SQUIRE PATTON BOGGS

2020 White Collar and Government Investigations Year in Review

US – January 2021

Introduction

In 2020, the United States Department of Justice (the DOJ) and the Securities and Exchange Commission (the SEC) set new benchmarks for corporate enforcement, surpassing all previous records for fines secured for violations of the Bank Secrecy Act, the Foreign Corrupt Practices Act, the Securities and Exchange Act of 1934, and the False Claims Act. In resolving these cases, the DOJ continued to demonstrate the importance of effective corporate compliance.

The DOJ also made significant efforts to respond to the COVID-19 pandemic. After Congress passed the Coronavirus Aid, Relief, and Economic Security Act (the CARES Act), launching, among other initiatives, the Paycheck Protection Program (the PPP), the DOJ moved quickly to prosecute pandemic-related fraud.

Below is a list of the topics discussed in this alert (you may click on a topic to review the relevant section). For each topic, we identify key developments in compliance and enforcement, and provide relevant takeaways for senior management and compliance professionals.

The CARES Act and the Paycheck Protection Program

In an attempt to mitigate the economic impact of the COVID-19 pandemic, Congress passed the CARES Act on March 27, and shortly thereafter, the Small Business Administration (SBA) launched the PPP.[1] The PPP authorized the SBA to guarantee loans under Section 7(a) of the Small Business Act, to assist struggling small businesses to continue operations and maintain their employment levels.[2] Under the program, small businesses could quickly receive loans that, if utilized in accordance with certain requirements, would be forgiven by the SBA. To date, the SBA has disbursed more than $525 billion through hundreds of participating financial institutions.[3]

1 See https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.
2 *Id.* at Section 1102.
3 See https://www.justice.gov/usao-mdla/pr/attorney-general-announces-results-paycheck-protection-plan-criminal-fraud-enforcement.

While the CARES Act has brought needed relief to many small businesses, unscrupulous actors have sought to take advantage of the government's relief efforts and those members of the private sector, particularly financial institutions, who are expending unprecedented efforts to facilitate CARES Act relief to small businesses. Through aggressive enforcement efforts, Congress and the DOJ have sought to hold these bad actors responsible, and we anticipate that CARES Act enforcement efforts will continue for many years. In the short term, regulators have focused primarily on simple PPP fraud schemes involving dishonest borrowers. We have yet to see a significant effort to target financial institutions, other participating lenders, or recipients under other CARES Act programs. However, the extensive oversight mechanisms included in the CARES Act will almost certainly result in long-term efforts by regulators to claw back funds that were obtained through fraud. Below, we discuss the enforcement risks facing borrowers and financial institutions, and consider how they can mitigate these concerns in 2021.

Short-term Enforcement Trends

In the short term, the DOJ has focused its enforcement efforts on low-hanging fruit, targeting individuals that were clearly ineligible, or that utilized funds for impermissible expenses. On March 16, 2020, Attorney General William Barr directed all 93 US Attorneys' Offices to prioritize investigating and prosecuting PPP loan fraud cases.[4] Since then, federal prosecutors have charged more than fifty defendants with filing fraudulent PPP applications, involving over $175 million in disbursed loans.[5] Cases generally involve high-priced luxury items, phantom businesses, fraudulent certifications of financial need and outright theft.[6]

In October, for example, federal prosecutors in the Eastern District of Wisconsin announced indictments against five individuals for a fraudulent scheme to obtain PPP loans.[7] According to the DOJ, the defendants filed false PPP loan applications on behalf of nonexistent companies.[8] To support these applications, the defendants created false tax documents, misrepresented employee counts and falsified payroll expenses. The defendants ultimately obtained more than $1.1 million in PPP disbursements.

We expect the DOJ will continue to pursue such obvious cases of fraud, with the majority of the investigations led by local federal prosecutors. As these cases proliferate, financial institutions should expect to receive subpoenas for relevant documents, and ensure that their internal procedures for processing these requests and disclosing the information conform to prevailing best practices and federal law.

Federal inspector-generals have also worked diligently to identify and investigate fraudulent pandemic-related disbursements. The Special Inspector General for Pandemic Recovery (SIGPR) has entered into Memorandums of Understanding with numerous US Attorneys, allowing SIGPR to work alongside DOJ in investigating fraudulent loans.[9] The Inspector General for the SBA has also warned the SBA's CARES Act loan and grant programs. We anticipate that these awards will be subject to further investigation by the Inspectors General, and may ultimately result in criminal enforcement.[10] The Memorandum warned of "widespread potential fraud" in CARES Act disbursements, and internal control deficiencies resulting in $250 million in loans and grants to potentially ineligible recipients and $45.6 million in duplicative payments.[11] We anticipate that these awards will be subject to investigation, and may ultimately result in criminal enforcement.

Meanwhile, the House Select Subcommittee on the Coronavirus Crisis (the SSCC), chaired by Rep. James Clyburn (D-S.C.), has begun several investigations into the distribution of CARES Act funds. The SSCC has requested documents from Eastman Kodak Company regarding a $765 million loan for the production of pharmaceutical ingredients.[12] Chairman Clyburn also has called on some CARES Act funds recipients, including in the nursing home and aviation industries, to return the funds they received, and several companies have done so.[13]

Long-term Enforcement Risk

The CARES Act established three regulatory bodies to monitor the disbursement of CARES Act funds: SIGPR, the Pandemic Response Accountability Committee, and the Congressional Oversight Commission. It also provided additional funds to existing oversight bodies, including $20 million to the Government Accountability Office and $148 million to existing inspectors general. To date, their enforcement efforts have been largely preliminary in nature. We do not expect that trend to continue. The increasing availability of COVID-19 vaccines will likely shift Congressional and agency priorities from economic stabilization, to investigation and enforcement.

For those seeking guidance on how CARES Act enforcement may proceed over the next five years, the work of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) provides a pertinent example. Over the past 12 years, SIGTARP has recovered $11 billion in improperly disbursed payments from the legislative measures passed in the wake of the 2008 financial crisis, through litigation and criminal investigations conducted in partnership with the DOJ. SIGTARP investigations have also resulted in 450 indictments, 389 convictions and 305 prison sentences for fraudulent conduct related to TARP.

4 See https://www.justice.gov/usao-mdla/pr/attorney-general-announces-results-paycheck-protection-plan-criminal-fraud-enforcement.
5 *Id.*
6 *Id.*
7 See https://www.justice.gov/usao-edwi/pr/five-charged-connection-covid-relief-fraud-scheme.
8 *Id.*
9 See https://www.sigpr.gov/news.
10 See https://www.sba.gov/sites/default/files/2020-07/SBA_OIG_Report_20-16_508.pdf, at 1.
11 See id. at 2.
12 SBA IG's EIDL report, also https://www.oversight.gov/sites/default/files/oig-reports/SBA%20OIG%20Report%2021-03.pdf, https://www.oversight.gov/sites/default/files/oig-reports/SBA/SBA-OIG-Report-21-06.pdf and https://www.oversight.gov/sites/default/files/oig-reports/SBA_OIG_Report_20-14_508.pdf.
13 See https://coronavirus.house.gov/news/press-releases/following-select-subcommittee-inquiry-nursing-home-chain-returns-109-million; https://coronavirus.house.gov/news/press-releases/clyburn-calls-cargo-carriers-return-hundreds-millions-taxpayer-dollars; https://coronavirus.house.gov/news/press-releases/company-returns-10-million-taxpayer-funds-intended-small-businesses-response.

Congress modeled the SIGPR on SIGTARP, and in our view, its efforts to claw back improperly disbursed PPP funds have only just begun. One potential area of scrutiny involves the necessity for PPP loans. The CARES Act and its implementing regulations allowed businesses to self-certify that the funds were necessary for ongoing operations, and while the SBA and the Department of the Treasury subsequently issued extensive guidance to clarify loan eligibility, companies that did not require the funds to retain employees may have received loans, particularly in the early days of the program. SIGPR, in coordination with other oversight/enforcement agencies, may investigate these loans in the coming months.

We also anticipate that the changing dynamics in Congress will create opportunities for the Congressional Oversight Commission to scrutinize PPP and other CARES Act expenditures, and hold public hearings to investigate potential malfeasance. It is, therefore, imperative for companies that participated in PPP to carefully review all loan documents to ensure accuracy and document financial need, and for financial institutions to prepare for significant scrutiny of PPP payouts. This is particularly true for the loan forgiveness process. Moreover, now that both houses of Congress are controlled by Democrats, we expect that the chairperson of the Congressional Oversight Commission, who must be agreed to by the Speaker of the House and the Senate Majority Leader, will be appointed shortly.

Bank Secrecy Act, Economic Sanctions and Financial Crime Developments

Regarding the Bank Secrecy Act (BSA), economic sanctions, and other financial crime-related policy and enforcement, enforcement agencies announced a number of high-profile enforcement actions, as well as new policies, regulations and calls for comments on proposed regulations.

DOJ Resolves BSA Violations by the Industrial Bank of Korea

In April, the Industrial Bank of Korea (IBK) and its New York Branch (IBKNY) (collectively, the "Bank") entered into a Deferred Prosecution Agreement (DPA) with the US Attorney's Office for the Southern District of New York (SDNY), to resolve violations of the BSA, as well as various statutes governing US sanctions on Iran.[14] The Bank also entered into concurrent agreements with the New York Attorney General and the New York Department of Financial Services (NYDFS) over violations of New York law. The violations stemmed from the processing of more than $1 billion in transactions in violation of US sanctions.[15] Notably, the settlements followed a 2016 written agreement between the Bank, NYDFS and the Federal Reserve Bank of New York (the FRBNY), reached after regulatory examinations identified serious deficiencies in IBNKY's BSA/AML compliance function and its efforts to comply with regulations of the Department of the Treasury's Office of Foreign Asset Control (OFAC).

Below, we summarize the conduct resulting in the regulatory and criminal resolutions. We highlight key features of the DPA, including the determination that the Bank suffered a "programmatic failure" of its compliance function, so severe that DOJ found that the Bank acted with criminal willfulness. In addition, we provide key takeaways for BSA/AML practitioners to consider as they review their compliance program.

The Bank's Compliance Failures

The facts giving rise to the Bank's settlements began with the adoption of an inadequate, manual transaction monitoring system. According to the DPA, between 2006 and 2013, the Bank processed IBKNY transactions using a manual review system that required its one New York-based compliance staffer to manually review every transaction. The result was a backlog that prevented timely reports on suspicious activity.[16]

These deficiencies were repeatedly escalated to IBKNY management, and identified by the Bank's regulator. No action was taken in response. When compliance made repeated requests for additional support and resources, the requests were ignored.[17] Instead, management assigned an IT employee with limited English fluency to assist part time. These failures made it possible for more than $1 billion in transactions linked to Iran to pass through IBK. The transactions were initiated by a US citizen, who conspired with Iranian nationals to bypass US sanctions, by transferring funds through accounts at IBK and IBKNY.[18]

The DPA

As noted above, the DPA marks a rare instance where compliance failures were deemed so severe as to constitute a willful failure – that is, the specific intent – to violate the BSA. In reaching this conclusion, the SDNY criticized the Bank's complete failure to implement, over numerous examination cycles, an adequate transaction monitoring system, and emphasized the decisions of IBK and IBKNY management to disregard repeated warnings from compliance.[19]

Despite these failures, the Bank was only required to forfeit $50 million – or roughly 5% of the roughly $1 billion in unlawful transactions that passed through IBKNY. This remarkable narrowing likely resulted from the Bank's substantial cooperation and remediation efforts.[20] The SDNY lauded the Bank for its efforts to conduct a thorough internal investigation, to perform a granular analysis of the relevant transactions, and to collect and produce evidence located in other countries.[21] The SDNY also praised the Bank's remediation, including enhancements to its global governance and the creation of senior management committees to oversee the compliance function.[22]

14 See Department of Justice, Deferred Prosecution Agreement (the IBK DPA), Industrial Bank of Korea, https://www.justice.gov/usao-sdny/press-release/file/1270016/download.
15 See Statement of Facts, att'd as Ex. C to IBK DPA, at ¶¶3-4.
16 See *Id.* at ¶¶10-15.
17 See *Id.*
18 See *Id.* at ¶¶19-22.
19 *Id.* at ¶¶11-18.
20 See IBK DPA, at ¶¶36-37.
21 See *Id.*
22 See *Id.*

Key Takeaways for BSA/AML Professionals

The actions against IBK and IBKNY highlight the importance of resolving deficiencies in a timely manner. Here, IBK had numerous opportunities to address shortcomings, and failed to do so. Had the Bank made meaningful efforts to respond to deficiencies, it is unlikely that the SDNY would have found willful intent. Banks must also precisely calibrate their transaction monitoring systems to the prevailing risk environment, and ensure adequate staff are available to review high-risk transactions. This is an issue of paramount importance to financial regulators, who believe that the failure to identify suspicious activity and resolve transaction alerts results in delinquent reporting, and limits effective enforcement. Finally, the DPA demonstrates that, in appropriate circumstances, cooperation remains an important avenue for mitigating criminal conduct. IBK and IBKNY paid a total of $86 million to resolve allegations that involved eight years of examination failures and more than $1 billion in transactions that violated US law.

BitMEX Actions

DOJ and the Commodity Futures Trading Commission (CFTC) both brought enforcement actions against BitMEX, an online trading platform for futures contracts and other derivative products tied to the value of cryptocurrencies. Each action alleged that BitMEX failed to implement required anti-money laundering policies and procedures. The SDNY charged four individuals with causing a financial institution to violate the BSA. The indictment asserted that BitMEX served customers located in the US, and, therefore, was a futures commission merchant that had to comply with the BSA. The defendants, all executives of BitMEX, allegedly failed to establish, implement and maintain an adequate AML program, including adequate customer identification (CIP) and "Know Your Customer" (KYC) programs. The defendants allegedly took steps to attempt to exempt the company from the application of US laws and regulations; for example, the indictment claims that the defendants incorporated BitMEX in the Seychelles, believing they could still serve US customers but avoid having to adopt BSA-compliant AML and KYC programs.

The indictment also focused on BitMEX's alleged failure to know the true identities of its customers. Customers could register to trade anonymously without providing any identifying information or documentation, and BitMEX's initial marketing advertised that it did not require advanced verification. Moreover, the government alleged that the steps that BitMEX did take, such as implementing an internet protocol (IP) address check in response to CFTC public enforcement orders, were intentionally designed to be ineffective. The IP address check only prevented using a US IP address to register with BitMEX. After successfully registering, a customer could freely access BitMEX's platform from US IP addresses or by using a virtual private network (VPN), which permitted the customer to circumvent the IP address check and which BitMEX took no steps to preclude.

DOJ Civil Forfeiture Recovery Relating to 1MDB

The DOJ in 2020 continued to seek the recovery of assets allegedly traceable to corruption involving 1Malaysia Development Berhad (1MDB), a Malaysian sovereign wealth fund. In July, the DOJ announced the filing of civil forfeiture complaints seeking the forfeiture and recovery of approximately $96 million in assets associated with funds allegedly embezzled from 1MDB.[23] This followed an announcement in May that DOJ had reached a settlement of civil forfeiture cases against more than $49 million worth of assets, and an April announcement that it had repatriated to Malaysia approximately $300 billion in additional funds misappropriated from 1MDB.[24] The DOJ announced in September that it had settled certain civil forfeiture cases against assets acquired with funds allegedly embezzled from 1MDB.[25] The DOJ announced a few days later that it had filed additional civil forfeiture complaints relating to assets allegedly associated with misappropriated 1MDB funds.[26]

Combined with earlier forfeiture complaints dating back to July 2016, the US has sought the forfeiture of more than two billion dollars in assets related to the 1MDB scandal. According to a DOJ press release, the case represents the largest action brought under the department's Kleptocracy Asset Recovery Initiative, as well as the largest civil forfeiture action in DOJ's history.

Statements on Enforcement of the Bank Secrecy Act

The Financial Crimes Enforcement Network (FinCEN) issued a Statement on Enforcement of the Bank Secrecy Act (the Statement) that described the agency's approach for future BSA investigations.[27] The Statement was intended to "provide clarity and transparency" on how FinCEN would impose penalties for failures in BSA compliance.[28] Most notably, FinCEN declared that in future investigations, it will not "treat noncompliance with a standard of conduct announced solely in a guidance document" as a separate violation of law.[29] Instead, enforcement actions will only occur if FinCEN can "establish a violation of law based on applicable statutes and regulations," after regulated parties receive "an opportunity to respond to and contest factual findings or legal conclusions."[30]

Two other aspects of the Statement deserve consideration. First, FinCEN affirmed that it will "consider the need to impose compliance commitments" to ensure that financial institutions satisfy all BSA obligations after the resolution of an investigation.[31] Second, FinCEN further stated that in determining whether to bring an enforcement action, it would review institutional compliance with "registration, recordkeeping, and reporting requirements," and review the adequacy of AML compliance programs.

23 https://www.justice.gov/opa/pr/us-seeks-recover-approximately-96-million-traceable-funds-allegedly-misappropriated-malaysian.
24 https://www.justice.gov/usao-cdca/pr/united-states-reaches-settlement-recover-more-49-million-assets-acquired-funds; https://www.justice.gov/opa/pr/us-repatriates-300-million-malaysia-proceeds-funds-misappropriated-1malaysia-development.
25 https://www.justice.gov/opa/pr/united-states-reaches-settlement-recover-more-60-million-involving-malaysian-sovereign-wealth.
26 https://www.justice.gov/opa/pr/us-seeks-recover-more-300-million-additional-assets-traceable-funds-allegedly-misappropriated#:~:text=The%20Justice%20Department%20announced%20today,(1MDB)%2C%20a%20Malaysian%20sovereign.
27 See https://www.fincen.gov/news/news-releases/fincen-statement-enforcement-bank-secrecy-act.
28 See *Id.*
29 See https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf.
30 *Id.*
31 *Id.*

Similarly, the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration, and Office of the Comptroller of the Currency (OCC) issued in August a Joint Statement on Enforcement of BSA/AML Requirements.[32] The Joint Statement indicated that it did not create new expectations or standards, but was intended to further clarify the agencies' enforcement of the BSA – particularly the conditions that require the issuance of a mandatory cease and desist order. The Joint Statement further noted that isolated or technical violations or deficiencies were generally not considered the types of issues that would result in an enforcement action. Additionally, the Joint Statement addresses how the agencies evaluate violations of the required "pillars" of a BSA/AML compliance program.

Final Rule on AML Compliance, Customer Identification and Beneficial Ownership for Banks Lacking a Federal Functional Regulator

In September, FinCEN issued a final rule establishing AML program standards for banks lacking a federal functional regulator, including private banks, privately insured credit unions and certain trust companies.[33] The rule also extended customer identification and beneficial ownership requirements to these institutions.[34] Institutions falling within the scope of the rule have until March 15, 2021 to comply. Previously, such institutions were required to comply with certain BSA obligations, including filing suspicious activity reports, but did not have to have in place AML programs that included the "four pillars" listed in the BSA at 31 U.S.C. § 5318(h): (1) internal policies, procedures, and controls; (2) a designated compliance officer; (3) an ongoing employee training program; and (4) an independent audit function. The final rule removes that exemption. Similarly, such institutions now must comply with BSA regulations that require banks' AML programs to have in place appropriate risk-based procedures for conducting ongoing customer due diligence. Such due diligence requires, at a minimum, procedures for (1) understanding the nature and purpose of customer relationships, and (2) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including the beneficial owners of legal entity customers.

Notably, FinCEN did not expect the rule to significantly increase compliance costs. Instead, the rule anticipates that institutions will be able to build upon their existing compliance practices and ensure compliance with "relatively minimal cost and effort."[35] FinCEN also incorporated flexibility into the rule, allowing banks to take a risk-based approach, and tailor their AML program to their specific size, needs and risks. For example, if a bank is small, has no high-risk customers, or does not engage in high-risk transactions, FinCEN anticipates that the burden of compliance will be "commensurately minimal."[36]

Advisories to Financial Institutions on Cyber-Events and Cyber-Enabled Crime

FinCEN issued in October an Advisory on ransom payments for cybersecurity attacks.[37] The Advisory recommended that financial institutions report payments potentially related to ransomware. FinCEN informed financial institutions that it expected a Suspicious Activity Report (SAR) if an institution suspected that a transaction involved a ransomware payment.[38] In keeping with prior FinCEN guidance on cyber-related crime, FinCEN also stated that SARs should include detailed cyber indicators, including email addresses, Internet Protocol addresses with respective timestamps, virtual currency wallet addresses, mobile device information, and descriptions and timing of suspicious electronic communications.[39]

For financial institutions, the Advisory has significant implications. While FinCEN previously advised banks to report suspicious transactions involving cybercrime, and incorporate details about the potential crime, the advisory expands those requirements to ransomware. Previously, FinCEN had not requested SAR information for transactions where legitimate entities made ransomware payments. The Advisory makes clear that any payment potentially involving a ransomware incident now requires the filing of a SAR that includes all relevant indicia of cybercrime. The Advisory also has implications for companies and individuals that suffer ransomware attacks. Companies that pay a cybercriminal in response to a ransomware attack should now expect that information about the payment will be disclosed to federal regulators, and could result in inquiries from law enforcement.

Similarly, OFAC issued an advisory on the potential sanctions risks for facilitating ransomware payments.[40] OFAC's advisory urges companies that engage with victims of ransomware attacks (e.g., cyber insurers, digital forensics and incident response firms, and financial institutions that may process ransom payments) to implement risk-based compliance programs that account for the risk that a ransomware payment may involve a specially designated national or blocked person, or a comprehensively embargoed jurisdiction. OFAC also noted that it would consider a company's self-initiated, timely and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining appropriate enforcement responses, should the situation be later determined to have a sanctions nexus.

32 https://www.fdic.gov/news/press-releases/2020/pr20091a.pdf.
33 See https://www.govinfo.gov/content/pkg/FR-2020-09-15/pdf/2020-20325.pdf.
34 See *Id.*
35 *Id.*
36 *Id.*
37 See https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
38 *Id.*
39 See https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.
40 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

Pandemic-Related Financial Crime Guidance

FinCEN, along with other regulators, issued a plethora of guidance and advisories in 2020 relating to the COVID-19 pandemic. FinCEN recognized that financial institutions might face hurdles in conducting business as usual, including BSA compliance, during the pandemic. It has asked COVID-19-impacted banks to let FinCEN know about potential delays in filing required BSA reports, such as SARs.[41] FinCEN created a COVID-19-specific online contact mechanism, and encouraged banks to contact their functional regulator or other BSA examining authority if it had BSA compliance concerns because of the pandemic.[42] Because FinCEN has specialized teams of lawyers and investigators for certain suspicious activity (e.g., medical scams, or fraud targeting the elderly), it has asked financial institutions to be specific in describing the COVID-19-related activity in their SAR narratives.

FinCEN also identified trends in malicious and fraudulent transactions arising out the pandemic. COVID-19-related financial crime trends and concerns include investment scams (e.g., a false claim that a product can prevent, detect, or cure COVID-19), imposter scams (e.g., providing personal information in return for COVID-related stimulus payments or benefits), product scams (e.g., transactions for unapproved or misbranded products), unemployment insurance fraud and using the emerging personal protective equipment market as a way to launder money. FinCEN's website provides detailed information on red flag indicators related to such transactions.[43] Additionally, FinCEN provided guidance on meeting BSA requirement relating to PPP (Payment Protection Program) loans, including a set of FAQs that explains when beneficial ownership should be collected for such loans.[44]

Other financial regulators issued similar COVID-19-related materials. For example, the OCC noted that it would work with affected banks to reduce their burden when scheduling examinations or inspections, and would work with banks that might experience problems fulfilling their reporting responsibilities under the BSA.[45] OFAC reiterated that the sanctions programs administered by OFAC generally allow for legitimate humanitarian-related trade, assistance or activity, and that, for items requiring specific licenses, it would prioritize and expedite the review of such requests.[46]

National Defense Authorization Act

A final key financial crimes compliance development this past year was the passage of the National Defense Authorization Act (NDAA). The NDAA passed in both the Senate and House of Representatives before President Trump vetoed it in December; Congress then passed the NDAA over the veto and the NDAA became law on January 1, 2021. The NDAA includes the Anti-Money Laundering Act of 2020 (AML Act) and the Corporate Transparency Act. The AML Act expands the BSA to mandate that AML/CFT programs should be risk-based, which includes "ensuring that more attention and resources of financial should be directed toward the higher-risk customers and activities, consistent with the risk profile of a financial institution, rather than toward lower-risk customers and activities." Keeping with this risk-based approach, the BSA will require the Secretary of the Treasury, alongside other government entities, to establish and make public priorities for AML/CFT policy.

The AML Act also expands the BSA's application to dealers in antiquities, and requires the assessment of BSA application to dealers in arts. The BSA's definition of "financial institutions" (31 U.S.C. § 5312) will now include persons "engaged in the trade of antiquities, including an advisory, consultant, or any other persons who engages as a business in the solicitation or the sale of antiquities." This provision will take effect on the effective date of the final rules issued by the Secretary of the Treasury to carry out the amendment; such proposed rules must be issued within 360 days after the Act's enactment. Additionally, the Act requires the Department of the Treasury, in coordination with other agencies, to perform a study of the facilitation of money laundering and the financing of terrorism through the trade in works of art.

The AML Act also amends the BSA's whistleblower section (31 U.S.C. § 5323), which previously allowed the Secretary of the Treasury to pay a reward to BSA whistleblowers, which led to recoveries exceeding $50,000 – the Secretary had discretion to determine the amount of the reward, but could not award more than 25% of the net amount of the recovery or $150,000, whichever was less. Now, the recovery threshold is for monetary sanctions that exceed $1 million, but allows recovery of up to 30% of what the government collects from the imposed monetary sanctions. The whistleblower provision provides the criteria the Secretary should consider when making an award, such as the significance of the information and the degree of assistance provided by the whistleblower. The whistleblower section also provides protection for whistleblowers by prohibiting employer retaliation.

41 https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions.
42 https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial.
43 https://www.fincen.gov/coronavirus.
44 https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial; https://www.fincen.gov/sites/default/files/2020-04/Paycheck_Protection_Program_FAQs.pdf.
45 https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-34.html.
46 https://home.treasury.gov/system/files/126/covid19_factsheet_20200416.pdf; https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200420.

The Corporate Transparency Act, also part of the NDAA, revolves around new beneficial ownership information reporting requirements. This Act notes that because most or all states do not require information about the beneficial owners of corporations and similar entities, federal legislation providing for the collection of beneficial ownership information was needed to set clear standards for incorporation practices, protect national security interests, and bring the US into compliance with international AML/CFT standards. This new section defines "beneficial owner" as an individual who, directly or indirectly, exercises substantial control over the entity or owns or controls not less than 25% of the ownership interests of the entity.

Following regulations prescribed by the Secretary of the Treasury, covered companies that have been formed or registered before the effective date of the regulations must, "in a timely manner, and not later than two years after the effective date of the regulations," submit a report to FinCEN regarding beneficial ownership. This report must identify each beneficial owner of the entity by full legal name, date of birth, current residential or business street address and a unique identifying number from an acceptable identification document (as an alternative to this last requirement, an entity can provide a "FinCEN identifier" number, issued by FinCEN). If an exempt entity has a direct or indirect ownership interest in the covered reporting company, the company need only list the name of the exempt entity. Covered companies formed or registered after the regulations must submit their reports to FinCEN at the time of formation or registration. Companies must then, "in a timely manner and not later than one year after the date on which there is a change," submit an updated report to FinCEN. Note that the Act lists numerous parties that are exempt from reporting beneficial ownership information. The Act generally prohibits FinCEN from disclosing reported beneficial ownership information, although it may disclose such information upon receipt of a request from certain federal and state agencies, as well as requests from financial institutions subject to customer due diligence requirements, with the consent of the covered reporting company, to facilitate the financial institution's compliance with due diligence requirements.

Anti-Bribery and Corruption Developments

This past year was a landmark one for the FCPA unit, a division of the Fraud Section of the DOJ vested with exclusive jurisdiction to enforce the Foreign Corrupt Practices Act (FCPA), 15 U.S.C. § 78dd-1, et. seq. In recent years, an apparent decline in FCPA investigations led many practitioners to speculate on the shifting priorities of Fraud Section leadership. The significant rise in declinations, and the skeptical views of the FCPA expressed by President Donald Trump, raised more questions about the future of FCPA enforcement.

Recent settlements with Airbus and Goldman Sachs prove that rumors of declining FCPA enforcement were exaggerated. The DOJ remains laser focused on policing corrupt conduct in foreign markets. Compliance professionals and senior management must, therefore, remain vigilant, and ensure that anti-bribery and corruption (ABC) programs evolve to target new risks. Below, we discuss these settlements, and highlight critical features of the respective agreements. We then discuss how companies and compliance professionals can apply lessons from these cases to enhance their ABC controls.

The DOJ also revised two critical guidance documents that focus on ABC compliance: the Resource Guide to the US Foreign Corrupt Practices Act (the Resource Guide)[47] and the Evaluation of Corporate Compliance Programs.[48] These documents provide a broad view of how the DOJ will approach allegations of corporate malfeasance, and identify key elements of an effective corporate compliance program.

Airbus Agrees to Resolve Bribery Claims With the DOJ and Foreign Regulators

The FCPA unit started 2020 by making international headlines. On January 31, authorities in the US, the UK and France jointly approved DPAs with Airbus S.E. (Airbus) in the largest corporate corruption settlement in history. Airbus agreed to pay over $3.9 billion to resolve allegations that it used third parties to bribe government officials, in violation of the FCPA, the Arms Export Control Act (AECA), and its implementing regulations, the International Traffic in Arms Regulations (the ITAR).[49]

The Bribery Scheme

The conduct at issue was straightforward, and unremarkable in the FCPA context. According to the DPA, in 2008, Airbus executives decided to bribe foreign officials to obtain business from state-owned entities, including foreign militaries and state-owned airlines. Over the next seven years, Airbus used consultants to pay these bribes, concealing the payments with fraudulent contracts, false invoices and false activity reports. These facts parallel many recent FCPA enforcement actions.

47 Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, "A Resource Guide to the U.S. Foreign Corrupt Practices Act" (Second Edition), https://www.justice.gov/criminal-fraud/file/1292051/download.

48 U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.

49 Press Release, U.S. Department of Justice, "Airbus Agrees to Pay Over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case" (Jan. 31, 2020).

What sets Airbus apart is the scale of the bribery payments. According to the DPA, Airbus allegedly funneled $50 million to AirAsia Group directors through the sponsorship of a sports team, $2 million to the wife of a Sri Lankan Airlines executive, $3.3 million to senior staff at Indonesia's national airline and millions more to Ghana military officials.[50] Further, between 2013 and 2015, Airbus allegedly bribed Chinese government officials, and hid these transactions through a Hong Kong bank account.[51] The DPA also emphasized the use of golf retreats and all-expense-paid trips.

The Deferred Prosecution Agreement

To resolve the allegations, Airbus agreed to a criminal fine of $527 million, and further agreed to pay $55 million to the State Department for violations of the ITAR.[52] As part of the DPA, the DOJ agreed to reduce the original penalty of $2.3 billion, based on payments made to French and UK authorities. Airbus received full cooperation credit for gathering evidence, identifying legal issues, and presenting relevant facts.[53] Airbus did not receive a voluntary disclosure credit, because it only disclosed the FCPA violations after the UK's own investigation became public.

Airbus also received remediation credit. Importantly, the DPA emphasized that Airbus rapidly implemented remedial measures, including the termination of relationships with business partners involved in the alleged bribery-related conduct. Airbus froze payments, sent formal termination notices, and adopted enhanced due diligence procedures to vet future business partners. The DPA also praised the company's efforts to enhance its compliance function, and take disciplinary action against culpable employees.

Key Takeaways

The Airbus resolution offers valuable insight into DOJ enforcement priorities, and practical lessons for ABC compliance. First, the DPA signals that the DOJ continues to enhance its ability to coordinate enforcement efforts with foreign authorities. To investigate Airbus, the DOJ worked with the UK's Serious Fraud Office, and the French National Financial Prosecutor. The DPA is also notable for the deference afforded to French and UK authorities. The DOJ followed its policy against duplicative penalties and "piling on", by giving Airbus credit for payments made to foreign authorities. The DOJ also decided against imposing a third-party monitor, instead allowing French authorities to oversee the company's compliance remediation efforts. These choices suggest that in the future, the DOJ may defer to foreign authorities with a clear jurisdictional nexus to the relevant conduct, provided the foreign government has adequate enforcement mechanisms.

The DPA also offers lessons for ABC compliance. The DOJ paid particular attention to the lavish gifts and travel offered to Chinese officials, noting that these luxurious trips to the US often coincided with business negotiations. The DOJ linked these expenses to the fraudulent scheme. Companies must remain vigilant when conducting business with foreign officials, and ensure that expenses are lawful, subject to thorough compliance oversight, and in line with industry norms.

The DOJ also emphasized the failure of Airbus to adopt a global emphasis on compliance. Specifically, the DPA emphasized that while Airbus had a written compliance program and a well-funded compliance infrastructure, the company failed to ingrain a compliance focus in its global operations. It is, thus, imperative that senior management instill the appropriate tone at the top regarding compliance. The strongest compliance program "on paper" is of little use if senior executives do not operationalize the program across corporate divisions and in all subsidiaries. The Airbus DPA signals that merely "checking the box" by building a formal compliance program will leave a company extremely vulnerable to regulatory scrutiny.

Revisions to Evaluations of Corporate Compliance Programs

Five months later, in June, the DOJ issued a revision to its criteria for the Evaluation of Corporate Compliance Programs.[54] The document was revised in April of 2019, so the changes were not extensive, but practitioners should still pay careful attention, as the revisions reflected the DOJ's ongoing emphasis on a practical, flexible approach to compliance focused on function, rather than form.

As an example, the DOJ modified one of its overarching questions – focused on the efficacy of implementation – to consider instead whether a program has sufficient resources and authority to achieve its objectives.[55] The update also instructed prosecutors to consider why a company has designed the compliance program, the goals of the program and how the program has evolved over time to address a changing risk environment.[56] Prosecutors will also consider whether a compliance program has sufficient flexibility, continuous access to relevant data from all corporate functions and robust testing procedures.[57]

The DOJ also addressed third-party risk management, and mergers and acquisitions. For third parties, the revision puts significant emphasis on efforts to track and monitor the relationship over the life of a contract.[58] Companies that only conduct preliminary due diligence, without revisiting the findings, arguably do not satisfy this standard. With respect to mergers and acquisitions, the revision instructs companies to ensure that they rapidly integrate an acquisition target into their existing compliance infrastructure, and pay close attention to the unique risks presented by the acquisition.[59]

50 DOJ Deferred Prosecution Agreement (Jan. 30, 2020).
51 *Id.*
52 DOJ Deferred Prosecution Agreement (Jan. 30, 2020).
53 *Id.*
54 See U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (Updated June 2020), https://www.justice.gov/criminal-fraud/page/file/937501/download.
55 See *Id.*
56 See *Id.*
57 See *Id.*
58 See *Id.*
59 See *Id.*

The revisions as a whole emphasized a practical approach to compliance, focused on ensuring adequate staff and resources, access to contemporaneous data about compliance risk, and mitigation of the risk environment. To ensure that their compliance function satisfies this standard, companies should take and document steps to ensure adequate funding, continuously review their risk environment, and whether the compliance function provides a sufficient deterrent, and conduct thorough auditing and risk testing to identify vulnerabilities.

Revisions to the FCPA Resource Guide

In July, the DOJ and the Securities and Exchange Commission (SEC) revised the Resource Guide – the primary enforcement manual for companies that operate overseas. Published in 2012 to educate compliance professionals, the Resource Guide summarizes DOJ and SEC expectations for ABC compliance, and offers practical examples from prior corruption investigations.

Eight years have passed since the publication of the Resource Guide. During that time, the anti-corruption landscape changed dramatically. Declinations have increased, monitors have fallen out of favor, the DOJ now routinely cooperates with foreign counterparts and data analytics has produced effective tools for reducing corruption risk. It was, therefore, surprising that the revisions were relatively modest, and largely reflect developments in DOJ policy and legal precedent over the past decade.

The first notable revision was the incorporation of new precedent. The rise of individual FCPA prosecutions has finally given the federal courts the opportunity to opine on the statutory language. The revised Resource Guide incorporates three of these decisions: United States v. Esquenazi, 752 F.3d 912 (11th Cir. 2014), United States v. Seng, No. 15-cr-706 (S.D.N.Y. July 26, 2017), and United States v. Hoskins, 902 F.3d 69 (2d. Cir. 2018).

Esquenazi defined "instrumentality" under the FCPA to include entities controlled by a foreign government, including state-owned corporations, provided the entity performed a function that the controlling government "treats as its own."[60] Seng limited the FCPA's "local law" defense to situations where the conduct at issue was expressly permitted by the written laws of the foreign jurisdiction.[61] And Hoskins limited secondary liability claims against foreign nationals – including conspiracy and aiding and abetting – to situations where the defendant could also be charged as a principal.[62] The Resource Guide acknowledges each of these decisions and the resulting limitations on future enforcement efforts, but also cites contrary precedent, such as the recent district court decision in United States v. Firtash, 392 F. Supp. 3d 872, 889 (N.D. Ill. 2019) (disagreeing with Hoskins on the application of secondary liability).

The Resource Guide also addressed corporate compliance programs. The DOJ provided anonymous case studies of resolved cases, showing that a declination is possible even when senior management approves large bribe payments. The DOJ also affirmed that even if an FCPA violation goes undetected, a declination is still possible, provided a company has a "robust compliance program" operated in good faith.[63] And the Resource Guide expanded the prior guidance on Hallmarks of Effective Compliance, requiring that companies now investigate, analyze and remediate all reported misconduct – "the truest measure of an effective compliance program."[64]

Finally, the Resource Guide considered the question of corporate monitors. Since 2012, monitors have been widely criticized by compliance professionals and corporate executives as a costly and unnecessary intrusion into corporate operations that continue long after appropriate remediation. The revisions incorporated language from a 2018 memorandum by then-Assistant Attorney General Brian Benczkowski, requiring prosecutors to balance the benefits of a monitor with the costs and long-term impact on operations, and providing a multi-factor test for whether a monitor is necessary.[65] However, the Resource Guide went beyond the memorandum to impose additional mandates, specifically, that monitors should never be imposed as a punitive sanction, and that where a company coordinates a settlement with the DOJ and the SEC, a single monitor will be sufficient to oversee both settlement agreements.[66]

Goldman Sachs Resolves 1MBD-Related Bribery Investigation

After beginning 2020 with the record-setting Airbus resolution, DOJ again made headlines in the fall, resolving long-standing allegations against Goldman Sachs. On October 22, the DOJ and the SEC settled allegations that Godman Sachs violated the FCPA by conspiring to pay more than $1 billion in bribes to officials in Malaysia and the United Arab Emirates.[67] Goldman Sachs admitted to violations of the FCPA, and further agreed to pay more than $2.9 billion in penalties and disgorgement.[68] Goldman Sachs also agreed to resolve similar claims with authorities in the UK, Malaysia and Singapore; the DOJ credited $1.6 billion in payments from these resolutions toward the $2.9 billion penalty. The settlement followed several individual prosecutions involving former Goldman Sachs employees.[69] In a parallel settlement with the SEC, Goldman admitted to violations of the "books and records" and internal controls provisions of the FCPA, and agreed to pay $600 million in disgorgement, and a $400 million civil penalty.[70]

60 *Hoskins*, 902 F.3d at 69.
61 Resource Guide, at 24.
62 *Hoskins*, 902 F.3d at 76-97.
63 Resource Guide, at 68.
64 *Id.*
65 See *Id.* , at 24.
66 See *Id.*
67 See https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.
68 See *Id.*
69 See *Id.*
70 See https://www.sec.gov/news/press-release/2020-265.

The Fraudulent Scheme

As part of the DPA, Goldman admitted to a five-year bribery scheme that began in 2009, and ultimately involved $1.6 billion in illicit payments.[71] Officials in Malaysia affiliated with the Malaysian Sovereign Wealth Fund, commonly known as 1MDB, would steer lucrative bond offerings to Goldman Sachs. In return, Goldman Sachs employees would divert payments from 1MDB back to these officials.[72] Similarly, officials in the United Arab Emirates that oversaw the Abu Dhabi sovereign wealth fund would steer opportunities to Goldman Sachs, and Goldman Sachs employees in the region would redirect a portion of the resulting fees to these officials.[73] To make these bribe payments, Goldman Sachs employees circumvented the bank's internal controls, disguising the payments and preventing accurate recording of the payments in the bank's books and records.[74] Goldman also failed to adequately conduct due diligence over the Malaysian officials involved in the scheme, failed to address red flags about corruption risk associated with the bond transactions, and failed to implement adequate internal controls to prevent the scheme.[75]

The Settlement Agreement

A number of elements of the DPA deserve mention. Goldman Sachs did not voluntarily disclose the wrongful conduct to the DOJ or the SEC, and the DOJ focused on the involvement of senior Goldman Sachs officials in approving the transactions at issue, noting that these officials ignored red flags and circumvented the bank's compliance program.[76] The DOJ also emphasized the scale of the bribery scheme, involving some $1.6 billion in payments, and the high-level officials in foreign markets that received the bribery payments.[77] While Goldman Sachs did cooperate in the DOJ investigation, the bank only received partial cooperation credit. The DOJ criticized the bank for its failure to timely produce relevant evidence, including telephone recordings where "bankers, executives and control function personnel discussed allegations of bribery and misconduct …."[78]

SEC Whistleblower Program Developments

Not to be outdone, the SEC also made headlines in 2020, resolving high-profile investigations of Wells Fargo and Goldman Sachs, and setting a record for the distribution of award payments to whistleblowers. The latter is particularly significant, because the staff awarded more whistleblower payments, to more individuals, than ever before.[79]

The SEC's whistleblower reward program dates to the 2010 Dodd-Frank Act, when Congress directed the SEC to establish the Office of the Whistleblower (the OWB) to approve and distribute payments to those providing material information about violations of the federal securities laws.[80] Under the implementing regulations, if a whistleblower provides information resulting in an enforcement action that results in sanctions of $1 million or more, the SEC may award the whistleblower between 10% to 30% of the sanctions collected.[81]

To date, the program has awarded over $735 million to 128 individuals. In 2020 alone, the staff awarded more than $175 million to 39 whistleblowers – more than 20% of the total amount disbursed since the program's inception.[82] The related cases ran the gamut of securities enforcement, from violations of the Foreign Corrupt Practices Act and insider trading, to accounting violations and false pricing. The SEC also adopted amendments to the rules governing the whistleblower program that will likely result in even larger awards in the coming years. We discuss each of these developments below.

Summary of 2020 Whistleblower Awards

As noted above, the SEC distributed a record number of payments in 2020. The 39 awards paid during fiscal year 2020 constitute 30% of the total number of awards since 2010. The OWB also processed more claims – 6,900 – than ever before.[83] That number represents a 31% increase over the previous high.[84]

Given these numbers, it is not surprising that the SEC also distributed the two largest awards in program history. In June, the SEC made a $50 million payment to an individual who provided detailed information regarding the misconduct of his employer – a scheme the SEC had yet to detect.[85] Then, in October, the SEC awarded an incredible $114 million to a whistleblower who provided information that resulted in concurrent enforcement actions by the SEC and another agency.[86] That award was particularly important because of the facts at issue; the whistleblower repeatedly attempted to report the misconduct, and only contacted the staff when the company failed to take meaningful action.[87]

71 See https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.
72 See *Id.*
73 See *Id.*
74 See Statement of Facts, att'd as Attachment A to Deferred Prosecution Agreement, "United States of America v. Goldman Sachs Group Inc.," October 22, 2020, at 9, https://www.justice.gov/criminal-fraud/file/1329926/download.
75 See https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion.
76 See *Id.*
77 See *Id.*
78 *Id.*
79 "2020 Annual Report to Congress, Whistleblower Program," U.S. Securities and Exchange Commission (FY 2020), https://www.sec.gov/files/2020%20Annual%20Report_0.pdf (hereinafter "2020 Annual Report").
80 Pub. L. No. 111-203, § 922(a), 124 Stat. 1841 (2010).
81 15 U.S.C. § 78u-6(b)(1).
82 See 2020 Annual Report.
83 *Id.*
84 *Id.*
85 "SEC Awards Record Payout of Nearly $50 Million to Whistleblower," Release No. 2020-126 (June 4, 2020), https://www.sec.gov/news/press-release/2020-126.
86 "SEC Issues Record $114 Million Whistleblower Award," Release No. 2020-266 (Oct. 22, 2020), https://www.sec.gov/news/press-release/2020-266.
87 *Id.*

The SEC also made two awards in 2020 to compliance and audit professionals.[88] Exchange Act Rule 21F-4(b)(4)(iii)(B) generally prohibits awards for information obtained from "compliance or internal audit responsibilities."[89] However, an exception applies if the whistleblower discloses the information to the audit committee, chief legal officer, or chief compliance officer, and at least 120 days pass.[90] In March, the SEC paid $450,000 to a compliance employee who reported misconduct to a supervisor, then waited 120 days before notifying Commission staff.[91] In December, the SEC awarded $300,000 to an auditor who disclosed potential violations of the federal securities laws.[92] Office Chief Jane Norberg highlighted that award as "an example of the important role that audit and compliance professionals can play in assisting the Commission's enforcement efforts, especially when the entity is attempting to thwart an investigation."[93]

Whistleblower Rule Amendments

In another significant development, the SEC amended the rules governing the whistleblower program to provide greater transparency, efficiency and clarity.[94] As amended, Rule 21F-6(c) creates a rebuttable presumption that a whistleblower is entitled to maximum award allowed by statute, provided the award payment is less than $5 million.[95] To rebut the presumption, the staff must cite one of the negative factors enumerated by Rule 21F-6(b).[96] These include shared culpability, unreasonable delay in disclosing information, and interference with internal compliance and reporting systems.[97] If the potential award exceeds $5 million, the staff will continue to apply the existing factors to award determinations.[98]

The SEC also clarified the scope of its discretion to determine awards, either as a percentage of the settlement, or as a fixed dollar amount.[99] Rule 21F-6 provides a number of factors for the staff to consider in determining the scale of an award, including the significance of information provided, the degree of assistance rendered, and the programmatic interests of the agency in the enforcement action.[100] In an effort to address public confusion about the Commission's discretion in applying those factors, the amendments expressly affirm the SEC's "broad discretion" to determine an award in percentage terms, dollar terms or some combination thereof.[101]

Key Takeaways

The growth of the whistleblower program in 2020 provides a timely reminder for public companies and regulated firms about the importance of a robust compliance function, and the value of thoroughly investigating internal reports of employee misconduct. As the SEC continues to expand the scope of the program, and the size of the awards grows, employees will have even more incentive to disclose wrongdoing – particularly when management ignores their concerns. It is, therefore, imperative that regulated entities devote sufficient resources to their compliance and audit departments, and develop a compliance culture that incorporates industry best practices and prevailing norms. In particular, companies must pay close attention to reports of misconduct made through employee hotlines, or to compliance officers. Over the past year, the staff has repeatedly demonstrated its willingness to punish companies that suppress or disregard valid concerns; companies must, therefore, carefully investigate all internal allegations, and if an allegation is deemed frivolous or unsupported, the basis for that determination should be supported by ample documentation.

The growth of the whistleblower program also merits a reminder about the prohibition on retaliation, and the parallel prohibition on impeding reports to the SEC. Section 21F(h)(1) of Dodd Frank Act and Exchange Act Rule 21F-17(a) prohibit companies from taking any action to prevent reports to the SEC.[102] The staff has brought a dozen enforcement actions or administrative proceedings involving violations of this rule, including one in FY 2020.[103] In this most recent action, the staff penalized the defendant, in part, for attempting to silence employees with threats and sanctions.[104] Companies must, therefore, adopt rigorous procedures to prevent retaliation, and ensure that all officers and managers receive adequate training on these procedures.

88 "SEC Awards $450,000 to Whistleblower," Release No. 2020-75 (Mar. 30, 2020), https://www.sec.gov/news/press-release/2020-75; "SEC Awards More Than $300,000 to Whistleblower with Audit Responsibilities," Release No. 2020-316 (Dec. 14, 2020), https://www.sec.gov/news/press-release/2020-316.
89 17 CFR § 240.21F-4(b)(4)(iii)(B).
90 17 CFR § 240.21F-4(b)(4)(v)(C).
91 "SEC Awards $450,000 to Whistleblower," Release No. 2020-75 (Mar. 30, 2020), https://www.sec.gov/news/press-release/2020-75.
92 "SEC Awards More Than $300,000 to Whistleblower with Audit Responsibilities," Release No. 2020-316 (Dec. 14, 2020), https://www.sec.gov/news/press-release/2020-316.
93 *Id.*
94 *SEC Adds Clarity, Efficiency and Transparency to Its Successful Whistleblower Award Program*, Release No. 2020-219 (Sept. 23, 2020), https://www.sec.gov/news/press-release/2020-219.
95 17 CFR § 240.21F-6(c).
96 17 CFR § 240.21F-6(b).
97 *Id.*
98 *SEC Adds Clarity, Efficiency and Transparency to Its Successful Whistleblower Award Program*, Release No. 2020-219 (Sept 23, 2020), https://www.sec.gov/news/press-release/2020-219.
99 *Id.*
100 See 17 CFR § 240.21F-6(a).
101 *Whistleblower Program Rules, Securities and Exchange Commission*, Release No. 34-89963 (Sept. 23, 2020), https://www.sec.gov/rules/final/2020/34-89963.pdf.
102 15 U.S.C. 78u-6(h)(1); 17 CFR § 240.21F-17(a).
103 *Securities and Exchange Commission v. Collector's Coffee (d/b/a Collectors Café), and Mykalai Kontilai*, No. 19-Civ-04355 (S.D.N.Y. filed May 14, 2019), https://www.sec.gov/litigation/litreleases/2019/lr24658.htm.
104 *Id.*

DOJ Efforts to Address the Opioid Epidemic

Since 2016, the Health Care Fraud Section of the DOJ has worked with federal prosecutors across the country to address the ongoing epidemic of opioid abuse. To combat the illicit distribution and use of opioid-based pain medications, the DOJ indicted physicians and drug manufacturers, increased regulatory enforcement, facilitated information sharing across state and federal agencies, and funded opioid-related research.[105] In 2020, the DOJ expanded these efforts, bringing a series of groundbreaking civil and criminal actions against individuals and opioid manufacturers. Below, we summarize these actions, and discuss the compliance implications for health care providers and drug manufacturers.

Sentencing of Insys Therapeutics Executives

The first major development in the opioid space occurred in January, when a federal judge in the District of Massachusetts sentenced senior executives of Insys Therapeutics (Insys) to lengthy prison terms for conspiring to bribe doctors to prescribe Subsys, their fentanyl-based spray. Dr. John Kapoor, the company founder and Chief Executive Officer, received 66 months in prison,[106] while other executives received terms ranging from 12 to 33 months.[107]

Prosecutors alleged that Kapoor and the other executives funneled the bribe payments through Insys "speaker programs."[108] These programs purportedly allowed physicians to discuss of the Insys fentanyl spray. In reality, Insys used the programs to direct substantial payments to physicians, in exchange for prescribing Insys opioids. Practitioners who failed to meet satisfactory prescribing requirements were ineligible for the program, and the speaker "meetings" often provided no professional education.[109] Instead, the meetings featured lavish dinners, organized by Regional Sales Director Sunrise Lee, a former exotic dancer. Lee received a 12-month sentence for her role in the conspiracy.[110]

Insys also defrauded insurers by obtaining prior authorization for opioid prescriptions. Many insurers initially refused to cover Insys products without such authorization. To circumvent this limitation, Insys built a call center, where employees posed as physicians and other medical professionals.[111] When an insurer refused to cover Insys products without prior authorization, Insys employees would call the insurer, falsely state their professional credentials and affiliation, and make misleading statements about the patient's condition to secure coverage.[112] The scheme often required Insys employees to exaggerate the severity of a patient's condition, as Subsys was approved for use only when other treatments failed to mitigate cancer pain.

Phillip Coyne, Special Agent in Charge of the U.S Department of Health and Human Services, Office of the Inspector General, commented that these sentences would "undoubtedly send a clear message to health care executives relying on illegal schemes to increase profits: they will be held accountable for corporate crimes." Coyne put drug manufacturers on notice that efforts to circumvent the law to increase profitability would result in severe consequences, and pledged to "attack the opioid crisis from all angles, including holding the pharmaceutical industry and its leadership accountable."[113]

Strike Force Takedowns

The onset of the COVID-19 pandemic in early March temporarily chilled opioid-related prosecutions, as the DOJ shifted its focus to pandemic-related fraud. That gap proved to be short-lived. In September, the DOJ and the Centers for Medicare and Medicaid Services (CMS) announced the largest coordinated health care fraud and opioid-related prosecution to date, charging 345 defendants with submitting false and fraudulent claims worth some $6 billion to federal health care providers and private health insurers.[114]

In addition to telemedicine fraud, the Strike Force focused on "sober homes" and traditional health care fraud. Sober homes provide inpatient treatment and services to patients seeking help with substance abuse. The DOJ charged more than a dozen defendants with submitting false and fraudulent claims for drug testing and drug treatment.[115] The defendants included physicians, treatment facility operators and so-called "patient recruiters" – contractors paid to identify addicts with sufficient resources to pay for treatment. The Strike Force also charged more than 240 defendants with conspiring to submit false and fraudulent claims to Medicare, Medicaid and private insurers.[116]

Commenting on the work of the Strike Force, Acting Assistant Attorney General Brian Rabbitt stated that the operation would "hold accountable those medical professionals and others who have exploited health care benefit programs and patients for personal gain."[117] Rabbit further emphasized the DOJ's "ongoing commitment to ensuring the safety of patients and the integrity of health care benefit programs," regardless of the ongoing pandemic.[118]

105 DOJ, *Department of Justice Strategy to Combat Opioid Epidemic* (Sept. 21, 2016), https://www.justice.gov/opioidawareness/file/896776/download.
106 DOJ U.S. Attorney's Office District of Massachusetts, "Founder and Former Chairman of the Board of Insys Therapeutics Sentenced to 66 Months in Prison" (Jan. 23, 2020), https://www.justice.gov/usao-ma/pr/founder-and-former-chairman-board-insys-therapeutics-sentenced-66-months-prison.
107 *Id.*
108 *Id.*
109 *Id.*
110 *Id.*
111 Id.
112 *Id.*
113 *Id.*
114 DOJ Office of Public Affairs, "National Health Care Fraud and Opioid Takedown Results in Charges Against 345 Defendants Responsible for More than $6 Billion in Alleged Fraud Losses," (Sept. 30, 2020), https://www.justice.gov/opa/pr/national-health-care-fraud-and-opioid-takedown-results-charges-against-345-defendants.
115 *Id.*
116 *Id.*
117 *Id.*
118 *Id.*

Settlement With Purdue Pharmaceuticals

Shortly after the Strike Force indictments, the DOJ announced the long-anticipated resolution of civil and criminal claims involving opioid manufacturer Purdue Pharmaceuticals, and a related civil settlement with members of the Sackler family who controlled the company.[119] As part of these settlements, Purdue agreed to cease operations in its existing form, and, after completion of bankruptcy proceedings, become a public benefit company (PBC) functioning entirely in the public interest.[120]

In settling the DOJ allegations, Purdue admitted criminal culpability. Purdue acknowledged that it deliberately marketed opioid products to health care providers, when the company had reason to believe these providers were unlawfully dispensing opioids.[121] Purdue further admitted to violating the Anti-Kickback Statute, by using cash payments to reward physicians for prescribing its opioid products.[122]

To resolve these criminal claims, Purdue agreed to a criminal fine of $3.5 billion, and further agreed to forfeit $2 billion in profits. However, Purdue can offset up to $1.775 billion of the forfeiture through contributions to state and local governments from its corporate successor.[123] Regarding the guilty pleas, Deputy Attorney General Jeffrey A. Rosen said that the settlement would "send a strong message to the pharmaceutical industry that illegal behavior will have serious consequences" and "underscore the Department's commitment to its multi-pronged strategy for defeating the opioid crisis."[124]

The concurrent civil settlement resolved additional claims against Purdue and individual members of the Sackler family. The DOJ alleged that by promoting the unnecessary and excessive distribution of opioids, and working with unethical physicians, Purdue and the Sackler family caused providers to submit false claims to Medicare and Medicaid.[125] The settlement also resolved allegations that Purdue engaged in kickback schemes to induce opioid prescriptions. Under the terms of the civil settlement, Purdue provided the US with an unsecured bankruptcy claim for $2.8 billion.[126]

The separate civil settlement with the Sackler family resolved allegations that family members focused corporate marketing efforts on high-volume opioid prescribers who engaged in unlawful and unethical practices, and transferred assets to avoid civil liability. Under the terms of the civil settlement, the named members of the Sackler family are required to pay the United States $225 million.[127] While the criminal and civil claims are now resolved, Purdue continues to face claims in bankruptcy court from the 24 states seeking to hold Purdue responsible for damages caused by opioid abuse.

Walmart Opioid Litigation

Finally, in December, DOJ announced a civil suit against Walmart Stores, alleging that the company unlawfully dispensed pharmaceuticals in violation of the Controlled Substances Act (the "CSA"). The complaint alleged that Walmart knowingly filled thousands of controlled substance prescriptions with no legitimate medical purpose, and further filled prescriptions outside the ordinary course of pharmacy practice. The complaint also alleged that, as the operator of its distribution centers, Walmart received hundreds of thousands of suspicious orders that it failed to report, as required to by the DEA.

"It has been a priority of this administration to hold accountable those responsible for the prescription opioid crisis. As one of the largest pharmacy chains and wholesale drug distributors in the country, Walmart had the responsibility and the means to help prevent the diversion of prescription opioids," said Jeffrey Bossert Clark, Acting Assistant Attorney General of the Civil Division. "Instead, for years, it did the opposite – filling thousands of invalid prescriptions at its pharmacies and failing to report suspicious orders of opioids and other drugs placed by those pharmacies. This unlawful conduct contributed to the epidemic of opioid abuse throughout the US. Today's filing represents an important step in the effort to hold Walmart accountable for such conduct."[128] At the time of the filing, Walmart was already facing civil claims brought by state and local governments alleging that Walmart pharmacies contributed to the opioid crisis. Walmart has denied those allegations, and in anticipation of the DOJ lawsuit, filed a lawsuit in October against DOJ and DEA, seeking clarification of its roles and responsibilities under the CSA.[129]

Key Takeaways

With vaccines for COVID-19 scheduled for widespread distribution in the coming months, it is all but certain that the DOJ and its partners will continue to pursue opioid-related cases, and bring indictments against physicians and pharmaceutical manufacturers. Therefore, the aggressive approach to opioid and health care enforcement taken by the DOJ over the past 12 months offers valuable lessons for pharmaceutical manufacturers, physicians and other health care providers.

119 DOJ Office of Public Affairs, "Justice Department Announces Global Resolution of Criminal and Civil Investigations with Opioid Manufacturer Purdue Pharma and Civil Settlement with Members of the Sackler Family," (Oct. 21, 2020) https://www.justice.gov/opa/pr/justice-department-announces-global-resolution-criminal-and-civil-investigations-opioid.

120 *Id.*

121 *Id.*

122 *Id.*

123 *Id.*

124 DOJ U.S. Attorney's Office District of New Jersey, "Opioid Manufacturer Purdue Pharma Admits Guilt in Fraud and Kickback Conspiracies" (Nov. 24, 2020), https://www.justice.gov/usao-nj/pr/opioid-manufacturer-purdue-pharma-admits-guilt-fraud-and-kickback-conspiracies

125 DOJ Office of Public Affairs, "Justice Department Announces Global Resolution of Criminal and Civil Investigations with Opioid Manufacturer Purdue Pharma and Civil Settlement with Members of the Sackler Family" (Oct. 21, 2020) https://www.justice.gov/opa/pr/justice-department-announces-global-resolution-criminal-and-civil-investigations-opioid.

126 *Id.*

127 *Id.*

128 DOJ Office of Public Affairs, "Department of Justice Files Nationwide Lawsuit Against Walmart Inc. for Controlled Substances Act Violations" (Dec. 22, 2020), https://www.justice.gov/opa/pr/department-justice-files-nationwide-lawsuit-against-walmart-inc-controlled-substances-act.

129 Walmart Inc., "Walmart Sues DOJ and DEA Seeking Clarity for Pharmacists in Dispensing Prescription Opioids" (Oct. 22, 2020), https://corporate.walmart.com/newsroom/2020/10/22/walmart-sues-doj-and-dea-seeking-clarity-for-pharmacists-in-dispensing-prescription-opioids.

First, it is clear from the actions against Purdue and Walmart that the DOJ remains focused on addressing the opioid epidemic, and will pursue claims against manufacturers and executives where possible. Drug makers involved in the distribution of opioid-based medications should carefully review their compliance program, and ensure the function has adequate staffing, sufficient funding and the complete support of senior management. Manufacturers should also review all marketing and distribution programs to ensure those programs are compliant with federal law and industry standards. Similarly, health care providers who submit claims to CMS for reimbursement must ensure that all services provided are medically necessary and supported by adequate documentation. Finally, providers engaged in the practice of pain management must fully adhere to the federal and state rules governing the distribution of pain medications, ensure that all patient prescriptions are medically required, and avoid accepting of any inducements from drug manufacturers.

Telehealth Developments and Risks of Fraud and Abuse

The COVID-19 pandemic provided the impetus for a dramatic expansion in virtual medicine and telehealth in 2020. To avoid unnecessary transmission of the virus, and to allow hospitals to focus their services on COVID-19 patients, providers began using videoconference services to diagnose and treat patients. The crisis atmosphere galvanized action by Congress and regulators, who moved quickly to remove long-standing regulatory barriers to virtual medicine, and rapidly allowed providers to adopt these platforms to treat patients, and receive appropriate compensation from Medicare. Private insurers followed suit, rapidly revising payment guidelines to facilitate telehealth services. While many of these decisions were cabined to the pandemic-driven "public health emergency," Centers for Medicare and Medicaid Services Administrator Seema Verma has commented that "the genie is out of the bottle," and does not anticipate a reduction in telehealth services when the pandemic subsides. Below, we discuss the most significant regulatory changes to the telehealth landscape, identify potential risks that providers face, and highlight best practices for providers to avoid regulatory scrutiny.

Changes to Medicare Provisions and Compliance Best Practices

Before the COVID-19 pandemic, government reimbursement for telehealth services was extremely limited. Medicare reimbursed a limited number of services, generally for patients in rural areas who would otherwise have to travel. Lawmakers crafted these provisions to address specific concerns about the risk of fraud and abuse.

The CARES Act directed CMS and the Department of Health and Human Services to broadly expand Medicare reimbursement during the COVID-19 public health emergency.[130] The expansion applies across the universe of patient care, encompassing reimbursable services, permissible service sites and professionals eligible for reimbursement. CMS and HHS have temporarily added more than 145 services that Medicare beneficiaries may receive by telehealth during the public health emergency. CMS has also lifted existing restrictions to where care may be delivered, and expanded allowable services to new patients.[131] For example, beneficiaries may now receive care, including check-ins and e-visits for existing patients, from the comfort of the home, and hospitals may bill Medicare for facility fees and services furnished remotely by hospital. Physicians may also provide services across state lines, subject to state licensure requirements. CMS has expanded the providers able to invoice for services provided remotely, to include all practitioners eligible to bill Medicare for professional services. There are some limitations – for example, CMS generally requires services be provided using devices that permit two-way, real time audio and/or visual communications – but most practitioners are now able to provide a much wider range of services remotely. Finally, CMS has waived, for the duration of the COVID-19 public health emergency, all previous limits for the frequency of telehealth visits, including for skilled nursing facility visits and critical care consultations.

The extent to which these modifications will be made permanent remains to be seen. Congress must waive the statutory restrictions on telehealth reimbursement for any permanent changes to occur; the CARES Act suspended these regulations for the duration of the pandemic. Congress has already proposed multiple amendments to the Medicare Act that would make it easier for beneficiaries to continue to receive care at home, and give HHS more authority to expand telehealth services.[132] CMS is actively working to expand telehealth services within the limits of existing law. For example, CMS recently finalized modest changes to its annual physician fee schedule for telehealth services.[133]

130 See Coronavirus Aid, Relief, and Economic Security Act (CARES Act) §§ 3703-3707.

131 See "Medicare and Medicaid Programs; Policy and Regulatory Revisions in Response to the COVID–19 Public Health Emergency," 85 Fed. Reg. 19,230, 19,244-19,245 (Interim Final Rule, April 6, 2020).

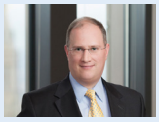
132 Examples of proposed legislation include the House's "Protecting Access to Post-COVID-19 Telehealth Act," which, among other things, would remove some originating site requirements for Medicare beneficiaries and make a patient's home an eligible site to receive telehealth care, and the Senate's "Telehealth Modernization Act," which would also remove geographic and originating site restrictions, as well as give HHS authority to permanently expand the types of authorized telehealth services and providers.

133 See Medicare Program; CY 2021 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment Policies; Medicare Shared Savings Program Requirements; Medicaid Promoting Interoperability Program Requirements for Eligible Professionals; Quality Payment Program; Coverage of Opioid Use Disorder Services Furnished by Opioid Treatment Programs; Medicare Enrollment of Opioid Treatment Programs; Electronic Prescribing for Controlled Substances for a Covered Part D Drug Under a Prescription Drug Plan or an MA-PD Plan; Payment for Office/Outpatient Evaluation and Management Services; Hospital IQR Program; Establish New Code Categories; and Medicare Diabetes Prevention Program (MDPP) Expanded Model Emergency Policy, 85 Fed. Reg. _____ (Dec. 2020).

Regardless of whether the status quo remains in place, the changes to telemedicine require careful attention by physicians and health care compliance professionals to reduce the risk of fraud and abuse. Providers should develop rigorous diagnostic procedures to ensure that patients – particularly new patients – are directed to the appropriate professional, whether that be in person or via telehealth. Providers should also anticipate that CMS and the HHS Office of the Inspector General (OIG) will carefully scrutinize telehealth claims. It is, therefore, highly important that providers and their staff document in detail the specifics of the services provided, including how the services were initiated, the audio-visual medium used and the duration of the service. Telehealth appointments billed in time increments are a particularly ripe area for scrutiny, so providers must pay careful attention to ensure all time entries are accurate, and correspond to services rendered. Finally, physicians should take care not to advertise the waiver of co-payments and deductibles. Generally, HHS and the DOJ view such waivers as inducements, in violation of the Anti-Kickback statute.

Authors

For more information about this publication or other related topics, please contact one of the lawyers listed below. We also encourage readers to subscribe to The Anticorruption Blog.



Colin R. Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Coates Lear
Partner, Denver
T +1 303 894 6141
E coates.lear@squirepb.com

Rebekah J. Poston
Partner, Miami
T +1 305 577 7022
E rebekah.poston@squirepb.com

Clay W. Porter
Partner, New York
T +1 212 872 9839
E claiborne.porter@squirepb.com

Kevin McCart
Partner, Washington DC
T +1 202 457 6457
E kevin.mccart@squirepb.com

Margaret E. Daum
Partner, Washington DC
T +1 202 457 6468
E margaret.daum@squirepb.com

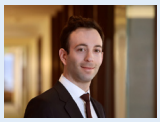
Marisa T. Darden
Principal, Cleveland
T +1 216 479 8627
E marisa.darden@squirepb.com

Rebecca A. Worthington
Principal, Washington DC
T +1 202 626 6654
E rebecca.worthington@squirepb.com

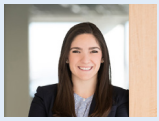
S. Babu Kaza
Senior Associate, Washington DC
T +1 202 457 6442
E babu.kaza@squirepb.com

Trevor T. Garmey
Senior Associate, Washington DC
T +1 202 457 6516
E trevor.garmey@squirepb.com

Ericka A. Johnson
Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com



Chase Goldstein
Associate, Los Angeles
T +1 213 689 5108
E chase.goldstein@squirepb.com



Elizabeth Weil Shaw
Associate, Denver
T +1 303 894 6129
E elizabeth.weilshaw@squirepb.com

Patrick Morris
Associate, Washington DC
T +1 202 457 6096
E patrick.morris@squirepb.com