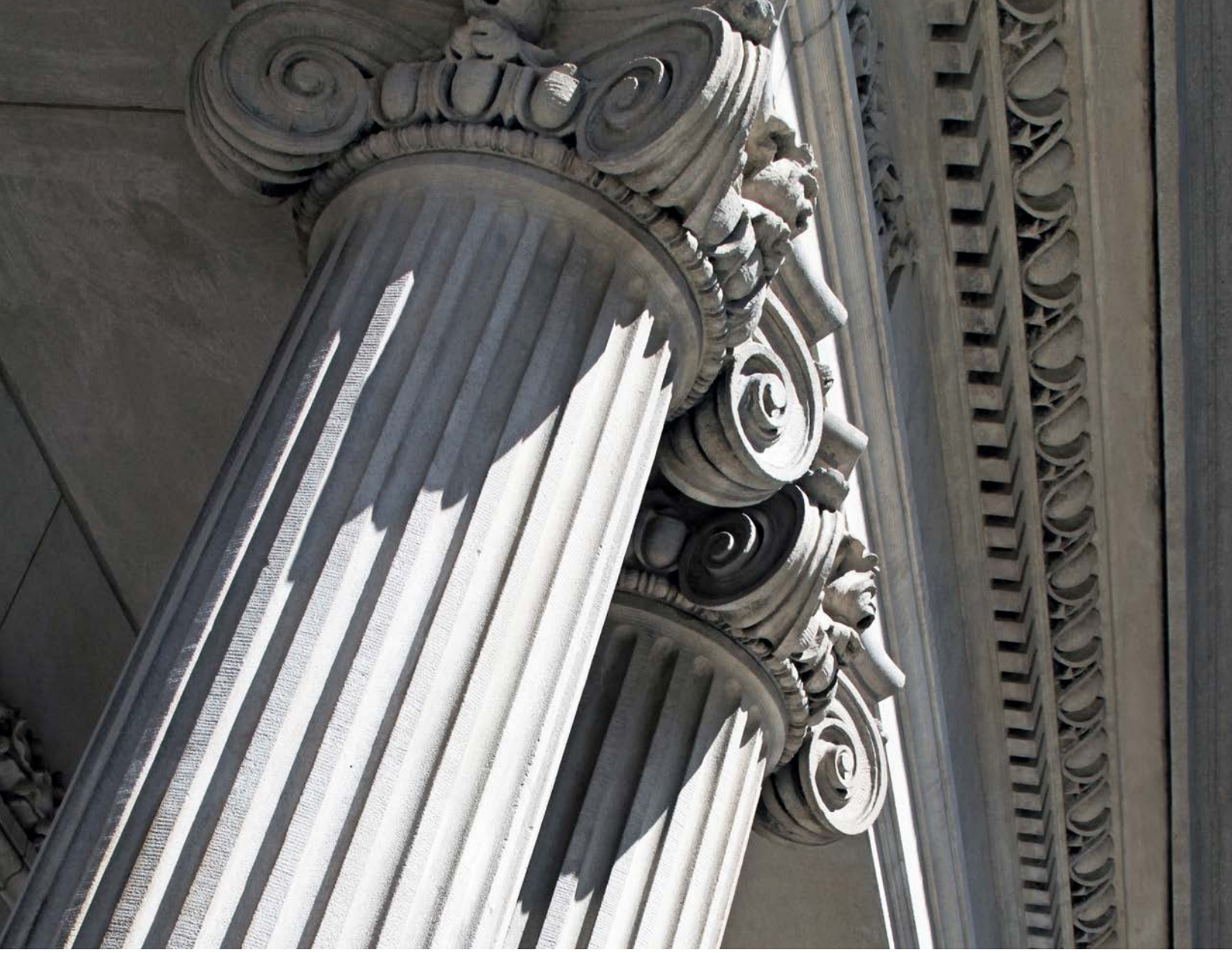


WHITE COLLAR WATCH

BLANKROME

DECEMBER 2018 • NO. 3

CONTENTS

Note from the Editors

All of us here at Blank Rome wish you and yours a happy and healthy holiday season and start to 2019.

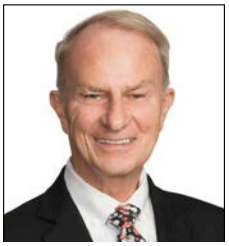
We are pleased to present our final 2018 edition of *White Collar Watch,* which includes timely articles that address key industry issues, such as how to avoid fraud in the areas of merchants' use of "sales suppression software" as well as in the FinTech space. In addition, Blank Rome's Insurance Recovery team discusses recent court decisions that could limit a company's ability to recover for SEC disgorgements. We also are alerting you to a new Department of Justice program—the "China Initiative"—that specifically targets Chinese companies at a level not previously seen. Lastly, this edition includes continued discussions of recent False Claims Act and Foreign Corrupt Practices Act developments.

We hope this edition is of interest to you and your company, and thank you for your readership and friendship this past year. We look forward to being of service to you in 2019.

With warm regards,

JOSEPH G. POLUKA
PARTNER

INBAL P. GARRITY
PARTNER



WILLIAM B. SHIELDS
OF COUNSEL

EDITORS, *WHITE COLLAR WATCH*

Don't Get Zapped: Enforcement against Businesses That Use Sales Suppression Software Is on the Upswing

BY JED M. SILVERSMITH

JED M. SILVERSMITH
OF COUNSEL

State and federal authorities are ramping up civil and criminal enforcement efforts against merchants who use electronic sales suppression ("ESS") software, also known as zappers and phantom-ware (collectively "zappers"). These devices are usually software patches that retailers apply to their Point of Sale ("POS") software. POS software is designed to record every transaction, and its internal records usually cannot be altered by the retailer (or its employees). When zappers are installed (usually by a USB flash drive), some percentage of the business' transactions are never recorded, thereby permanently altering corporate books and records from the outset. Given that zappers are usually only operational when a flash drive is plugged into the POS software, it is next to impossible for outside auditors to detect their use. Obviously, in a cash-intensive business, the use of a zapper makes recreating a paper trail impossible.

In the last few years, state governments have placed a greater emphasis on identifying merchants that use zappers. Their concern is real. In 2011, the province of Quebec began ordering certain retailers to install "black boxes," which served as a state-controlled backup to the POS software. Boston University Professor Richard Ainsworth compared the sales data in Quebec from before and after black boxes were in effect. Extrapolating this data to the United States, he concluded that there has been a $21 billion annual loss for state taxing authorities, including a $1.8 billion shortfall for New York, $799 million shortfall for New Jersey, and $922 million shortfall for Pennsylvania.[1]

Authorities Are Fighting Back

On August 9, 2018, the U.S. Attorney for the Northern District of Illinois indicted five Chicago-area restaurants for under-reporting their gross receipts with the aid of zappers.[2] One restaurant owner also was prosecuted by the Illinois Department of Revenue.[3]

Zapper enforcement has been on the upswing in Pennsylvania, too. On May 9, 2018, Governor Tom Wolf presented the Governor's Award for Excellence to seven employees of the Pennsylvania Department of Revenue for their efforts in abating pervasive use of zappers throughout the Commonwealth.[4] In his announcement, Governor Wolf stated that the team collected over six million dollars in unreported sales tax revenue, much of which was concealed using zappers.

During a May 16, 2018, presentation to the Pennsylvania Restaurant and Lodging Association, employees of the Department of Revenue provided additional statistics. The Department reported that, between 2014 and 2017, it conducted 176 audits and uncovered $78 million in unreported sales. It also reported that over 40 percent of the companies that it audited used some type of zapper software.

In 2016, Pennsylvania enacted Bill 84 (codified at 72 Pa. Cons. Stat. § 7268), which makes it a misdemeanor to "purchase[], install[] or use[]" zappers. Pennsylvania joined at least 26 other states that have enacted similar anti-zapper statutes.[5] New York is considering Senate Bill S5852A, a similar

law, which makes it a felony to knowingly "purchase, possess, install, update, maintain, upgrade, transfer, or use" a zapper. Washington state requires businesses found to have used this technology to adopt "…electronic monitoring of the business's sales, by a method acceptable to the department [of Revenue]," if they want to remain in business. R.C.W. 82.32.290. *See also* R.C.W. 82.32.670.

Possession or use of zappers is *per se* evidence of tax fraud. Businesses that use these devices will be subject to heightened penalties. Because sales tax is collected by the merchant for the state, it is usually considered a trust fund tax (*i.e.,* the merchant holds the tax on behalf of the state). In a number of jurisdictions, including New Jersey, New York, and Pennsylvania, individuals are personally liable if they fail to pay the company's state sales tax.

State revenue departments and the Internal Revenue Service ("IRS") share information—if an individual is audited by one governmental entity, the results are available to the other entity. Thus, individuals who use zappers and are caught by state taxing authorities may ultimately have to face the IRS.

These five Illinois cases against Chicago-area restaurants appear to be the first federal cases against businesses that use zappers.[6] This is surprising, because businesses that evade state income taxes usually evade federal income taxes, as well. Just by way of example, if a Pennsylvania business "skims" $100,000 in cash receipts, it is failing to pay about $5,660 in Pennsylvania state sales tax. If the skim is used to fund a cash payroll, then the employer is also liable for $15,300 in FICA (*i.e.,* Social Security and Medicare) taxes. State revenue departments and the Internal Revenue Service ("IRS") share information—if an individual is audited by one governmental entity, the results are available to the other entity. Thus, individuals who use zappers and are caught by state taxing authorities may ultimately have to face the IRS.

Don't Get Zapped!

Businesses that use zappers do have an opportunity to come clean. The IRS and state authorities, including New Jersey, New York, and Pennsylvania, have voluntary disclosure programs. Individuals and businesses who enter the program are immunized from criminal prosecution and generally pay a penalty (usually less than the penalty assessed during civil audits).

If you are involved in operating a business that uses or used a zapper, you may wish to contact a lawyer. If you are a tax return preparer whose client uses or used a zapper, you should also determine whether you and/or your client needs counsel. ◻

1. *See* Tax-Zapping Software Costing States $21 Billion, *Bloomberg,* Sept. 15, 2017.
2. *See* justice.gov/usao-ndil/pr/owners-five-chicago-area-restaurants-charged-federal-investigation-targeting.
3. *See* illinoisattorneygeneral.gov/pressroom/2017_08/20170802.html.
4. *See* media.pa.gov/Pages/Revenue-details.aspx?newsid=251.
5. *See* bna.com/taxzapping-software-costing-n57982088046.
6. In 2016, the U.S. Attorney's Office for the Western District of Washington prosecuted a defendant for wire fraud and conspiracy to defraud the government, based upon his sale of zapper software. *See* justice.gov/usao-wdwa/pr/everett-software-salesman-sentenced-prison-selling-tax-zapper-software-enable-cheating.

DOJ Declares "Enough Is Enough"—Targets Chinese Companies with "China Initiative"

BY CARLOS F. ORTIZ, MAYLING C. BLANCO, RUSSELL T. WONG, MATTHEW J. THOMAS, AND ALEXANDRA CLARK

CARLOS F. ORTIZ
PARTNER

MAYLING C. BLANCO
PARTNER

RUSSELL T. WONG
PARTNER

MATTHEW J. THOMAS
PARTNER

ALEXANDRA CLARK
ASSOCIATE

On November 1, 2018, then-U.S. Attorney General Jeff Sessions announced the creation of the China Initiative (the "Initiative") to support the U.S. Department of Justice's ("DOJ") "priority of countering Chinese national security threats…" The Initiative consists of a task force aimed at identifying suspected Chinese trade theft cases for investigation and enforcement. Sessions stated, "[t]his theft is not just wrong; it poses a grave threat to our national security. And it is unlawful." In short, "Enough is enough. We're not going to take it anymore." This Initiative comes after several high-profile investigations of Chinese enterprises and citizens concerning espionage and theft of key U.S. technologies and intellectual property. Of note are the Initiative's focus on one specific country—China—and the strong language used by Sessions in his comments.

> If a U.S. company reasonably believes that it lost a government contract in a foreign country to a Chinese company due to an alleged FCPA violation, prosecutors are encouraging companies to come forward with that information.

The Initiative

The Initiative will be led by Assistant Attorney General John Demers and is composed of senior DOJ and Federal Bureau of Investigation personnel, including five U.S. attorneys. Prosecutions will utilize several federal statutes to meet their stated objectives. The task force is charged with addressing 10 goals, including: 1) identifying priority trade secret theft cases; 2) implementing the Foreign Investment Risk Review Modernization Act ("FIRMA") for the DOJ; and 3) identifying violations of the Foreign Corrupt Practices Act ("FCPA") by Chinese companies competing with American businesses.

Setting an Example

During the rollout of the Initiative, Sessions announced that the DOJ had indicted a Chinese company for allegedly engaging in economics espionage. The indictment, filed September 27, 2018, but unsealed November 1, accused Fujian Jinhua Integrated Circuit Co. Ltd. (a Chinese state-owned company), United Microelectronics Corp. ("UMC") (a Taiwanese semiconductor company listed on the NYSE), and three Taiwanese nationals, of stealing trade secrets from Micron Technology, a U.S. semiconductor manufacturer. The Jinhua/UMC case is, in all likelihood, to be among the first of these types of cases that focus on targeting Chinese companies that compete with American businesses. Given the stated policy of the DOJ, there are likely more prosecutions in store for Chinese companies for such violations.

The basis for the case against Jinhua/UMC is the Economic Espionage Act ("EEA"), as amended by the Defend Trade Secrets Act ("DTSA"). These laws give the U.S. government broad powers in prosecuting theft of trade secrets claims against Chinese companies. The EEA and the DTSA have broad jurisdictional reach by applying to conduct outside the United States: a) if the offender is a citizen or permanent resident alien of the United States or an organization under the laws of the United States; or b) if some act in furtherance of the offense takes place in the United States.

Company executives also face significant risks as a result of the Initiative. For example, shortly after the Initiative was announced, on December 1, 2018, Meng Wanzhou, the CFO of Chinese telecommunications company Huawei Technologies Co., was arrested for extradition to the United States while switching planes in Canada. Huawei confirmed that Ms.

Wanzhou faces prosecution in the Eastern District of New York, whose U.S. Attorney is a working group member for the Initiative. The charges against Ms. Wanzhou were "unspecified" at the time of her arrest.

The FCPA Focus

The Initiative's specific goal of identifying FCPA cases involving Chinese companies that compete with American businesses is particularly noteworthy, given the relative lack of FCPA enforcement actions against Chinese companies to date. While China has been the source of a wealth of FCPA enforcement in recent years, Chinese-based companies are rarely the subject of prosecutions. Indeed, over 30 percent of all corporate FCPA cases since 2011 involved improper conduct in China, but none of these cases involved China-based companies. Rather, the target of those enforcement actions were multinational companies with Chinese business operations.

It will be interesting to see how the Initiative achieves its FCPA goal. The FCPA's jurisdictional reach applies only to Chinese companies if they qualify as "issuers," or if any part of the related transaction touches U.S. soil. This can be as simple as a transfer of funds through a U.S.-correspondent bank account or an e-mail passing through a U.S.-based server. Thus, if a Chinese company competing with a U.S. company for business in South America or Africa meets one of these jurisdictional hooks, it could soon find itself in the DOJ's crosshairs under the new Initiative if it violates the FCPA. As cases like the recent FIFA prosecution demonstrate, the DOJ is not averse to prosecuting foreign companies and individuals, and certainly possesses the experience and the tools to do so, as well as the creativity to find jurisdictional hooks. Here, the Initiative expressly directs prosecutors to identify violations of the FCPA—something they have become very good at doing over the past decade.

The Initiative also provides a forum for U.S. companies to raise concerns to federal prosecutors of potential FCPA violations. If a U.S. company reasonably believes that it lost a government contract in a foreign country to a Chinese company due to an alleged FCPA violation, prosecutors are encouraging companies to come forward with that information. This could result in a DOJ investigation, including a request for information directed to the foreign country where the alleged violation took place. Such a request could, in turn, lead to an investigation in that other country, as well.

Preparing for the Initiative

As a result of the Initiative, Chinese companies, particularly those in the technology or manufacturing sector, should evaluate their past and present international trade practices to ensure ongoing compliance to avoid being targeted by the DOJ. Moreover, Chinese companies that do business with foreign governments would be well advised to have strong anti-corruption policies and processes in place to ensure that their activities do not run afoul of the FCPA. A well-designed anti-bribery compliance program can provide tangible benefits for a company, including the avoidance of enforcement actions, a reduction in the fines or penalties sought by regulators, and the establishment of credibility within an industry. Chinese companies also would be well served to review their policies and procedures for protecting proprietary technology legally obtained from other companies, as well as procedures ensuring that technology does not enter the company inappropriately. Implementation of appropriate procedures may be useful in defending against an EEA claim. The DOJ's message cannot be any clearer—for Chinese companies, the time to act is now. ◘

Blank Rome Teams Join Forces to Provide Expanded Government Relations & Political Law Services to Clients

Former Federal Election Commission Chair Scott Thomas and team expand capabilities of Blank Rome Government Relations in the areas of campaign finance, election, lobbying, ethics, and tax law.

Blank Rome is pleased to announce the formal alignment of **Blank Rome Government Relations LLC** ("BRGR") with the Firm's **Policy & Political Law** ("P&PL") group to further strengthen our government relations practice and the interrelated services we offer our clients.

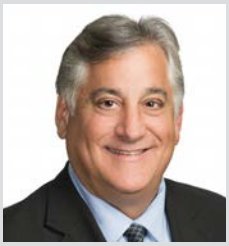
BRGR brings together the Firm's top legal, lobbying, and strategic communications professionals into a powerful team that can manage virtually every aspect of any governmental issue facing a client. Led by **C.J. Zane**, our BRGR team will continue to focus its efforts on developing federal laws, regulations, and policies that support our clients' goals. With the addition of the P&PL team, led by **Scott E. Thomas**, former chairman of the Federal Election Commission, BRGR will now have expanded capabilities to help its clients navigate the complex maze of campaign finance, election, lobbying, ethics, and tax laws at the federal, state, and local levels.

In today's environment, characterized by changes in domestic government policy, international trade, increased national defense outlays and challenges, and potential leadership changes in Congress, important developments can occur virtually overnight. Our multifaceted government relations service, provided by BRGR's group of bipartisan professionals, allows us to work with "both sides of the aisle" in Congress, as well as with the current and any future administration, to help our clients successfully navigate the ever-changing landscape in Washington, D.C. From working to overcome onerous trade tariffs, to procuring important tax provisions, assisting with federal procurement issues, and much more, we strive to bring consolidated yet comprehensive government relations experience to our clients. Thus, for greater efficiency and enhanced capability, we have aligned and combined BRGR with our P&PL practice.

We have consolidated, yet expanded, our government relations services because any organization or individual affected by federal government policy must understand that while the federal government appears stymied and stuck in partisan bickering and political maneuvering, important legislation continues to move forward. In the past year, Congress has passed more major legislation on time, including national defense policy bills, tax reform legislation, Federal Aviation Administration reauthorization, and more appropriation bills, than at any time over the past 15 years. Things are indeed happening in Washington, D.C., and our combined capabilities will enhance our performance on behalf of our clients. ◘

For more information on BRGR's new policy and political law capabilities, please visit blankromegr.com or contact C.J. Zane or Scott E. Thomas.

C. J. Zane
Managing Principal,
Blank Rome Government Relations LLC
202.772.5975
zane-cj@blankrome.com



Scott E. Thomas
Senior Principal,
Blank Rome Government Relations LLC
Partner, Blank Rome LLP
202.420.2601
sthomas@blankrome.com

You Win Some, You Lose Some: Recent FCA Litigation Developments

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

NICHOLAS C. HARBIST
PARTNER

LAUREN E. O'DONNELL
ASSOCIATE

This article explores two recent developments in False Claims Act ("FCA") litigation—one that should provide reassurance to potential FCA defendants, and one that may trouble them.

Government Dismissals of FCA Cases

In January 2018, Michael Granston, the Department of Justice ("DOJ") civil fraud chief, issued a memorandum on FCA case dismissals (the "Granston Memo"). As previously discussed in our April 2018 article, False Hope for False Claims Act Defendants? Government Dismissals of *Qui Tam* Cases May Increase, the Granston Memo provided guidance to DOJ lawyers about when they should dismiss FCA cases. Historically, such dismissals have been rare. In fact, a 2013 study by Stanford Law School professor David Freeman Engstrom concluded that since 1986, the government had unilaterally dismissed only 30 of 4,000 unsealed whistleblower FCA complaints.

> Healthcare providers may be troubled by the seemingly new trend of data mining relators—relators who have no actual connection to the providers, but whose analyses of providers' claims data form the basis of a FCA suit.

Since the Granston Memo was issued, the government has already advocated for the dismissal of three FCA cases. The first case is pending before the U.S. Supreme Court, *Gilead Sciences Inc. v. U.S. ex rel. Jeffrey Campie et al.,* 17-936. At the end of November, the DOJ filed an amicus brief indicating that it will move to dismiss the case if it is sent back to the district court, as "continued prosecution of the suit is not in the public interest." The DOJ explained that it is concerned about both parties making "burdensome" requests for Food and Drug Administration ("FDA") documents and testimony if the case proceeds. According to the DOJ, such requests would distract from the FDA's public health responsibilities. As the DOJ wrote, "The government has concluded that allowing this suit to proceed to discovery (and potentially a trial) would impinge on agency decisionmaking and discretion and would disserve the interests of the United States."

The second action, *Maldonado v. Ball Homes LLC,* 17-CV-00379 (E.D. Ky.), involved Federal Housing Administration insurance. The DOJ called the whistleblower's allegations weak, and a Kentucky federal judge agreed to dismiss the case accordingly. The third case was *U.S. ex rel. Manchester v. Purdue Pharma LP et al,* 16-CV-10947 (D. Mass.), a prescription opioid case filed against OxyContin maker Purdue Pharma LP and three drug distributors. The government moved to dismiss the Massachusetts suit because it found that the whistleblower's allegations were not new and should be dismissed under the FCA's public disclosure bar. The motion to dismiss is pending.

Given this recent government advocacy for dismissal, it appears that government attorneys are heeding the guidance in the Granston Memo. Thus, defense counsel should continually refer to this DOJ guidance to frame motion practice, government presentations, and discovery in an effort to persuade the DOJ to consider dismissal.

Data Mining Relators

In August, federal courts unsealed two False Claims Act complaints filed by a company that analyzed public data to find potential fraud allegations. Unlike a typical whistleblower action, the company that filed these cases did not have direct knowledge of wrongdoing. After the company used algorithms and statistical processes to analyze Medicare claims data, it alleged that the defendants used certain procedure codes to improperly inflate reimbursement. The company then filed federal whistleblower lawsuits, claiming fraudulent upcoding

of more than $61 million in one case, *U.S. ex rel. Integra Med Analytics LLC v. Baylor Scott & White Health et al.,* 17-CV-0886 (W.D. Tex.), and $188 million in the other, *U.S. ex rel. Integra Med Analytics LLC v. Providence Health Services et al.,* 17-CV-01694 (C.D. Cal.).

Healthcare providers may be troubled by the seemingly new trend of data mining relators—relators who have no actual connection to the providers, but whose analyses of providers' claims data form the basis of a FCA suit. Providers should push courts to conclude that Centers for Medicare & Medicaid Services data files are information published online by the government and thus insufficient to provide a basis for a FCA suit under the public disclosure bar. Providers also should question whether FCA complaints based upon data mining, rather than knowledge of wrongdoing, satisfy the requirements under Federal Rule 9(b) that allegations of fraud be plead with particularity.

Blank Rome Achieves Mansfield Certification for Participation in Diversity Lab's Mansfield Rule Program

Mansfield Rule™ Certified 2018 Powered by DIVERSITYLAB

Blank Rome LLP is proud to announce that the Firm has achieved Mansfield Certification after successfully completing Diversity Lab's inaugural one-year Mansfield Rule pilot program. The certification recognizes 41 "trailblazing law firms" participating in the Mansfield Rule that have affirmatively considered at least 30 percent women and attorneys of color for leadership and governance roles, equity partner promotions, and senior lateral positions, to boost the representation of diverse lawyers in law firm leadership.

According to Diversity Lab's press release announcing the firms that have achieved Mansfield Certification, one of the favorable outcomes of the inaugural Mansfield Rule is the significant surge in firms that now track and measure their candidate pipelines. Additionally, there is a reported incremental increase in diverse candidates considered for leadership roles, equity partner promotions, and lateral hiring by firms that tracked their pipelines prior to adopting the Mansfield Rule. Lisa Kirby, Director of Research & Knowledge Sharing at Diversity Lab, further stated in the press release that tracking candidate pipelines for "every single path that leads to leadership" as well as increasing the diversity of these pipelines is a positive step towards diversifying law firms' next generation of leaders.

As a reward for achieving Mansfield Certification, Blank Rome and other participating certified firms will be able to send their newly promoted diverse and women partners to one of three upcoming Diversity Lab Client Forum events in New York, San Francisco, and Minneapolis/St. Paul. At the client forums, the diverse and women partners will learn from and have an opportunity to connect one-on-one or in small groups with legal department lawyers from more than 60 legal departments from leading companies across the country.

To read Blank Rome's press release announcing this achievement, please click here.

Insurers Seize on *Kokesh* Ruling to Disclaim Coverage for SEC Disgorgement

BY JUSTIN F. LAVELLA AND ALEXANDER H. BERMAN

JUSTIN F. LAVELLA
PARTNER

ALEXANDER H. BERMAN
ASSOCIATE

In April 2017, white collar and securities attorneys, as well as potential defendants, cheered the Supreme Court's unanimous opinion in *Kokesh v. SEC,* which held that civil disgorgement, when imposed as part of a Securities and Exchange Commission ("SEC") enforcement proceeding, is a "penalty" and therefore subject to a five-year statute of limitations.[1] At the time, *Kokesh* was hailed as limiting the size of future disgorgement awards, in some cases dramatically. However, the court's categorization of SEC disgorgement as a "penalty" may have much wider ripple effects that could jeopardize billions of dollars in potential future insurance recoveries. This ripple effect first manifested itself in *J.P. Morgan Sec., Inc. v. Vigilant Ins. Co.,* where New York's intermediate appellate court recently held that an SEC disgorgement settlement was no longer a covered "loss" under the defendant's insurance policy, because *Kokesh* recategorized such disgorgements as non-covered "penalties."[2]

While *Kokesh,* on the one hand, may save SEC enforcement targets hundreds of millions of dollars, it also may greatly complicate their insurance claims for the amounts they do pay either in settlement or judgment. In response, potential SEC enforcement targets should:

- be aware of the *Kokesh* decision and its potential effects on existing insurance policies;
- consider avoiding civil disgorgements in future settlement negotiations with the SEC; and
- contact their insurance brokers and insurance counsel to negotiate modifications to future renewals of their directors' and officers' liability ("D&O") and errors and omissions ("E&O") insurance policies.

The *Kokesh* Decision and Its Effects

In *Kokesh,* the defendant had been ordered to pay a $2.4 million civil monetary penalty, $34.9 million in disgorgement, and $18.1 million in prejudgment interest. Though the five-year statute of limitations of 28 U.S.C. § 2462 applied to the civil penalty, the district court held that the limitation period did not apply to the disgorgement remedy, because disgorgement is not a "penalty."[3] The Court of Appeals for the Tenth Circuit affirmed, but the Supreme Court unanimously reversed.[4]

The court found that an SEC disgorgement is a "penalty" on three grounds: 1) disgorgement is often imposed in recognition of harms done to the general public, as opposed to harms committed against specific individuals;[5] 2) disgorgement is used primarily for its deterrent purpose, which renders it punitive as opposed to remedial;[6] and 3) because a court has discretion over where disgorgement funds are sent, such amounts are more of a penalty against the wrongdoer, rather than a tool for compensating injured parties.[7]

> In tying payments closer to compensation for the allegedly wronged parties, companies can distinguish such payments from the SEC disgorgement scheme that was considered punitive and thus a "penalty" in *Kokesh.* That distinction could well be the difference between obtaining hundreds of millions of dollars in insurance coverage or not.

In September 2018, the latest opinion was issued in the long-running *Vigilant* coverage action, which involves Bear Stearns' attempts to secure insurance for liabilities arising from certain institutional investors being permitted to "market time" select investment funds. Decided before *Kokesh,* the *Vigilant* trial court held in April 2017 that Bear Stearns' $140 million disgorgement settlement was a covered "loss" under its D&O insurance policies, because the amount was calculated based upon the money gained by third parties, which Bear Stearns agreed to reimburse to its other investors, and not on

the amount of disgorgement of Bear Stearns's own ill-gotten gains.[8] However, in September 2018, the New York Appellate Division held that *Kokesh* had changed the law, and that disgorgement payments were a "penalty," and thus not covered by Bear Stearns's insurance policies, which exclude "fines or penalties imposed by law" from the definition of "loss."[9]

Given that the vast majority of analogous insurance policies with similar "loss" definitions exclude "penalties," the *Kokesh* and *Vigilant* decisions may further complicate the already hotly contested question of whether "disgorgement" is a covered loss under D&O and E&O insurance policies.[10] In fact, *Kokesh* may result in opening a completely new front in this long-running battle between insurers and their policyholders.

The law could, of course, change again: *Vigilant* is highly likely to be appealed again to the New York Court of Appeals. But until other courts issue more policyholder-friendly precedent, or the SEC refines how it applies disgorgement to remove the punitive aspects relied upon by the Supreme Court, companies and their counsel should take steps in the short term to limit their now arguably uninsured potential liabilities.

Consider Alternative Remedies in Negotiations with SEC

As a result of *Kokesh,* companies should look to alternative bases of settling with the SEC, besides disgorgement. In tying payments closer to compensation for the allegedly wronged parties, companies can distinguish such payments from the SEC disgorgement scheme that was considered punitive and thus a "penalty" in *Kokesh*. That distinction could well be the difference between obtaining hundreds of millions of dollars in insurance coverage or not. Of course, companies must weigh the insurance coverage implications of *Kokesh* and *Vigilant* against the beneficial five-year statute of limitations established by *Kokesh.*

Alternatively, Consider Requesting Modified Language in Future Renewal Policies

Companies also could attempt to negotiate with their D&O and E&O insurance carriers to amend future renewal policies to create a limited carve-out to the general exclusion for "penalties." There is, in fact, precedent for such a modification, as many existing D&O and E&O policies already explicitly carve out certain penalties that can be imposed under Sarbanes-Oxley. Nonetheless, insurers may be cautious in modifying their policies in the coming months and years as they evaluate the potentially combined impact of *Kokesh* and *Vigilant*. □

1. *Kokesh v. SEC,* 137 S. Ct. 1635, 1639, 198 L. Ed. 2d 86 (2017).
2. *J.P. Morgan Sec., Inc. v. Vigilant Ins. Co.,* No. 600979/09, 2018 WL 4494692, at *3 (N.Y. App. Div. Sept. 20, 2018).
3. *Kokesh,* 137 S. Ct. at 1641.
4. *Id.* at 1639, 1641.
5. *Id.* at 1643.
6. *Id.* at 1643-44.
7. *Id.* at 1644.
8. *Vigilant,* 2018 WL 4494692, at *2.
9. *Id.* at *3.
10. *Compare Level 3 Communications Inc. v. Federal Ins. Co.,* 272 F.3d 908 (7th Cir. 2001) *with Mills, Ltd Partnership v. Liberty Mut. Inc. Co.,* No. C.A. 09C-11-174 FSS, 2010 WL 8250837 (Del. Super. Ct. Nov. 5, 2010).

Recent & Upcoming Events

Mayling Blanco:

- Blockchain and Cybercurrency at the New York State Bar Association's program on "Cutting Edge Technologies and Your Practice: What Lawyers Need to Know Today to Prepare for the Digital Future" (December 6, 2018).
- Hot Topics in Compliance 2018 at the Hispanic Bar Association of New Jersey's Ninth Annual Corporate Counsel Conference (November 28, 2018).
- "Tax and Business Considerations of Transactions Using Blockchain and Cryptocurrency" at Blank Rome's Tax Update in New York (November 7, 2018) and Philadelphia (November 1, 2018).

Mark Lee:

- White Collar Defense Strategies, Lorman Webinar and CLE (January 30, 2019).
- Cryptocurrencies and ICOs: Navigating the Regulatory Landscape and Responding to Government Investigations at the Pennsylvania Association of Criminal Defense Lawyers' 2018 White Collar Practice Seminar (November 15, 2018).

Carlos Ortiz:

- New Developments in Criminal Tax Enforcement at the American Bar Association's 33rd Annual National Institute on White Collar Crime (March 6, 2019).
- "Cracking Down on Cryptocurrencies & Criminalizing Unfair Competition" at the American Chamber of Commerce in Shanghai's co-hosted lunch event on U.S. Compliance and Recent Trends of Legal and Board Governance Risks (November 27, 2018).
- "Tax and Business Considerations of Transactions Using Blockchain and Cryptocurrency" at Blank Rome's Tax Update in New York (November 7, 2018) and Philadelphia (November 1, 2018).

Joseph Poluka:

- "Managing Company Exposure and the Critical Role of In-House Counsel: Disasters, Security Breaches, #MeToo Minefields, and More" at Blank Rome's Annual Emerging Litigation & Employment Issues for In-House Counsel (November 16, 2018).
- The Intersection of Forfeiture and Bankruptcy Law at the Eastern District of Pennsylvania Bankruptcy Conference Fall Forum (November 13, 2018).
- "Cyber-Jeopardy: The Evolving Cyber Crisis and How to Protect Your Energy Enterprise" at Blank Rome's Fourth Annual Pittsburgh Energy Industry Update (November 1, 2018).
- Cryptocurrency: Trash or Treasure? hosted by Blank Rome for the Pennsylvania Association of Criminal Defense Lawyers (October 10, 2018).
- "What Are Common Mistakes in Internal Investigations, Including Audit Committee Investigations?" at the 2018 Association of Audit Committee Members Annual Meeting (October 5, 2018).

Recent & Upcoming Events

Jed Silversmith:

- "Tax Reporting of Cryptocurrency Transactions" at the Pennsylvania Society of Tax and Accounting Professionals' Tax Potpourri CPE (February 1, 2019).
- International Money Laundering and Tax Enforcement Update at the Philadelphia Area Chapter of the Certified Fraud Examiners' 26th Annual All-Day Fraud Training Conference and Luncheon (December 3, 2018).
- International Tax Compliance: What Every Tax Practitioner Must Know at the Pennsylvania Institute of Certified Public Accountants' Greater Philadelphia Chapter Annual Tax Conference (November 28, 2018).
- FBAR and FATCA 2018: Preparing for the Next Round of Offshore Tax Compliance, Clear Law Institute Webinar (November 20, 2018).
- "Tax and Business Considerations of Transactions Using Blockchain and Cryptocurrency" at Blank Rome's Tax Update in Philadelphia (November 1, 2018).
- Cryptocurrency, Taxation of Cryptocurrency, and Other New IRS Topics course for the Pennsylvania Society of Tax and Accounting Professionals (October 17, 2018).

Ariel Glasner:

- White Collar Defense Strategies, Lorman Webinar and CLE (January 30, 2019).
- False Claims Act Roundtable, ABA Criminal Justice Section: White Collar Crime Committee (TBA, March 2019).
- DC Bar Criminal Law and Individual Rights Community Annual Panel on Representing Individuals in White Collar Cases (TBA, February 2019).

The Maritime Industry: The DOJ FCPA Unit's Next Port of Call

BY CARLOS F. ORTIZ, MAYLING C. BLANCO, AND ALEXANDRA CLARK

CARLOS F. ORTIZ
PARTNER

MAYLING C. BLANCO
PARTNER

ALEXANDRA CLARK
ASSOCIATE

The maritime industry, by its nature, involves the movement of goods and vessels across international borders, and requires routine interaction with government officials. Historically, many in the industry viewed bribery of these officials in many parts of the world as a "cost of doing business." Increased cooperation between the U.S. government and foreign governments has led to intensive efforts to investigate and fight corruption across the globe. Recent actions by the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC") in the maritime-related oil and gas industry make it clear that Foreign Corrupt Practices Act ("FCPA") enforcement may soon take a closer look at the maritime industry.

As a preliminary matter, for over a decade, the oil and gas industry has been the focus of investigation and has seen more FCPA enforcement actions than any other industry.[1] In the last two years, however, some of these actions have involved maritime companies in the oil and gas trade. For companies with an international presence, which is the case for many maritime companies, a single bribe could expose the company and its employees to violations of anti-bribery laws in multiple jurisdictions. The maritime industry should understand the risks of violating the FCPA, how to mitigate them, and the consequences for violations.

What Does the FCPA Prohibit and to Whom Does It Apply?

The anti-bribery provisions of the FCPA prohibit providing or promising to provide anything of value to a foreign official to gain an improper business advantage.

The FCPA originally applied only to U.S. companies and individuals and issuers of U.S. securities. In 1998, the FCPA's jurisdiction expanded to apply to any individual or company, regardless of nationality, engaging in prohibited acts in the United States. For foreign companies, the FCPA's expanded jurisdiction has a significant impact. Foreign companies can be liable for FCPA violations if a prohibited act occurs in the United States. Prohibited acts can be as simple as the transfer of money through U.S. banks or the routing of an e-mail through a U.S.-based server. Moreover, the FCPA imposes derivative liability on companies for the actions of its employees and for any third party acting on the company's behalf, as well as individuals involved in or authorizing such conduct.

What Are the Consequences of a Violation of the FCPA?

Violators of the FCPA face serious consequences. Companies found guilty of violating the FCPA often pay tens of millions of dollars (or more) in criminal fines and/or civil penalties,

and are forced to disgorge all profits obtained in connection with the bribery. In addition, a company in violation of the FCPA must bear the cost of investigation, the risk of potential imposition of a compliance monitor, suspension and/or debarment from government contracts, a limit on its ability to obtain an export license, and reputational damage. And it is not only

the company facing liability—executives and employees at all levels may be prosecuted for FCPA violations. In recent years, the government has enforced its stated policy to hold individuals accountable for FCPA violations. Individuals found guilty of violating the FCPA face criminal fines, civil penalties, and imprisonment.

What Are the Risk Areas in the Maritime Industry?

The high-risk areas for FCPA violations in the maritime industry are:

- tendering process & requests for proposals with governments or state-owned businesses;
- use of third parties (*e.g.,* local agents, consultants, customs brokers, freight forwarders);
- excessive gifts, entertainment, and travel provided to foreign officials that are not tied to a proper business purpose;
- mergers, acquisitions, and joint ventures;[2]
- tax and customs avoidance; and
- regulatory avoidance (*e.g.,* permits, environmental issues, audits).

What Can a Maritime Company Do to Mitigate Its Risks?

Because violating the FCPA requires an offer to give or giving something of value to a foreign official, companies should evaluate their FCPA liability by assessing their interactions with foreign officials. The FCPA's definition of "foreign official" is broad and includes employees of government agencies, legislators, employees of state-controlled entities, and consultants working on behalf of a government. Unique to the maritime industry, companies may deal with foreign officials who are employees of state-owned commodities, energy or petroleum companies; government-controlled ports; and consultants working with or on behalf of foreign governments.

Companies must evaluate the risk of using third parties to conduct business outside of the United States. An intermediary, such as a local agent, can create individual and corporate FCPA liability by making payments to a foreign official on behalf of the company. Past FCPA prosecutions have included payments of commissions to third parties who used those funds, in part, to bribe foreign officials in exchange for contracts with state-owned companies.

For companies concerned about FCPA exposure, the first question is whether the company is operating and/or transacting any type of business abroad with a foreign government, government-owned entities, or involving foreign officials—either directly, through joint ventures, or through agents. Implementation of an FCPA compliance program, educating employees about anti-corruption laws applicable to the company's operations, and thoroughly vetting third-party agents are important steps that a company must take to minimize risk.

> For companies with an international presence, which is the case for many maritime companies, a single bribe could expose the company and its employees to violations of anti-bribery laws in multiple jurisdictions.

What Can a Company Do If There Already Has Been a Violation?

The FCPA does not mandate self-disclosure of wrongdoing. However, remediation of any known violation is necessary to minimize exposure. The DOJ offers credit for self-disclosure, and a company that uncovers and remediates a violation should decide if self-disclosure is a good option. Companies must have an effective anti-corruption program, and not merely a manual on the shelf. However, that program can be tailored to fit the size and operations of the company, taking into consideration its risks and resources.

Why Is Now so Critical?

As a result of the investigations involving government officials in the oil and gas industries, most recently in Brazil and Venezuela, the DOJ has prosecuted numerous companies and individuals. These investigations and prosecutions, and the resulting cooperation agreements, provide prosecutors with a wealth of information and industry insight that will lead to additional investigations and prosecutions. The time to act and become compliant is now, before the DOJ or SEC comes calling. ◘

1. *See, e.g., Heat Map by Industry,* Stanford Law School Foreign Corrupt Practices Clearinghouse, fcpa.stanford.edu/industry.html (Last accessed December 7, 2018).
2. Blank Rome has reported on the DOJ's policy with respect to voluntary disclosures in the context of mergers and acquisitions. *See* DOJ Urges U.S. Companies Acquiring or Merging with Foreign Companies to Self-Disclose FCPA Misconduct Identified during Due Diligence.

The FinTech Revolution: Fraud Prevention in the FinTech Space

BY ARIEL S. GLASNER AND BRIDGET MAYER BRIGGS

ARIEL S. GLASNER
ASSOCIATE

BRIDGET MAYER BRIGGS
ASSOCIATE

This is the sixth installment in a series of articles. For more background on this topic, please read our previous articles:

1. An Introduction to Financial Technology
2. The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications
3. The FinTech Revolution: The Impact of Blockchain Technology on Regulatory Enforcement
4. The FinTech Revolution: Complying with Anti-Money Laundering Laws to Avoid Regulatory Enforcement Actions
5. The FinTech Revolution: How Data Breaches Can Result in Regulatory Enforcement Actions

As the FinTech industry rises in popularity, the number of digital transactions—also known as e-commerce—is sky-rocketing, creating ever-greater opportunities for fraud.[1] These vulnerabilities are compounded by an expansion in the range and assortment of digital transactions. As a result, there is a critical need for companies in the FinTech industry to ensure that they have sound and comprehensive fraud prevention strategies, policies, and programs in place.

The Problem

People seeking to engage in fraudulent schemes or artifices are attracted to an industry that is on the cutting edge of technological development where they see opportunities to exploit weaknesses in data protection. Identity theft (the misappropriation of someone else's identity by targeting his or her personal information), and "phishing" (using fraudulent communications such as websites, text messages, and e-mails to induce people to part with their personal information), are two of the more common types of fraudulent devices that are employed, in addition to other sophisticated fraudulent schemes.[2]

Because of constant changes in technology and the increase in the frequency and volume of digital transactions, companies are not always fully equipped to prevent fraud. This is true even for enterprises that have diligently implemented traditional fraud prevention policies and programs, such as robust anti-money laundering ("AML") compliance programs. Why so? Because many current fraud prevention techniques are rooted in the idea of manual detection (*i.e.,* before a company can implement preventative measures, a form of fraud must be detected by an individual).[3] As discussed below, companies should consider adopting a more comprehensive approach to combatting fraud by combining traditional, manual fraud

prevention policies and programs with more cutting-edge fraud prevention techniques that utilize artificial intelligence ("AI").

The Solution

One way the FinTech industry has been supplementing traditional fraud prevention policies and programs is through the continued development of machine learning fraud prevention approaches using AI. With machine learning, a computer is able to recognize schemes that are likely to be fraudulent by analyzing prior data and then making decisions with respect to ongoing transactions, with or without continuous human interaction. "Supervised" machine learning, which requires human interaction, involves the selection of a random set of transactions that are then manually sorted into "fraudulent" or "non-fraudulent" buckets. The results of this sorting are then used to create an algorithm that enables computers to recognize and flag other fraudulent transactions as they occur.[4] "Unsupervised" machine learning, by contrast, is a type of machine learning that analyzes a randomized dataset for patterns or potential indicators of fraud without manual input by an individual. The results of the analysis are then extrapolated to larger sets of data.[5]

One way the FinTech industry has been supplementing traditional fraud prevention policies and programs is through the continued development of machine learning fraud prevention approaches using AI.

Several FinTech companies are focused specifically on helping other companies in the industry to mitigate or prevent exposure to fraud. For example, some companies use machine learning and data analysis to prevent fraud in payment processing, opening new customer accounts, and validating customers, among other things. Other services allow businesses from different industries to share positive and negative information about devices so that merchants can determine whether a device has been previously linked to fraudulent activity. Similarly, some services use data from numerous sources to collect and share information on billions of people, allowing e-commerce merchants to verify new customers, and thus reducing the risk of fraudulent purchases and subsequent chargebacks.

Conclusion

Given the evolution of fraud and fraud prevention tools, financial institutions and other businesses susceptible to e-commerce fraud should carefully review and evaluate their fraud prevention policies and programs to ensure that their businesses and customers are adequately protected. In addition, they should consider whether they should supplement their existing defenses with the incorporation of machine learning solutions. ◘ – ©2018 BLANK ROME LLP

1. *See* Experian Report, *E-commerce Attack Rates,* available at experian.com/decision-analytics/identity-and-fraud/ecommerce-attack-rates.html.
2. *See* fintech.finance/01-news/types-of-fraud-in-e-commerce.
3. *See* innoarchitech.com/machine-learning-fintech-secret-weapon-against-fraud.
4. *Id.*
5. *Id.*