January 23, 2019

White Collar and Regulatory Enforcement: What Mattered in 2018 and What to Expect in 2019

Introduction

Now that we are two years into the new administration, we have a far clearer picture than we had last year of white collar and regulatory enforcement priorities, policies and trends. This is due, in part, to the fact that more leadership positions at the SEC, DOJ and the United States Attorneys' Offices around the country have been filled, these new leaders have given speeches and issued policy pronouncements that have clarified and, in some cases, altered the government's approach and priorities, and accumulated data on dispositions, declinations, and fine levels have given us a better sense of trends and patterns.

We've also been gratified that DOJ in particular has pursued several policy changes that we had suggested should be considered by the new administration in our year-end memo two years ago. White Collar and Regulatory Enforcement: What to Expect in 2017. Notable examples include:

- DOJ announced on October 18 a new policy on the selection of monitors, clarifying the appointment process and acknowledging how burdensome the imposition of a monitor can be;
- DOJ broadened the scope of the FCPA Enforcement Policy to cover all white collar categories and provided clarity about the actual benefits, including penalty discounts, that cooperating companies can expect to receive.

The balance of this memo provides updates on key developments during 2018 and a forecast of what to expect as 2019 unfolds, in the following areas:

- DOJ developments, changes in policy and enforcement trends;
- The rise of state Attorneys General as a major regulatory force and enforcement threat;
- The international arena and the increasing sophistication of cross-border cooperation; and

If your address changes or if you do not wish to continue receiving these memos, please send an e-mail to Publications@wlrk.com or call 212-403-1443.

- Developments in the conduct of internal investigations, especially in regard to how the Fifth Amendment privilege against self-incrimination can potentially be implicated during internal reviews.

The upshot is that companies will continue to face a wide array of white collar and regulatory enforcement risks in the coming year, but there is now greater clarity about the benefits that can accrue to well-managed companies by properly responding to issues, fully cooperating with inquiries, and instituting comprehensive remediation and reform measures. All of this reinforces the need for well-designed and expertly implemented compliance systems and policies so that companies will be able to deter wrongdoing, detect misconduct, and consider whether it would be appropriate to self-report.

Cybersecurity Developments

Data privacy and protection risks continued to draw public and regulatory attention throughout 2018, reminding all companies that the cybersecurity landscape remains hazardous. Data breaches across a range of industries demonstrated the continuing challenges of securing company data systems, while increased public attention to corporate use of personal data highlighted the importance of careful data management and attention to data privacy. Meanwhile, regulators worldwide were granted broad new powers in this area and were increasingly active, with the sweeping provisions of the EU's General Data Protection Regulation (GDPR) serving as the most prominent example. The result: in 2019, companies must navigate across an increasingly complex terrain marked by varying data protection and privacy laws, regulations, best practices, and industry and customer expectations, with governments and the media paying increasingly close attention to every step.

The GDPR took effect on May 25, 2018, simultaneously broadening and tightening regulations governing the handling of personal data of individuals located in the EU. With its strict requirements, extraterritorial reach, and severe penalties for noncompliance — up to 4% of the offending company's worldwide revenue — the GDPR has caused many corporations to refashion their approaches to data privacy and protection, not just in the EU but across the globe. In July 2018, data protection authorities in the United Kingdom brought the first GDPR-related enforcement action against AggregateIQ, a Canada-based analytics company that processed personal data to develop targeted pro-Brexit political ads. And on January 21, 2019, French data protection authorities leveled a €50 million penalty against Google for violating transparency obligations and consent

requirements imposed by the GDPR in connection with the company's processing of user personal data to target personalized advertising. Developments in these enforcement actions will be closely watched as first tests of the GDPR regime.

In the United States, the SEC focused its attention on market disclosure, breach notification, and internal controls. In February, the SEC issued new guidance to clarify its expectations as to market disclosures by public companies. While much of the 2018 disclosure guidance focused on "reinforcing and expanding upon" the SEC's 2011 guidance, the 2018 guidance did break some new ground — particularly in the areas of board oversight, disclosure controls and procedures, insider trading, and selective disclosures. With respect to board oversight, the 2018 guidance advises that public companies should disclose the role of the board in cyber risk management, at least where cyber risks are material to a company's business. While most boards are likely already engaged in cyber risk oversight, the SEC's call for more public disclosure may prompt consideration of whether to deepen or sharpen that engagement.

The SEC also adopted a more aggressive posture, engaging in high-profile enforcement actions following data breaches at Yahoo! and Equifax that highlight the SEC's priorities. In April, the SEC announced that Altaba, the entity formerly known as Yahoo!, had agreed to pay a $35 million penalty to settle charges that it misled investors by waiting two years to disclose a data breach in which hackers stole the personal information of more than 500 million Yahoo! users. While the Yahoo! case should not be read as requiring public disclosure of every data breach, it does highlight the need for effective corporate controls to ensure that internal reports of cyber incidents are properly and timely assessed for potential disclosure. In March and June, DOJ and the SEC filed criminal and civil charges against two former Equifax employees — a chief information officer and a software engineer — for insider trading in advance of the company's 2017 announcement of a breach that exposed the personal data of almost 150 million customers. In light of the government's enhanced focus in this area, companies would be wise to examine their insider trading policies and procedures to ensure they operate effectively in the wake of cyber incidents, including by considering whether to restrict trading by insiders before public disclosure.

Through both its disclosure guidance and its enforcement actions, the SEC stressed the importance of internal controls, a topic to which it returned by issuing an investigative report assessing whether nine public companies victimized by cyber fraud had failed to implement and maintain adequate internal controls that, in theory, could have protected them. The companies had fallen victim to "business email compromise" schemes, a widespread form of cybercrime in which

criminals pose as company executives or vendors to send email requests for wire transfers to bank accounts they control; after failing to detect the spoofed nature of such email requests, the companies transferred nearly $100 million to cyber criminals. While the SEC determined not to pursue any enforcement action against the companies, its report highlights the focus on cyber-related internal controls and serves as a warning that the Commission may consider such charges in the future.

While the SEC was active, many of the year's most important developments took place at the state level. All 50 states now have data breach notification laws, with requirements as to notification content, timing, and recipients varying across the country. In 2018, California not only passed a data privacy law modeled on the GDPR, but also enacted legislation addressing internet-based bot activity and security of devices connected to the Internet of Things (IoT). And the prescriptive cybersecurity regulations promulgated by New York's Department of Financial Services continued to take effect in rolling fashion. Absent preemptive legislation at the federal level, where proposals are currently stalled in Congress, we expect cybersecurity and data privacy laws and regulations to proliferate at the state level. Meanwhile, in connection with many of the year's most high-profile data breaches, it was state Attorneys General who took the lead in pursuing enforcement actions. For example, in the wake of Marriott's November announcement of a breach exposing the personal data up to 500 million customers, multiple state Attorneys General announced the opening of investigations. And in a first-of-its-kind state action to enforce the federal Health Insurance Portability and Accountability Act (HIPAA), the Attorneys General of twelve states joined forces in December to sue a medical records company for failing to safeguard patient data and timely disclose a breach that compromised the medical records of nearly four million individuals. From a practical perspective, these developments highlight the importance of monitoring state activity to anticipate future compliance challenges; on a policy level, they serve as a reminder that the consequence of federal inaction is not the *status quo*, but a ceding of leadership to state actors.

As cyber risks proliferate and the focus of legislators, regulators, and consumers on data protection and privacy intensifies, companies should ensure that their investment in, and attention to, cybersecurity and data privacy programs are properly calibrated. Close attention should be paid to the legislative and regulatory environment at the state, federal, and international levels to ensure that companies are not caught flat-footed by new compliance requirements. As emphasized by the SEC, companies should assess internal controls to ensure they address cyber-related risks, regularly review and exercise incident response plans to ensure

resilience, and gauge whether boards of directors are optimally engaged. Consideration should be given to the role cyber insurance could play as part of a risk mitigation program, and to the deployment of a program benchmarking tool, such as the NIST Cybersecurity Framework.

DOJ Developments

A year ago, we predicted that the second year of the current administration might well bring a decrease in corporate criminal enforcement actions. This prediction appears to have been on target. According to data compiled by Syracuse University, the number of white collar prosecutions fell by 3.7% compared to 2017 and by 31.1% since 2013. Notably, corporate fines and other monetary penalties have dropped even more precipitously: *The New York Times* estimates a 72% decline in corporate penalties in the first 20 months of this administration as compared to the last 20 months of the previous administration. It is hard to know whether these trends reflect a genuine shift in criminal enforcement policy or are simply the result of high-profile/high-penalty cases having already worked their way through the system since the financial crisis of 2008-09. Whatever the basis, in looking ahead, we suspect that DOJ will continue on the course it has followed for the past two years.

Importantly, DOJ announced a series of policy changes in 2018, signifying a more balanced approach to corporate enforcement. These policy revisions appear designed to provide greater transparency, predictability, and proportionality to corporations under investigation by increasing incentives to create and maintain robust corporate compliance programs and by clarifying the benefits from self-reporting wrongdoing and undertaking prompt remedial measures. Here are the highlights:

First, DOJ expanded the scope and applicability of its FCPA Corporate Enforcement Policy. In March 2018, DOJ announced that its FCPA Corporate Enforcement Policy would serve as "nonbinding guidance" in all — not just FCPA-related — Criminal Division corporate fraud investigations. In doing so, DOJ's Criminal Division agreed to extend leniency to companies that self-report corporate wrongdoing of all types, make proactive efforts to cooperate with DOJ, adopt comprehensive remediation programs, and disgorge any ill-gotten gains. During the summer and fall of 2018, DOJ further clarified that the benefits of the FCPA Corporate Enforcement Policy are available to companies that promptly self-report corporate wrongdoing discovered in the context of an acquisition or a merger, whether the conduct is FCPA-related or not.

Second, in November 2018, Deputy Attorney General Rod Rosenstein announced changes to the so-called "Yates Memo," which set forth requirements for companies to earn cooperation credit in connection with DOJ investigations. Under the Yates Memo, companies were required to identify *all* potentially culpable individuals to be eligible for *any* cooperation credit. While the identification of individuals responsible for wrongdoing remains a top priority, under the modified DOJ policy, corporations can qualify for full cooperation credit when they identify all individuals "substantially involved" in misconduct.

Third, DOJ codified its policy to discourage government authorities from "piling on" through the assessment of duplicative penalties for the same conduct, where a company faces overlapping inquiries from multiple authorities. Among other things, this policy instructs federal prosecutors to coordinate with one another and with all other federal, state, local, and foreign authorities in achieving the resolution of a matter.

Finally, DOJ modified its approach to the use of corporate monitors, narrowing the circumstances in which a monitor will be considered an appropriate component of a resolution. Now, corporate monitors may only be imposed where there is "a demonstrated need for, and clear benefit to be derived from" a monitor when compared to the costs and burdens. Moreover, according to DOJ, a monitor will likely be unnecessary where a corporation has a robust compliance program. In cases where a monitor is deemed necessary, the new policy mandates that the monitorship be "tailored" to the issues giving rise to it.

These new policies plainly provide greater clarity for corporations considering how best to respond to white collar investigations and potential enforcement proceedings. Recent non-prosecution agreements (NPAs) and deferred prosecution agreements (DPAs) likewise offer signals revealing what DOJ views as full cooperation and show the concrete advantages that may arise from such cooperation.

For example, in 2018, two financial institutions that had been investigated by DOJ's Fraud Section regarding payments allegedly made to bribe Libyan government officials resolved those inquiries on the same day. One institution received "full credit for its cooperation" and hence was able to resolve the investigation through an NPA, with no criminal charges filed. By contrast, the government granted the other institution only "substantial credit" for its cooperation and criminally charged that institution, requiring a DPA resolution at the parent level and a guilty plea by a wholly owned subsidiary. Through this pair

of contrasting resolutions, the government clearly intended to signal to the broader corporate audience that early and complete cooperation will be rewarded.

Cyber-related investigations were also a principal area of focus in 2018. As discussed in our cybersecurity update above, DOJ brought insider trading charges against corporate executives trading ahead of public disclosure of significant data breaches. Working with the CFTC, DOJ has also brought an increasing number of prosecutions relating to "spoofing," where traders use electronic bids to engage in market manipulation. With the CFTC publicly touting its commitment to spoofing enforcement, we expect this will remain an area of sustained focus in 2019. Another important institutional change is the newly created Task Force on Market Integrity and Consumer Fraud. While this task force, established in July, has a broad mandate, we expect a primary focus will be cyber fraud and other criminal misuse of technology.

SEC Developments

For the first time since 2015, the SEC operated with a full complement of five commissioners throughout most of 2018. Fiscal 2018 (which ended September 30) was also the SEC's first full year with Chairman Jay Clayton at the helm, and the enforcement docket now clearly reflects the priorities he identified early in his tenure.

Foremost among those priorities are an emphasis on combatting cyber threats and protecting retail investors. Highlights of the SEC's cyber program are discussed above at pages 2–3. While a wide variety of cases come within the effort to protect "Main Street" investors, the SEC highlighted two components in its own year-end enforcement review. First, was the Share Class Selection Disclosure Initiative, a self-reporting initiative addressing disclosure failures with respect to conflicts of interest associated with mutual fund fees. Second, the Enforcement Division devoted substantial resources to investigations involving initial coin offerings and digital assets, an area that will continue to receive emphasis.

While there has been some commentary suggesting that SEC enforcement activity has slowed, the results over the past year do not support that theory. Enforcement Division Co-Directors Stephanie Avakian and Steven Peikin have correctly observed that quantitative metrics — such as numbers of cases filed or total amounts of penalties assessed — are often not a very meaningful method to

measure the effectiveness of an enforcement program. Nonetheless, the SEC's 2018 enforcement statistics reflect some interesting trends.[1]

The SEC brought a total of 490 stand-alone enforcement actions in 2018 (excluding follow-on administrative proceedings and delinquent filing cases) — an increase over the 446 such cases filed in 2017 and the third-highest total since 2013. Indeed, after some decline in the number of cases brought in 2017 and the first half of 2018, there was a surge in enforcement activity in the second half of 2018. A similar pattern is evident in cases against public companies and their subsidiaries. In each six-month period from March 2015 through March 2017, the SEC brought between 44 and 54 cases against public companies. These numbers dropped to 19 cases in the second half of FY 2017 and 16 cases in the first half of FY 2018. That short trend reversed dramatically in the second half of FY 2018, when the SEC brought 55 cases against public companies. These fluctuations are not likely the result of any change in policy, and it is more likely that a push by the prior administration to bring cases before leaving office reduced the number of late-stage investigations in the pipeline by January 2017. High turnover in senior enforcement ranks early in the new administration likely had some impact on the progress of investigations. The current level of enforcement activity is noteworthy, given the hiring freeze in place since 2016.

The whistleblower program remains an important component of the SEC's enforcement arsenal. On February 21, 2018, in *Digital Realty*, the Supreme Court held that standing as a whistleblower for certain retaliation claims requires that a complainant have submitted a report to the SEC, rather than simply invoking internal corporate reporting mechanisms. *Digital Realty* thus magnified the financial incentive for potential whistleblowers to submit their concerns to the SEC. Not surprisingly, the SEC thereafter observed an increase in incoming reports, receiving 5,282 reports in 2018, the most in the whistleblower program's seven-year history. Consistent with historical experience, a large portion of the reports related to corporate disclosures and financial statements, exceeded only by reports of offering frauds. The agency distributed a total of $168 million in bounty payments to 13 whistleblowers in 2018 — more than the $158 million awarded in the entire prior history of the program. On July 20, 2018, the SEC proposed amendments to its whistleblower rules, including revisions to afford the Commission more flexibility in making awards. The public comment period ended

[1] The NYU Pollack Center for Law & Business and Cornerstone Research have published an informative study; see SEC Enforcement Activity: Public Companies and Subsidiaries.

on September 18, and it is likely that the Commission will act on the rule proposal in 2019.

In our annual review last year, we expressed the hope that the SEC would dial back some elements of the criminalization of its enforcement process that had arisen following the financial crisis. We did see some signs of a recalibration in 2018, including greatly reduced use of admissions in settled enforcement actions. The SEC obtained admissions in four books-and-records cases against broker-dealers that had submitted erroneous trade information to the Commission's own staff in response to "blue sheet" requests. The SEC also obtained admissions in a handful of other cases involving other reporting and internal controls violations, and one case in which a broker-dealer inaccurately reported to customers the venues in which trades were executed. While the SEC's more limited use of admissions is a positive development, we continue to see this enforcement tool as one that lacks a persuasive public policy rationale.

State Attorneys General

Since the change in administration in early 2017, we have expected state attorneys general to pursue more aggressive regulatory enforcement inquiries as part of an effort to compensate for real (or perceived) reductions in federal enforcement activity, including by DOJ, the SEC or the EPA. Indeed, in the aftermath of the presidential election, several historically active AG offices publicly pledged to expand their enforcement agendas.

In keeping with our prediction, many state AGs have commenced high-profile investigations in areas previously viewed as largely federal domains, such as the opioid abuse epidemic, climate change, financial services and environmental issues. Thus, in 2017, a coalition of 41 AGs issued subpoenas and document demands to leading pharmaceutical companies seeking information about how those companies manufactured, marketed and distributed prescription opioids. Over the past year, 10 AGs filed lawsuits against pharmaceutical distributors, and more than 30 AGs have brought claims against pharmaceutical manufacturers, in state and federal courts across the country. And AGs have gotten considerably more aggressive in pursuing claims for damages against various industries over alleged harm to the environment. Notably, as in other such AG actions, many of the AGs filing such lawsuits are assisted by outside counsel.

Similarly, a number of AGs have commenced investigations against energy-producing companies addressing the issue of climate change. In October

2018 — in perhaps the most high-profile of these investigations — the NYAG sued Exxon alleging that Exxon's public statements regarding climate change were false and misleading because they were inconsistent with Exxon's internal scientific findings.

Likewise, 50 AGs focused this past year on the financial services industry, an area historically dominated by federal regulation. In October 2018, the NYAG reached a $65 million settlement with Wells Fargo to resolve allegations that it misled investors regarding its cross-selling business model and related sales practices. Shortly thereafter, Wells Fargo also agreed to pay $575 million in a 50-state settlement resolving allegations of unfair trade practices — namely, that the bank had violated state laws by opening unauthorized accounts and enrolling customers into online banking services without their knowledge or consent.

These instances of large-scale AG investigations in 2018 exemplify a trend we expect will continue. As noted in our prior memos, state AG investigations can be particularly burdensome for companies for several reasons: *first*, while DOJ has announced a formal policy designed to deter multiple agencies from "piling on," state AGs have not hesitated to pursue investigations even when federal authorities already are focused on the same issues; *second*, as the above-cited examples demonstrate, AGs often work together, thereby creating risks of simultaneous litigation in multiple jurisdictions, with that threat often creating pressure to resolve such investigations even if the company is confident in its position; *third*, state AG litigation can be particularly difficult to defend, including because AGs often claim the right to seek aggregate damages on behalf of an entire State and to be exempt from certain defenses that ordinarily protect companies against private claims (*e.g.*, statute of limitations); and, *finally*, political considerations frequently drive such investigations, making resolutions harder to achieve. These factors illustrate why well-managed public companies should bear in mind that state-led inquiries will remain an important, and potentially challenging, feature of the regulatory and white collar landscape as 2019 unfolds.

Cross-Border Enforcement Developments

A. Economic Sanctions

Since taking office in January 2017, the new administration has continued a long-standing practice of relying on sanctions in support of foreign policy initiatives. In addition to sanctions involving Iran, which the current

administration has reinstated and expanded, the U.S. government continues to administer new and pre-existing sanctions involving Russia, North Korea, Venezuela and Cuba, among other countries. Against this backdrop, on November 19, 2018, DOJ announced an agreement with Société Générale to settle a long-running investigation of violations of U.S. sanctions laws targeting Cuba, Iran and Sudan. As part of the settlement — the first major sanctions case involving a global bank during the Trump administration — Société Générale agreed to pay a total of over $1.34 billion to resolve inquiries by DOJ and other federal and New York state authorities.

Meanwhile, the U.S. continues to seek the extradition of the Chief Financial Officer of Huawei Technologies, the world's second-largest smartphone vendor, who was recently arrested in Canada. Her high-profile arrest was based on allegations of trade sanction violations, for which Huawei is currently under investigation.

Given the often changing and complicated nature of sanctions regimes, and the administration's high-profile use of sanctions in policy matters, multinational companies are well advised to ensure that their sanctions compliance programs are up-to-date and that mechanisms are in place to review periodically the scope and effectiveness of those programs.

B. Deferred Prosecution Agreements in Foreign Countries

Outside of the United States, foreign governments are increasingly looking to the use of DPAs as an important new enforcement tool for resolving corporate criminal investigations. For example, in the three years since the U.K. Serious Fraud Office entered its first DPA with Standard Bank in 2015, it has secured three additional agreements (one in 2015 and two in 2017).

The French National Financial Prosecutor (PNF), which announced its first negotiated DPA agreement (known as a *convention judiciaire d'intérêt public* or CJIP) in November 2017, entered four new agreements in 2018. The most recent CJIP with French bank Société Générale, announced on June 4, 2018, resolved foreign bribery and corruption charges and was entered in conjunction with a settlement reached by the bank with DOJ based on the same conduct. Under the CJIP agreement, Société Générale agreed to pay penalties of over €250 million and be subject to a two-year monitorship by the French Anticorruption Agency. In its DOJ resolution, the bank agreed to a total penalty of more than $860 million, although DOJ agreed to credit the bank's payment to PNF.

Beyond these now-established DPA regimes in the U.K. and France, a similar regime — involving so-called "remediation agreements" — took effect in Canada in September 2018. The Canadian government stressed that the new regime was anticipated to "add[] new incentives for corporations to self-report and encourage[] stronger corporate compliance in a continually evolving marketplace." Similarly, Singapore passed legislation in March 2018 introducing a new DPA regime. Additional countries are currently at different stages of considering or implementing their own DPA regimes, including Australia and Switzerland, where DPA proposals are under consideration by lawmakers.

While the development and use of DPAs in foreign countries is still in its infancy, it is important to keep an eye on these developments as, in the right case, a foreign DPA regime may afford companies a tool for beneficial resolution of a cross-border investigation.

C. Foreign Corrupt Practices Act

FCPA enforcement continued at a crisp pace in 2018, consistent with the administration's stated commitment to robust enforcement. In 2018, DOJ secured seven corporate FCPA resolutions, including three DPAs and four NPAs, and monetary penalties ranging from $25 million to $853 million, while also bringing FCPA charges against 31 individuals. Meanwhile, applying its FCPA Corporate Enforcement Policy, DOJ declined to prosecute four corporations for FCPA violations based on their self-disclosure, full cooperation, and disgorgement of ill-gotten gains.

FCPA resolutions in 2018 also highlighted DOJ's increasing coordination with foreign enforcement agencies and its policy discouraging "piling on." For example in resolving a long-running and internationally coordinated FCPA investigation with an NPA and a $850 million penalty, DOJ afforded the Brazilian conglomerate Petrobras credit against 90 percent of the penalty for the fines it separately paid to Brazilian authorities and the SEC.

With the increasing level and sophistication of international cooperation and the number of foreign countries implementing anti-corruption laws, we expect continued growth in the volume of multinational investigations. Recent case law will likely reinforce this trend. *United States* v. *Hoskins* limited the extraterritorial scope of the FCPA by foreclosing the use of conspiracy or accomplice charges to extend the FCPA's extraterritorial reach to individuals and entities not otherwise subject to the statute's jurisdictional hooks, thereby likely spurring DOJ to work even more closely with its international partners.

D. Cross-Border Tax Enforcement

For some ten years running, cross-border tax enforcement has been a significant priority for the DOJ and IRS. While some wondered whether the final resolution under the DOJ's Swiss Bank Program in January 2016 might presage a substantially lower level of activity, events in 2018 make clear that cross-border tax enforcement remains high on the enforcement docket.

In September 2018, DOJ announced its first-ever conviction for failing to comply with the Foreign Account Tax Compliance Act (FATCA). The former Chief Executive and Chief Business Officer of Loyal Bank, an offshore bank (now in liquidation) with offices in Hungary and St. Vincent & the Grenadines, pled guilty to conspiring to defraud the IRS by failing to comply with the bank's FATCA reporting obligations for certain U.S.-related accounts. The case arose out of a sting operation in which the defendant agreed to help an undercover agent posing as a U.S. citizen engaged in a stock manipulation scheme to open bank accounts that would hide the purported U.S. client's beneficial ownership, including by failing to include the accounts in the bank's FATCA reporting. Over the course of 2018, DOJ also resolved three long-running Category 1 Swiss bank investigations — *i.e.*, that were initiated before the DOJ's Swiss Bank Program was announced in August 2013 — as well as a case with a Swiss asset management firm. Of note, in one of the Category 1 bank cases resolved by a DPA, the DOJ made a point of noting that the bank received reduced cooperation credit for dissuading two employees who had been indicted in 2012 from cooperating with the DOJ's investigation — even though the employees eventually agreed to plead guilty to a single misdemeanor conspiracy charge in connection with the resolution of the bank's case. Finally, DOJ and the IRS periodically underscore that they are mining a huge volume of data obtained from the array of DOJ and IRS enforcement efforts for additional investigative leads that span a multitude of offshore jurisdictions. Indeed, a senior DOJ Tax Division official recently noted that, in connection with its ongoing review of such data, DOJ is considering whether it makes sense to expand its successful Swiss Bank Program to financial institutions in other foreign jurisdictions.[2] While no decision has yet been made, the official sounded a cautionary note — *i.e.*, the data suggests that "some countries seem to be more popular than others" as destinations for assets leaving Swiss banks.

Against this backdrop of significant enforcement activity and risk, it remains critical for foreign financial institutions to ensure that they have effective

[2] Law 360 Tax Authority, 313-181, *DOJ Unsure On Expanding Swiss Bank Tax Crackdown*, November 9, 2018.

controls aimed at ensuring that U.S. indicia or other information that might suggest an undisclosed U.S. beneficial owner underlying an account or similar business relationship is properly identified, resolved, and documented in the on-boarding process or thereafter as a result of changes in status or receipt of new information.

E. Panama Papers

The massive leak of documents from the files of Panama-based law firm Mossack Fonseca, first reported in April 2016, was met with much fanfare. While enforcement authorities in a number of countries initiated inquiries, there were few major enforcement developments on this front until December 2018, when federal prosecutors in New York announced the first major Panama Papers-related prosecution. The case involves tax fraud, money laundering and other charges against four individuals connected to the now-shuttered offshore law firm, including a former Mossack Fonseca senior lawyer and a partner of a U.S.-based accounting firm. Of note, the indictment explains that, in connection with their investigation, U.S. authorities used undercover agents and covert recordings of conversations between one of the defendants and a cooperating former client. Less than a week after the indictment was unsealed, law enforcement officials in Frankfurt raided the offices of Deutsche Bank as part of a German investigation of the bank relating to an ongoing money laundering probe stemming from disclosures in the Panama Papers.

Protecting Privilege/Fifth Amendment Rights While Cooperating with the Government

In 2018, two cases illustrated the potential hazards that can arise when companies' efforts to cooperate with the government later provide a basis for individuals questioned during internal investigations to claim that their Fifth Amendment rights against self-incrimination were compromised. In *United States* v. *Connelly*, a former Deutsche Bank trader, on trial in the Southern District of New York for manipulating LIBOR rates, argued that statements he made to the bank's outside counsel during an internal investigation should be suppressed under the Fifth Amendment. He claimed that the bank, which had a policy requiring employees to cooperate with internal investigations or face termination, effectively acted as an arm of the government, particularly where it was shown that government prosecutors and regulators had consulted with the bank on which employees would be interviewed and outlined the scope and priorities of the internal investigation. To avoid an adverse ruling, prosecutors chose not to introduce the trader's statements at trial. Similarly, in *United States* v. *Blumberg*, a

securities brokerage executive argued that the government had violated his Fifth Amendment rights by delegating its investigative work to the brokerage firm's lawyers to such an extent that records of the company's internal investigation were essentially part of the government's files, thus obligating prosecutors to search those files for exculpatory materials.

In light of these developments, corporations conducting internal investigations — while also seeking full cooperation credit from the government— must be careful to design an internal review genuinely independent from the government and make clear when conducting employee interviews that counsel has been engaged by the company (or its board in appropriate cases) and that it will be up to the company (or board) to decide what use to make of information obtained in the interview. Such precautions will not only ensure that the company's attorney-client privilege under *Upjohn* v. *United States* will be properly protected, they will also blunt any later effort by inculpated employees to claim that the company participated in a violation of their Fifth Amendment rights.

Conclusion

As our summary suggests, 2018 turned out to be more eventful — at least in terms of new policy pronouncements — than one might have guessed at the outset of the year. As for 2019, our best sense at this point is that most of the trends identified here will continue largely on track. For that reason, careful due diligence — focused on potential white collar and regulatory issues — remains critically important for any contemplated transaction. This means not simply spotting issues, of course, but prudent analysis of possible self-reporting and the skillful design of an effective remediation plan. Likewise, the design, implementation, and periodic pressure-testing of compliance systems to ensure they are tailored to the reputational, legal, and regulatory risks faced by the underlying businesses are as important as ever.

John F. Savarese	Ralph M. Levene
Wayne M. Carlin	David B. Anders
Jonathan M. Moses	Marshall L. Miller