records.
15. 26 C.F.R. § 1.6038A-6.
16. FinCEN FAQ 13; 31 C.F.R. § 1010.230.
17. FinCEN does not require identification of the beneficiary of the trust even though the bank account is held for the benefit of the trust's beneficiary/beneficiaries.
18. Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (Apr. 3, 2018), available at fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf.

Notable Industry Events & Presentations

Featured Event

Cryptocurrency: Trash or Treasure?

Co-sponsored by Blank Rome LLP and the Pennsylvania Association of Criminal Defense Lawyers White Collar Practice Committee

Wednesday, October 10 • 6:00–8:00 p.m.
Blank Rome's Philadelphia Office

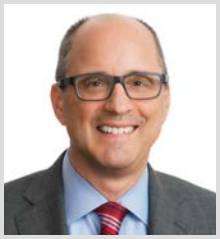
One Logan Square • 130 North 18th Street Philadelphia, PA 19103

Click here to register.

This complimentary CLE will cover the latest information on cryptocurrency, including:

- Introduction to blockchain, cryptocurrency, and ICOs/token offerings
- Update on the SEC's new cyber unit and recent SEC enforcement actions
- Discussion on what other regulators are doing

BLANK ROME PARTICIPANTS



Joseph G. Poluka
Course Planner and Moderator
Partner, White Collar Defense & Investigations

Mark M. Lee
Course Planner
Partner, White Collar Defense & Investigations

Michelle Ann Gitlitz
Panelist
Partner & Co-Chair, Blockchain Technology & Digital Currencies

Please contact **Marianne Talbot** for more information about this event.

Recent and Upcoming Events

- **Mayling C. Blanco** served as a panelist for Leave Your Wallets at Home! Legal Trends Surrounding the Emergence and Regulations of Cryptocurrencies, Initial Coin Offerings & Distributed Ledger Technologies at the 2018 Hispanic National Bar Association Annual Convention (September 6, 2018).
- **Bridget Mayer Briggs** presented on Using Electronic Evidence at the Pennsylvania Bar Institute's Skills of the Successful Lawyer 2018 (August 16, 2018).
- **Mark M. Lee** (along with numerous other Blank Rome attorneys) presented on The #MeToo Minefield: From Privilege to Punitives at a Blank Rome webinar (May 8, 2018).
- **Nicholas C. Harbist** moderated The Intersection of Compliance and Risk Management at a Rutgers School of Law CLE (April 13, 2018).
- **Carlos F. Ortiz** and **Shawn M. Wright** (along with numerous Blank Rome attorneys) presented on Blockchain and Cryptocurrency Litigation Concerns: Class Actions, Criminal Exposure, and Criminal Tax Implications at a Blank Rome webinar (April 11, 2018).