BLANK ROME LLP
COUNSELORS AT LAW

MARCH 2017 • VOL 1, ISSUE 1

White Collar Watch

INSIDE

THIS ISSUE

A NOTE FROM THE EDITORS

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, or self-discovered misconduct. With the relaunch of this quarterly newsletter, our team of white collar attorneys will discuss key industry topics and provide insightful analysis on a wide range of practical issues potentially impacting companies and individuals within numerous industries.

Authored by members of our team, many of whom are former prosecutors, this inaugural edition features articles on the Foreign Corrupt Practices Act, the "FinTech" industry, Department of Justice compliance updates, and the impact of IRS tax liens on passport revocations.

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 whom you think may find it useful. Our White Collar Defense & Investigations practice group is here to be of service to you, and your companies, in every way possible.

With warm regards,

Joseph G. Poluka, Inbal Paz Garrity, and William B. Shields

Editors, *White Collar Watch*

Poluka@BlankRome.com

JOSEPH G. POLUKA

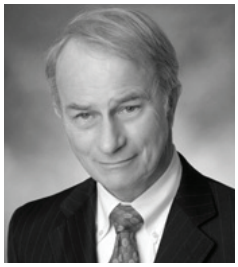
PARTNER

IPaz@BlankRome.com

INBAL PAZ GARRITY

PARTNER

WShields@BlankRome.com



WILLIAM B. SHIELDS

OF COUNSEL

New York Department of Financial Services Implements New "First-in-the-Nation" Cybersecurity Regulations

BY INBAL PAZ GARRITY AND NICHOLAS R. TAMBONE


IPaz@BlankRome.com
INBAL PAZ GARRITY
PARTNER


NTambone@BlankRome.com
NICHOLAS R. TAMBONE
ASSOCIATE

As of March 1, 2017, New York financial institutions subject to the oversight of the New York Department of Financial Services ("DFS") are required to comply with a new cybersecurity regulatory scheme. Compliance deadlines for certain measures are coming as early as August 28, 2017. Affected financial institutions should take action now to ensure timely compliance.

Following months of public comments and revisions, DFS' new cybersecurity regulations, 23 NYCRR §§ 500.00-500.23, went into effect on March 1, 2017.[1] Entitled "Cybersecurity Requirements For Financial Services Companies," these "first-in-the-nation"[2] cybersecurity rules are "designed to promote the protection of customer information as well as the information technology systems of regulated entities." In short, the regulations require New York financial institutions subject to the oversight of DFS ("Covered Entities") to adopt a robust cybersecurity program and policy, and the first compliance deadline is coming this summer.

Failure to comply with the new regulations may result in fines or other civil penalties. Here are the specific deadlines for the new measures that you need to be aware of:

August 28, 2017: 180-Day Transition Period Ends
Although the new regulations went into effect on March 1, 2017, DFS has provided for a transition period, which ends after 180 days, or August 28, 2017. Covered Entities are required to be in compliance with a number of the new regulations by that date. Covered Entities will then have additional time to comply with certain enumerated regulations, which are described below.

1. 23 NYCRR § 500, available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.
2. Press Release, N.Y. Dep't of Fin. Servs., "DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions" (Dec. 28, 2016), available at http://www.dfs.ny.gov/about/press/pr1612281.htm.

February 15, 2018: First Certification of Compliance Due to DFS
Beginning on February 15, 2018, and continuing on an annual basis thereafter, Covered Entities must submit to the superintendent of DFS a written statement certifying that the Covered Entities are in compliance with the regulations.[3]

March 1, 2018: One-Year Additional Transition Period Ends
By March 1, 2018,[4] a Covered Entity must be in compliance with the following provisions:

- Regulations concerning the annual report of the Chief Information Security Officer ("CISO") to the Covered Entity's board of directors.[5]
- Regulations concerning annual penetration testing and bi-annual vulnerability assessments of the Covered Entity's Information Systems.[6]
- Regulations concerning periodic risk assessment of the Covered Entity's Information Systems.[7]
- Regulations concerning the implementation of multi-factor authentication.[8]
- Regulations concerning cybersecurity awareness training.[9]

September 1, 2018: 18-Month Additional Transition Period Ends
By September 1, 2018,[10] a Covered Entity must be in compliance with the following provisions:

- Regulations concerning reconstruction of material financial transactions and audit trails.[11]
- Regulations concerning application security.[12]
- Regulations concerning data retention and secure disposal of nonpublic information.[13]

3. 23 NYCRR §§ 500.17(b), 500.21.
4. *Id*. § 500.22(b)(1).
5. *Id*. § 500.04(b).
6. *Id*. § 500.05.
7. *Id*. § 500.09.
8. *Id*. § 500.12.
9. *Id*. § 500.14(a)(2).
10. *Id*. § 500.22(b)(2).
11. *Id*. § 500.06.
12. *Id*. § 500.08.
13. *Id*. § 500.13.

- Regulations concerning the monitoring of authorized users.[14]
- Regulations concerning encryption of nonpublic information.[15]

March 1, 2019: Two-Year Additional Transition Period Ends

By March 1, 2019,[16] a Covered Entity must be in compliance with regulations concerning third-party service providers.[17] Essentially, this regulation will require a Covered Entity to implement written policies and procedures designed to ensure that a Covered Entity's vendors and other third parties with access to nonpublic information employ adequate cybersecurity practices.

Blank Rome's White Collar Defense and Investigations practice group is well-positioned to advise clients on legal compliance with areas under the oversight of DFS and cybersecurity matters. Our attorneys are also available to provide tailored compliance training to high-risk employees.

14. *Id*. § 500.14(a)(1).
15. *Id*. § 500.15.
16. *Id*. § 500.22(b)(3).
17. *Id*. § 500.11.

BLANK ROME NEWS

MBlanco@BlankRome.com
MAYLING C. BLANCO
PARTNER

The Blank Rome White Collar Defense & Investigations group is proud to announce the promotion of **Mayling C. Blanco** to partner.

Ms. Blanco represents corporations and individuals in white collar defense, government investigations, and commercial litigation matters, notably concentrating her practice on the Foreign Corrupt Practices Act and corporate fraud, as well as matters implicating criminal tax exposure. She has conducted domestic and international, multijurisdictional investigations for clients with ventures in Latin America, Asia, and Europe, and has represented her clients before the U.S. Department of Justice's Criminal, Civil, and Tax Divisions. She also advises corporations and financial institutions in connection with corporate governance and compliance matters. In litigation, Ms. Blanco has experience before various Federal District Courts, U.S. Tax Court, the Superior Court of New Jersey, the New Jersey Appellate Division, and the New Jersey Supreme Court, defending clients in white collar, tax, commercial, employment, and constitutional matters. She is a member of the Seton Hall Alumni Council, the Firm's Diversity Committee, and active with the Hispanic National Bar Association and the New Jersey Hispanic Bar Association. She practices in Blank Rome's New York and Princeton, N.J. offices.

U.S. Department of Justice Issues New Guidance on Corporate Compliance Programs

BY SHAWN M. WRIGHT, CARLOS F. ORTIZ, AND NICHOLAS R. TAMBONE


Wright@BlankRome.com
SHAWN M. WRIGHT
PARTNER


COrtiz@BlankRome.com
CARLOS F. ORTIZ
PARTNER


NTambone@BlankRome.com
NICHOLAS R. TAMBONE
ASSOCIATE

The U.S. Department of Justice ("DOJ") Criminal Division, Fraud Section, recently published new guidance on corporate compliance programs. All corporate counsel, officers, and directors should be aware of this guidance, and corporate compliance professionals should ensure not only that compliance policies follow this guidance, but that actual practices also meet the expectations outlined by the DOJ.

On February 8, 2017, the DOJ published guidance entitled, "Evaluation of Corporate Compliance Programs,"[1] which "provides some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program." This is important information for every business to be aware of, and this guidance is particularly interesting because it is the first formal guidance issued by the DOJ under the Trump administration and Attorney General Jeff Sessions.

Federal prosecutors are guided by factors set forth in "The Principles of Federal Prosecution of Business Organizations," published in the *United States Attorneys' Manual*[2], when determining whether to bring criminal charges against a corporate entity. Among these so-called "Filip Factors" are "the existence and effectiveness of the corporation's pre-existing compliance program," and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."[3]

1. U.S. Department of Justice, Criminal Division, Fraud Section, "Evaluation of Corporate Compliance Programs," available at www.justice.gov/criminal-fraud/page/file/937501/download.
2. U.S. Attorneys' Manual § 9-28.000, available at www.justice.gov/usam/usam-9-28000-principles-federal-prosecution-business-organizations.
3. Id. § 9-28.300, available at www.justice.gov/usam/usam-9-28000-principles-federal-prosecution-business-organizations#9-28.300.

The DOJ's new compliance guidance sets forth 11 high-level topics. The topics are compiled from other resources, including the *United States Attorneys' Manual*; the *United States Sentencing Commission's Guidelines Manual*; the DOJ's November 2012 publication, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*; and the Organization for Economic Co-operation and Development Council's 2013 publication, *Anti-Corruption Ethics and Compliance Handbook for Business*, among others.

The 11 High-Level Topics in the Guidance Are:

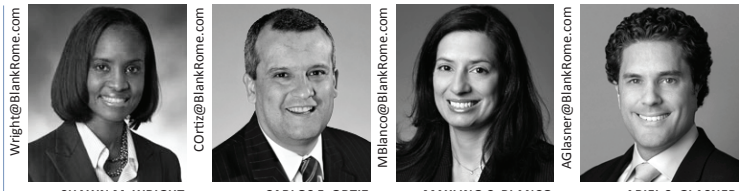
1. Analysis and Remediation of Underlying Conduct
2. Senior and Middle Management
3. Autonomy and Resources
4. Policies and Procedures
5. Risk Assessment
6. Training and Communications
7. Confidential Reporting and Investigation
8. Incentives and Disciplinary Measures
9. Continuous Improvement, Periodic Testing, and Review
10. Third Party Management
11. Mergers and Acquisitions

Under each of these 11 topics, the DOJ's guidance sets forth multiple sample questions that prosecutors are likely to probe into during an investigation. A few examples are:

- **Analysis and Remediation of Underlying Misconduct:** Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations involving similar issues?
- **Senior and Middle Management:** How has senior leadership modelled proper behavior to subordinates?
- **Risk Assessment:** What methodology has the company used to identify, analyze, and address the particular risks it faced?
- **Training and Communications:** What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees that addressed the risks in the area where the misconduct occurred?
- **Confidential Reporting and Investigation:** How has the company collected, analyzed, and used information from its reporting mechanisms? —

The Global Anti-Corruption Corner: A Primer to the Foreign Corrupt Practices Act

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



Any company doing business abroad is subject to the long reach of the Foreign Corrupt Practices Act ("FCPA"). Small or privately held companies, just like large or public companies, are subject to the criminal specter of the FCPA. The operative inquiry is whether the company is operating and/or transacting any type of business abroad with the government, government-owned entities, or involving foreign officials—either directly, through joint ventures, or indirectly, through agents. A foreign official also includes employees of entities owned by the government.

Although the FCPA was first enacted in 1977, it was not widely enforced until the turn of this century; since then, the law has resulted in a steady flow of significant corporate settlements. Indeed, in the last approximately two decades, enforcement of the FCPA has increased exponentially, with the second-largest number of enforcement actions having been brought in 2016 (2008 had the greatest number). Before the FCPA, no country considered bribing a foreign official for business purposes to be illegal—it was simply considered a cost of doing business abroad. The United States was the first country to outlaw the practice and recently published a comprehensive resource guide to compliance with the act.

Presently, for companies that are engaged in international business, some of the countries that are considered high risk for FCPA exposure include Mexico, Panama, Russia, China, Ukraine, Brazil, Nigeria, and Lebanon.

The following is a primer about FCPA and its basic provisions.

What Is the Foreign Corrupt Practices Act?

The FCPA targets public corruption and fraud in the international marketplace. It does so in two main ways:

1. The FCPA prohibits any U.S. person or entity (including privately held companies), or any issuer of U.S. securities, from making any corrupt payment or offering anything of value to any foreign official for the purposes of obtaining or retaining business, or gaining any improper advantage. The statute covers U.S. companies, citizens, and permanent residents (and their agents) anywhere they act in the world. The act also specifically covers foreign individuals and entities so long as any aspect of the transaction touches U.S. soil.

2. The FCPA requires all companies whose securities are listed on U.S. stock exchanges to maintain accurate accounting records and implement an adequate system of internal controls. This provision of the FCPA is generally referred to as the "book and records" provision and can have a very broad interpretation.

Very importantly, the FCPA ascribes liability to companies both for the actions of its own employees and for any third-party acting on the company's behalf, as well as individuals involved or authorizing such conduct.

What Is a "Thing of Value?"

A "thing of value" has had an evolving focus. While the initial FCPA violations involved cash and luxurious gifts, more recent cases have reflected an increasing sophistication of the term to include: cash equivalents (gift cards); excessive travel and entertainment; loans; political and charitable contributions or donations; and employment, internships, or scholarships. The "thing of value" may be for the benefit of the official directly, but also includes anyone in their family.

What Are Penalties for Violations of the FCPA?

For companies, violations of the FCPA carry hefty financial penalties that amount to hundreds of millions of dollars. In addition to the financial penalties, negotiated settlements with the government typically require the disgorgement of any profits resulting from the unlawful conduct, an agreement to cooperate with government investigations for a period of multiple years, and the implementation of an enhanced compliance program. Companies can also be fined by multiple countries if the conduct violates the other country's anti-corruption statute.

In recent years, the government has also sought to hold individuals accountable for FCPA violations. Accordingly, corporate resolutions of FCPA investigations are now often accompanied by prosecutions of individuals the government considers responsible for corporate wrongdoing. *(See chart on next page.)*

How Are FCPA Violations Discovered?
FCPA violations are discovered in numerous ways, both inside and outside of the company.

Internally, potential FCPA violations can be discovered through the report of a whistleblower to company management or via a report from an internal compliance hotline. Routine business activities, such as the reimbursement of expenditures, can trigger investigations by a company's compliance or legal department, as can less routine activities such as compliance audits and due diligence related to company acquisitions. The Securities and Exchange Commission ("SEC") also has a very user-friendly whistleblower website that is available to individuals across the globe.

Externally, FCPA investigations can be triggered by whistleblower reports, court filings in lawsuits brought by private plaintiffs, enforcement actions brought by foreign governments, or even by anonymous tips.

Who Enforces the FCPA?
The FCPA is primarily enforced by the U.S. Department of Justice ("DOJ") (anti-bribery provisions) and the SEC (books and records and internal controls provisions). The DOJ and SEC have increased their concerted efforts to coordinate their investigations with foreign prosecutorial agencies, an initiative that has been enhanced by the proliferation of anti-bribery laws in other countries. Accordingly, many FCPA investigations now expand into multi-lateral prosecutions and investigations.

What Should a Company Do When a Potential Violation Arises?
If a company suspects that a potential FCPA violation has occurred or that it is being investigated by a government agency, it may, in coordination with its legal counsel, consider one or a combination of several steps. These steps may include, for example, the company conducting its own investigation to assess the scope of the alleged wrongdoing, considering a voluntarily disclosure of unlawful conduct to the government, cooperating with a government's investigation into a specific industry or number of companies, improving its compliance program, and remediating the harm that has resulted from the alleged unlawful conduct.

How Can a Company Protect Itself?
While a given company's FCPA exposure depends on various factors, including the industry in which the company operates, as well as the countries in which it does business, FCPA compliance programs typically include the following:

- a clear set of policies and procedures regarding anti-corruption compliance;
- a comprehensive training program to educate employees about anti-corruption laws (including the FCPA) applicable to the company's operations and compliance of such laws; and
- processes for ensuring that appropriate due diligence is undertaken for new hires, including third-party agents, and for the acquisition of any new ventures, particularly with respect to foreign entities.

The Global Anti-Corruption Corner will appear as a regular column in this newsletter, and will focus on legal issues related to the FCPA and other anti-bribery laws.

	Maximum Fine Per Count (Corporations)	Maximum Fine Per Count (Individuals)	Maximum Imprisonment Per Count (Individuals)
Anti-Bribery Violations	$2 million	$100,000	5 years
Accounting Violations	$25 million	$5 million	20 years

The FinTech Revolution: An Introduction to Financial Technology

BY ARIEL S. GLASNER AND BRIDGET BRIGGS

"FinTech" has become a buzzword of the decade. The term, which is a moniker for "financial technology," captures all manner of technological innovation in personal and commercial finance; innovations that are increasingly gaining the attention of regulators seeking to prevent money laundering and financial frauds. FinTech includes applications that support and enable financial and banking services, such as mobile banking apps, credit card strip readers that attach to mobile devices and tablets, and software that allows companies to process payments from customers. It also encompasses technology that has changed the way money is exchanged, such as through peer-to-peer lending apps, programs that permit monetary transfers online or through mobile devices, and financial advisory and online wealth management services that provide automated, algorithm-based portfolio management advice. Additionally, FinTech includes cryptocurrencies like Bitcoin, which are "virtual currencies" that exist in databases and are transacted through online networks, but, unlike physical currencies, have no intrinsic value, no physical form, and are not regulated through a central bank.

The products and services that fall under the FinTech umbrella have led to a significant disruption of the financial services industry. Part of this disturbance is attributable to the fact that FinTech is designed to make financial transactions more accessible. Accordingly, companies like Square, PayPal, and Venmo offer mobile payment services, which permit business customers to pay for products and services in new ways; companies like Prosper, Funding Circle, and Lending Club provide loan options not offered by banks; and other companies like TransferWise and World Remit provide online money transfer services as alternatives to visiting the local Western Union or MoneyGram outlet. FinTech has provided a channel for startup companies to challenge an industry that historically has been dominated by big banks, which, as with many blue chip companies, are generally more resistant to change.

In challenging the status quo, FinTech companies have raised a variety of legal issues, including whether the regulatory framework that, until now, primarily has applied to large financial institutions, applies to these startup companies and is suitable for a rapidly changing industry. As white collar practitioners, we are well-positioned to advise FinTech companies and their customers so that they have an understanding of the tools that are available to law enforcement authorities in regulating FinTech, the enforcement actions that already have been pursued, and whether new regulations might be on the horizon. Over the course of the next several editions of this newsletter, we will examine these issues, including, for example:

- How are FinTech companies subject to Anti-Money Laundering/Bank Secrecy Act Requirements?
- What enforcement actions have been brought against cryptocurrencies to ensure that they do not proliferate as a vehicle for malfeasance?
- What steps are government agencies proactively taking to address FinTech?

We look forward to sharing our insights and to exploring this exciting young industry in future issues of this newsletter.

IRS Announces Plans to Move Forward with Passport Revocation Program

BY JED M. SILVERSMITH AND JEFFREY M. ROSENFELD

United States citizens who owe more than $50,000 in unpaid federal taxes are at substantial risk of having their U.S. passports revoked within the next few months and should contact counsel for help with reaching an immediate resolution with the Internal Revenue Service ("IRS"). Citizens living abroad also should be aware that they may be forced to return to the United States until they resolve their tax debts.

In December 2015, Congress enacted legislation requiring the IRS to provide a list of names to the State Department of individuals with "seriously delinquent tax debt."[1] That term was defined in the statute to mean tax debt of over $50,000, including interest and penalties. 26 U.S.C. § 7345(b). The legislation also requires that the State Department refuse to issue new passports, and gives it the discretion to revoke currently issued passports. *See* 22 U.S.C. § 2714A.

In February 2017, the IRS announced that it would begin sending, within 30 days, IRS Letters 508C, notice of certification of seriously delinquent federal tax debt to the State Department, to the taxpayer's last known address. The letter will inform the taxpayer that the IRS has certified him/her as owing "seriously delinquent tax debt." At that time, the IRS also will send the certification to the State Department.

The IRS reports that the State Department will take action within 90 days. Taxpayers who have a tax debt can avoid passport revocation only if the taxpayer pays the tax in full or enters into an installment agreement or an offer in compromise with the IRS. Taxpayers who have made a timely request for a collection due process hearing also can avoid revocation while the hearing is pending. Of particular note, the 2015 legislation severely limits the right of an individual to appeal the IRS' and State Department's decision, so individuals who have substantial tax debt will have to come into compliance. —©2017 Blank Rome LLP

To learn more about Blank Rome's White Collar Defense & Investigations group, visit www.blankrome.com.

SPEAKING ENGAGEMENTS

Joseph G. Poluka:
The Pendulum Has Swung: Off-Label Use and a New World Order at the American Conference Institute's 29th FDA Boot Camp, March 24, 2017, in New York, NY.

Mayling C. Blanco:
Corruption in the GlobalGateway: Developments and Enforcement Trends Under the FCPA and Other Anti-Bribery Laws at the Hispanic National Bar Association Corporate Counsel Conference & Moot Court Competition, March 31, 2017, in Miami, FL.

Carlos F. Ortiz and Mayling C. Blanco:
Hot topics – Criminal Tax Enforcement at the 2017 New Jersey State Bar Association Annual Meeting, May 17-19, 2017, in Atlantic City, NJ.