Diligent

2021 White Collar Enforcement Review and Expectations for 2022

The inauguration of Joseph R. Biden, Jr. as President of the United States in January of 2021 marked not just the transition of power to new Administration, but a seismic shift in enforcement priorities as well. Unlike the Trump Administration—which had proven to be exceptionally business-friendly in many regards—the Biden Administration promised to usher in a new era of broad accountability for industry and government alike.

2021 began however, not with action on the part of the Biden Administration, but with an announcement on January 8, 2021 by the lame duck Trump Administration of a $130 million settlement with Deutsche Bank Aktiengesellschaft over alleged violations of the Foreign Corrupt Practices Act ("FCPA") and purported commodities fraud. With respect to the FCPA specifically, a criminal probe into Deutsche Bank by the U.S. Department of Justice ("DOJ") revealed a scheme to conceal corrupt payments and bribes made to third-party intermediaries by falsely recording corresponding entries in Deutsche Bank's books and records and circumventing internal accounting controls designed to detect and deter such unlawful conduct. Under a Deferred Prosecution Agreement ("DPA") reached with the DOJ, Deutsche Bank agreed to pay a criminal monetary penalty of $79,561,206 related to its FCPA misconduct and a separate criminal monetary penalty of $5,625,00 related to resolving commodities fraud charges, in addition to criminal disgorgement of $681,480 and another $1,223,738 in victim compensation. In a separate action with the U.S. Securities and Exchange Commission ("SEC"), Deutsche Bank agreed to cease and desist from further violations of the FCPA and to pay additional disgorgement and prejudgment interest of $43,329,622.

Unlike blockbuster enforcement activities of the previous year—which included enormous multi-billion-dollar settlements with aviation giant Airbus SE—the Deutsche Bank settlement was the first in a steady stream of enforcement activities announced by the DOJ and SEC to resolve longstanding investigations. In total, the DOJ initiated or resolved approximately two-dozen FCPA enforcement actions for the year, while the SEC initiated a total of five such actions.

As of the date of this publication, official statistics concerning qui tam actions—that is, claims brought by private citizens to recover government expenditures made as the result of fraud or other misconduct under the auspices of the False Claims Act ("FCA")—were not immediately available. However, if 2020 was any indication, the number of qui tam actions filed in 2021 is likely to be even more substantial than the previous year. As the COVID-19 pandemic showed no signs of relenting and governmental expenditures on healthcare needs (including personal protective equipment, respirators, and vaccinations) soared to unprecedented heights, 2021 created an environment that was ripe for corruption and fraud. In a February 17, 2021 speech at the Federal Bar Association's Qui Tam Conference, Acting Assistant Attorney General Brian M. Boynton placed pandemic-related fraud at the very top of the list of the Civil Division's enforcement priorities for the year. In the same speech, Boynton announced the first successful settlement involving the Coronavirus Aid, Relief, and Economic Security ("CARES") Act's Paycheck Protection Program ("PPP"). SlideBelts, Inc. (an internet retail company) and its CEO Brigham Taylor, agreed to pay $100,000 in damages and penalties to the U.S. government over allegations that it made false representations as to its status as a debtor in bankruptcy to obtain $350,000 in PPP loans.

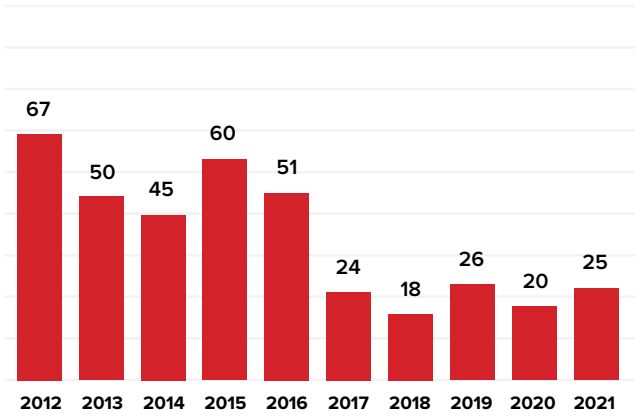
In this white paper, we provide a high-level review of some of the more significant developments, activities, enforcement actions, and resolutions at the SEC, DOJ (Criminal and Civil Divisions), the Commodity Futures Trading Commission ("CFTC"), the U.S. Department of the Treasury (including the Office of Foreign Asset Control or "OFAC"), and the Financial Crimes Enforcement Network, with a focus on the FCPA, antitrust laws, financial and accounting fraud, and U.S. sanctions violations. Because U.S. regulatory agencies frequently coordinate to bring criminal and/or civil actions against the same entities and individuals based on the same or similar misconduct, for some significant areas of the law (e.g., antitrust, FCPA), we will discuss those legal topics as a whole; in other sections, we will discuss the agencies. As such, there is some unavoidable overlap. Additionally, while the focus of this white paper generally corresponds to FY 2021, there are instances in which more recent developments—those occurring after September 30, 2021—are mentioned for additional context.

Antitrust In 2021 And Beyond

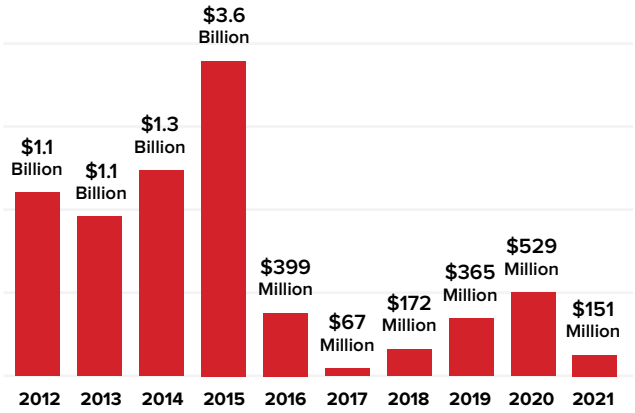
Criminal Enforcement:

As of November 16, 2021, the DOJ's Antitrust Division secured $151 million in criminal fines and penalties in FY2021—down a five-year high of $529 million in 2020. The following are the Antitrust Division's "Criminal Enforcement Trend Charts" showing 2021 statistics in relation to previous years:

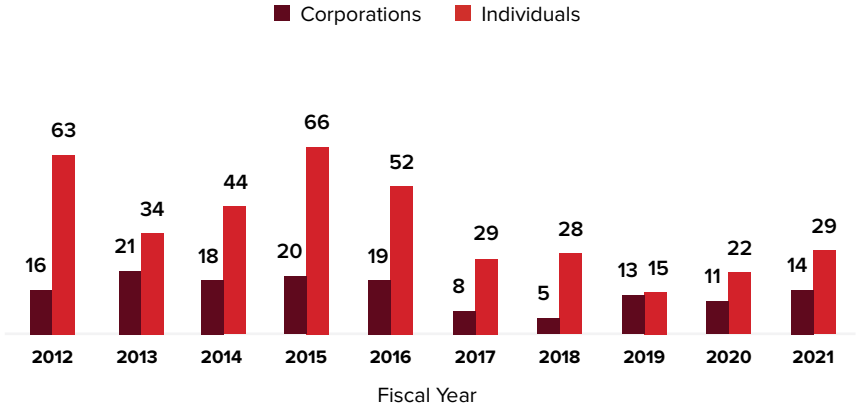
Total Criminal Cases Filed



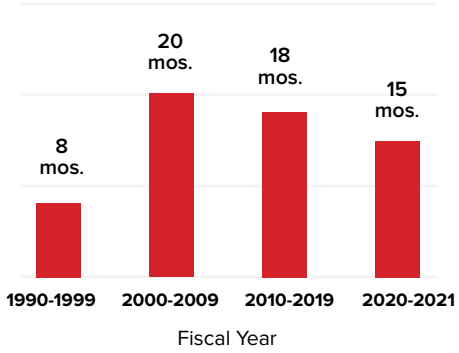
Total Criminal Fines & Penalties



Corporations & Individuals Charged



Average Prison Sentence in Months



Noteworthy Antitrust Actions:

The COVID-19 pandemic prompted a major federal inquiry into noteworthy U.S. companies, including Walmart, Amazon and Procter & Gamble (among others) over supply chain disruptions that threatened to thwart economic recovery. On November 29, 2021, by a vote of 4-0, the U.S. Federal Trade Commission ("FTC") issued an order to the companies utilizing its authority under Section 6(b) of the Federal Trade Commission Act ("FTC Act") to obtain all "information regarding supply chain disruptions affecting [their] business in consumer goods, including food." The 6(b) report is part and parcel of the FTC's broader inquiry into whether such supply chain disruptions have led to anticompetitive conduct and higher prices in the market for consumer goods.

Big Tech also continued to be a prime target for federal regulators in 2021, with an amended complaint brought by the FTC against Facebook in August 2021 over allegations that the social media giant sought to systematically "stymie emerging mobile threats" through acquisitions of popular social media platforms like WhatsApp and Instagram. To "buttress its acquisition strategy," the FTC further alleged that Facebook implemented and enforced a series of anti-competitive conditional dealing policies that effectively "pulled the rug out from under firms perceived as competitive threats." For instance, the FTC contended that while Facebook originally granted open access to developers to its critical application programming interfaces ("APIs"), it quickly discontinued that practice and transformed its API policies into an anticompetitive weapon—developers could only use Facebook's platform if they agreed not to compete with its core services or facilitate the growth of potential Facebook rivals. While the action remains unresolved—Facebook sought to dismiss the FTC's amended complaint in a November 17, 2021 filing—federal scrutiny of tech giants like Facebook is likely to continue unimpeded. In particular, the DOJ is widely expected to bring a second action against Google over its advertising practices. Google—a target of the DOJ's antitrust ire during the Trump Administration over the dominance of its web search capabilities—is also the subject of an ongoing federal probe targeting its ad-buying and ad-publishing operations.

2021 Laws:

While no new antitrust statutes were enacted by the Congress or signed by the President in 2021, a slew of new antitrust proposals were introduced in both the House and Senate that seek to modernize federal antitrust laws, which were largely enacted—and last updated—in the wake of the Industrial Revolution.

Chief among these bills is the Competition and Antitrust Law Enforcement Act of 2021 ("Klobuchar Bill") introduced by Senator Amy Klobuchar (D-MN) in February 2021. Among other things, the Klobuchar Bill would amend Section 7 of the Clayton Act to shift the burden from the government to merging parties to prove that certain mergers would not create an appreciable risk of materially lessening competition or tend to create a monopoly or monopsony. Significantly, the Klobuchar Bill would also substantially modify the standard used to assess whether potential mergers pose a monopolistic risk generally by substituting the new 'creating an appreciable risk of materially lessening competition' standard for the Clayton Act's current 'substantially lessen competition' standard.

Several key pieces of antitrust legislation also originated in the House, including but not limited to the Ending Platform Monopolies Act and the Merger Filing Fee Modernization Act. Under the former bill, technology platforms with at least 50,000,000 monthly active U.S. users and market capitalization of over $600 billion would be barred from selling products or services they own and control. The latter bill dramatically increases the fees associated with Hart-Scott-Rodino ("HSR") Act filings for the largest mergers. Parallel legislation to the Ending Platform Monopolies Act—the American Innovation and Choice Online Act—was also introduced in the Senate in October 2021. Under that proposal, specific forms of conduct that are detrimental to small businesses, entrepreneurs and consumers would be prohibited. These practices include (1) preventing another business's product or services from interoperating with the dominant platform; (2) requiring a business to buy a dominant platform's goods or services in exchange for preferred placement on the platform; (3) misusing a business's data to compete against it; and (4) rigging search results in favor of the dominant firm.

As of the date of this publication, however, none of the legislative proposals mentioned in this update have been subjected to a floor vote.

FTC/DOJ Challenges to Proposed Mergers:

In November 2021, the DOJ filed an antitrust lawsuit to prevent the acquisition of Imperial Sugar Company by its rival United States Sugar Corporation. In a complaint filed in the United States District Court for the District of Delaware, the DOJ alleged that the transaction would leave an overwhelming majority of refined sugar product—an estimated 75% of such product overall—in the hands of only two domestic producers. As a consequence, the DOJ contended that the price for refined sugar—an essential ingredient in many food products—would rise precipitously.

In the same month, the DOJ also sued to block the acquisition of Simon & Schuster by publishing giant Penguin Random House. In a suit filed in the United States District Court for the District of Columbia on November 2, 2021, the DOJ contended that as the world's largest book publisher, Penguin Random House's acquisition of Simon & Schuster would cause the former to control close to half of the market for the acquisition of publishing rights to "anticipated top-selling books" leaving authors with significantly less influence in negotiations and consumers with less choices on the shelves.

The most noteworthy action in 2021 by the FTC involved blocking the proposed acquisition of semiconductor chip design provider Arm Ltd. by U.S. chip supplier Nvidia Corporation—a $40 billion deal overall. In early December 2021, the FTC sued to block the acquisition of the United Kingdom-based chip designer, contending that such a vertical acquisition would stifle the "innovation pipeline for next-generation technologies." Arm Ltd.'s technology—comprised of microprocessor designs and architectures—is a critical input for Nvidia's line of computer chips that power a wide range of modern electronic devices, including but not limited to, smartphones and complex computer systems. If permitted, the FTC contends that the merger would be "felt throughout the computing industry" and significantly impair the development of markets for products used in datacenters, including networking and central processing.

2022 and Beyond:

The Biden Administration has plainly stated that vigorous and concerted enforcement of existing antitrust laws is a key priority of federal agencies with relevant jurisdiction over the enforcement of the Sherman and Clayton Acts. This was underscored by the issuance of Executive Order 14036 on July 9, 2021, which among other things, directed federal agencies to adopt a "whole-government approach" to promoting competition in domestic marketplaces. Importantly, the Executive Order directed the DOJ and FTC to consider whether to revise their joint 2016 Antitrust Guidance for Human Resource Professionals. The Executive Order also encouraged the FTC to exercise its rulemaking authority to "curtail the unfair use of non-compete clauses and other clauses and agreements that may unfairly limit work mobility." More broadly, Executive Order 14036 urged the FTC to address what the President described as "persistent and recurrent practices that inhibit competition"—including, but limited to, unfair data collection practices that damage competition, consumer privacy and autonomy; anticompetitive restrictions on third-party repair or self-repair of items commonly found in the agricultural sector; agreements in the prescription drug industry to delay the market entry of generic drugs; unfair competition in Internet marketplaces; anticompetitive occupational licensing restrictions; and tying and exclusionary practices in the brokerage or listing of real estate.

Biden's nomination and the Senate's confirmation of key antitrust proponents to the FTC and DOJ—namely, Lina M. Khan as chair of the FTC and Jonathan Kanter as the head of the DOJ's Antitrust Division—are critical indicators that robust enforcement of antitrust laws (including the expansion of their applicability to areas once considered off-limits for antitrust regulators) is likely to continue in earnest.

FCPA In 2021 and Beyond

As noted previously, FCPA recoveries in 2021 were substantially less in monetary terms than the previous year, which saw major settlements with Airbus SE and Novartis AG worth hundreds of millions of dollars. In contrast, total FCPA actions involving the SEC and DOJ were de minimis.

The most significant FCPA recoveries in 2021 involved Deutsche Bank (as previously mentioned), Amec Foster Wheeler Ltd., and WPP plc. While the Deutsche Bank settlement was by far the largest, the SEC's resolution of FCPA violations with Amec Foster Wheeler Ltd.—a U.S.-based company that provides project, engineering and technical services to energy and industrial markets on an international basis—in June 2021 was a close second at $22.7 million. In that case, Amec Foster Wheeler Ltd.'s UK subsidiary, Foster Wheeler Energy Limited, made improper payments totaling approximately $1.1 million to Brazilian officials in connection with efforts to win a contract for oil and gas engineering and design on the so-called UFN-IV Project. These bribes were paid largely through third-party intermediaries, one of whom conspicuously failed Foster Wheeler's own due diligence process and posed an elevated risk of corruption to the company from a bribery perspective. Foster Wheeler consented to the SEC's cease-and-desist order finding that it violated the antibribery, books and records, and internal accounting controls provisions of the FCPA. Under the same agreement, Foster Wheeler agreed to pay $22.7 million in disgorgement and prejudgment interest. Separately, Foster Wheeler entered into a three-year DPA with the DOJ under which it acknowledged responsibility for criminal conduct related to the findings in the SEC order.

In September 2021, the SEC also initiated and settled an action with WPP plc—the world's largest advertising group—over allegations that poor internal controls and lack of oversight of its foreign subsidiaries led to bribery and graft schemes in India, China, Brazil, and Peru whereby WPP plc illegally secured lucrative government contracts, curried favor with governmental officials over tax audits, and solidified its political support by making improper payments to the campaign of a foreign official disguised as legitimate business expenses. In addition to its agreement to cease and desist from any further violations of the FCPA, WPP agreed to pay disgorgement, prejudgment interest, and civil monetary penalties in the amounts of $10,114,424.86, $1,110,234.68, and $8,000,000 respectively, for a total recovery by the SEC of $19,224,659.54. The relatively favorable treatment of WPP plc was the direct result of its cooperation with the SEC. As noted in the cease-and-desist order, WPP undertook extensive remediation efforts, including the termination of senior executives and rank-and-file employees involved in the misconduct, strengthening its global compliance, internal investigations, and risk and control functions, and enhancing the procedures for the engagement of third parties, among other things.

As in 2020, corporate monitors were used extremely sparingly with respect to companies that violated the FCPA, in spite of particularly egregious errors made by WPP plc in failing to ensure that its corporate governance and compliance functions were integrated across its various foreign subsidiaries.

2022 and Beyond:

Data consistently shows that enforcement of the FCPA is fairly constant regardless of which party controls the White House. While FCPA enforcement action in 2021 seemed to be negligible, we largely attribute this result to the transition to a new Presidential Administration and significant delays in filling key positions caused by political intrigue in the Senate. Furthermore, the lack of publicly announced FCPA settlements this year is not a reliable indicator of whether the DOJ and/or SEC are pursuing other, more extensive investigations involving sophisticated bribery schemes. As enforcement recent enforcement trends demonstrate, the outright bribery of foreign government officials by individuals on behalf of an organization is an increasingly rare occurrence. Instead, organizations intent on violating the antibribery proscriptions of the FCPA are doing so circuitously—relying increasingly on intermediaries and other third parties with little or no connections to the organization itself to do their proverbial dirty work. The reliance on such third parties by these organizations makes it more difficult for U.S. and foreign regulators to track the ultimate source of improper payments or gifts back to the principal actor. Given this phenomenon, it is entirely possible that enforcement efforts have been thwarted to a certain degree by the ongoing pandemic and inability of government officials to conduct robust onsite investigations. In short, we anticipate that as 2022 progresses, the public announcement of FCPA enforcement actions involving longstanding investigations will increase.

False Claims Act In 2021 and Beyond

As of the date of this report, no official statistics for FY 2021 have been published by the DOJ with respect to False Claims Act recoveries. As such, we attempt to highlight the most significant enforcement developments and priorities in the context of the False Claims Act.

What Happened At DOJ and Other Agencies In FY 2021 Related to the FCA:

In June 2021, the U.S. Department of Health and Human Services (“HHS”) opened a reporting channel for recipients of Provider Relief Fund Payments made to healthcare providers under the auspices of the 2020 CARES Act. Among other things, recipients of Provider Relief Fund Payments are required to explain how the payments were utilized. As a predicate to receiving such funds, healthcare providers made various representations to the government—including a commitment to utilize the funds for the purposes of preventing, preparing for, or responding to the coronavirus pandemic. Guidance issued by HHS concerning permissible use of CARES Act funds during the pandemic has been notoriously confusing and inconsistent. As a consequence, it is highly likely that healthcare institutions will be exposed to FCA liability for perceived mismanagement of Provider Relief Fund payments.

In September 2021, the DOJ intervened in a high-profile lawsuit against Independent Health Association, Independent Health Corporation ("Independent Health"), DxID LLC, and the former Chief Executive Officer of DxID over allegations that the parties defrauded the government and violated the FCA by submitting inaccurate information concerning the health status of beneficiaries enrolled in Medicare Advantage plans to increase reimbursements. Specifically, DOJ contends that DxID—a wholly owned subsidiary of Independent Health Corporation—asked healthcare providers to sign addenda forms up to a year after medical visits by covered beneficiaries to add diagnoses that were not initially documented. DxID allegedly benefitted from this illegal arrangement by collecting a contingency fee of up to 20% of any additional recovery it received from Medicare Advantage plans.

Finally, in December 2021, the DOJ raised the per claim penalties under the FCA to $11,803 to $23,607 per violation occurring after November 2, 2015. According to an official notice published in the Federal Register, the adjustment in per claim penalties reflects current inflationary pressures, with a factor of 1.01182—a marginal increase overall from 2020's inflation factor of 1.01764.

2022 and Beyond:

In FY 2021, the U.S. government spent a total of $6.82 trillion, an increase of $270 billion over FY 2020. A staggering $3.46 trillion has been spent by the federal government since the beginning of the COVID-19 pandemic to help healthcare providers, employers, individuals and institutions grapple with COVID's devastating economic effects. This unprecedented level of public spending in a time of a global health crisis automatically lends itself to the potential for fraud, abuse, and misuse of trillions of dollars in federal funds designated for a specific purpose. As such, there is little doubt that we will witness a significant uptick in related FCA audits, investigations, enforcement actions, qui tam lawsuits, and settlements and judgments over the next several years.

As articulated by Acting Assistant Attorney General Brian M. Boynton earlier this year at the previously mentioned Federal Bar Association Qui Tam Conference, other priorities of the DOJ in the FCA space include a focus on the marketing and sale of opioids; fraud targeting senior citizens; inducements paid to healthcare providers to convert to electronic health records systems; fraud in the delivery of telehealth services; and malfeasance in delivering cybersecurity services to the government.

On the legislative front, we also expect to see efforts by Senator Chuck Grassley (R-IA) and others to amend the FCA in the wake of the Supreme Court's decision in *United Health Services v. United States ex rel. Escobar*, 136 S.Ct. 1989 (2016) gain considerable traction. Under current law, a defendant can avoid liability under the FCA for defrauding the federal government by contending that her fraud was not material simply because the government continued payment. Under the Grassley proposal, the burden of proof in FCA cases would be modified to allow the government or a relator to establish materiality by mere preponderance of the evidence. A defendant may rebut an argument of materiality by clear and convincing evidence.

The Agencies: SEC

First, The Statistics:

Despite the ongoing COVID-19 pandemic, the SEC showed no signs of relenting in its core mission of protecting investors from unscrupulous actors and domestic markets from manipulation.

For FY 2021, the SEC again aggressively collected money from violators through enforcement efforts (nearly $3.8 billion) including $2.4 billion in disgorgement and more than $1.4 billion in penalties. In all, in FY 2021, the SEC:

1. Filed a total of 697 enforcement actions, comprising 434 new actions and 120 actions against issuers who were delinquent in making required filings with the SEC—a three-percent decrease overall from FY 2020;

2. Initiated new enforcement actions in emerging areas, including but not limited to securities using decentralized finance ("DeFi") technology and securities laws violations on the "dark web";

3. Charged entities and individuals with unregistered and/or fraudulent offerings of digital or "crypto" currency, including Ripple Labs and two of its executives (alleging a $1.3 billion unregistered offering);

4. Aggressively pursued improper conduct by investment professionals, including an action against a UK-investment advisor BlueCrest Capital Management for inadequate disclosures, misstatements, and omissions concerning its transfer of top traders to another fund, with nearly $170 million being returned to investor victims—a substantial percentage of the $521 million the SEC returned to aggrieved investors overall in FY 2021;

5. Pursued insider trading charges against a multitude of individuals, including a former biopharmaceutical company employee who traded on material non-public information that his company would be acquired by Pfizer Inc., and an insider trading ring that generated more than $3 million in profits by trading on proprietary information concerning Netflix's subscriber growth;

6 Held individual executives affiliated with prominent companies—including the former CEO and Chairman of Wells Fargo and the founder, former CEO, and former executive chairman of Nikola Corporation—accountable for fraudulent conduct and making misleading statements both to the public and in connection with securities filings;

7 Brought charges against The Cheesecake Factory for making misleading disclosures about the impact of the COVID-19 pandemic on its business operations and financial condition;

8 Awarded $114 million and $110 million—the largest individual awards in SEC Whistleblower Program history—to two individuals whose information, assistance, and independent analysis led to the successful enforcement/advancement of unrelated SEC actions;

9 Rewarded cooperation and remediation efforts by defendants (in one case, imposing a modest penalty of $88,248 against Gulfport Energy Corporation and its CEO Michael G. Moore for violations of certain executive disclosure rules); and

10 Acted swiftly to protect market integrity—bringing charges against Morningstar Credit Ratings for internal controls violations in the rating of commercial mortgage-backed securities and UBS and other investment advisers for violations of securities laws detected by the emerging use of trading data analytics.

A Few Noteworthy Events:

In addition to expanding its regulatory reach to the Dark Web, DeFi, and digital currency, the SEC took action in conventional contexts as well to protect the interests of investors from unscrupulous market actors. Among these actions:

1 The SEC settled an action against General Electric ("GE") for disclosure failures in its power and insurance businesses. In 2017 and 2018, GE's stock price declined by nearly 75% as "challenges in its power and insurance businesses were disclosed to the public." According to the SEC's order, GE misled investors in describing its GE Power profits by omitting the critical fact that one-quarter

of its profits in 2016—and nearly half of its profits in the first three quarters of 2016—stemmed from reductions in prior cost estimates. The SEC also found that GE failed to inform investors that its reported increase in current industrial cash collections came at the expense of cash in future years and was generated primarily through internal receivable sales between GE Power and GE Capital. Citing the fact that investors were entitled to accurate information concerning a company's material operating results, the SEC found that GE flagrantly violated the antifraud, reporting, disclosure controls, and accounting controls provisions of applicable securities laws. As a consequence, GE agreed to pay a $200 million penalty to settle the disclosure charges.

2

The SEC settled charges against The Kraft Heinz Company (“”Kraft”) and two former executives for engaging in an expense management scheme that resulted in the restatement of several years of financial reports. According to the SEC's order, from the last quarter of 2015 to the end of 2018, Kraft engaged in various types of accounting misconduct including recognizing unearned discounts from suppliers and “maintaining false and misleading supplier contracts, which improperly reduced the cost of goods sold” and resulted in fraudulent “cost savings.” Kraft's then-Chief Procurement Officer Klaus Hoffmann approved these contracts and certified the accuracy and completeness of his division's financial statements with full knowledge that the misconduct was occurring. Kraft touted its “savings” to the market and artificially inflated its EBITDA numbers—a key metric for discerning investors. Kraft subsequently restated its financial statements on Form 10-K, which included financial data reported for FY 2015, as well as the financial statements contained in Forms 10-Q and 10-K for FYs 2016 and 2017, and the first three quarters of FY 2018. The SEC also found that Kraft's then-Chief Operating Officer—Eduardo Pelleissone—received several “warning signs indicating that expenses were being managed through manipulating supplier agreements.” Despite these warnings, Pelleissone approved Kraft's financial statements, which he should have known were materially false and misleading. Without admitting or denying the SEC's findings, Kraft consented to the entry of a cease-and-desist order under which it agreed to refrain from future violations of securities laws and pay a civil penalty of $62 million. Pelleissone agreed to pay disgorgement and prejudgment interest of $14,211.31 and a civil penalty of $300,000. Under a separate agreement in federal court, Hofmann consented to entry of judgment permanently enjoining him from future violations, ordering him to pay a civil penalty of $100,000, and barring him from serving as an officer or director of a public company for a period of five years.

3

The SEC also settled a significant action involving TIAA subsidiary TC Services. The $97 million in restitution to investors is the result of an SEC investigation and cease-and-desist order that found TC Services willfully violated certain provisions of both the Securities Act and Investment Advisers Act when it failed to disclose the full nature and extent of conflicts of interest that encouraged its Wealth Management Advisers ("WMAs") to advise clients to roll over their retirement assets into a product ("Portfolio Advisor") that was not tailored to a client's individual investment needs—in spite of representations by WMAs that their advice was "objective" and "non-commissioned." To the contrary, the SEC found that TC Services and its WMAs stood to financially benefit from the arrangement, which generated asset-based advisory fees ranging from .40% to 1.15% annually. TC Services incentivized this behavior by encouraging its WMAs in training materials to utilize a prospective client's "pain points" to pressure them into a managed investment solution as the best alternative.

Holding Individuals Accountable:

In 2021, the SEC continued to prioritize individual liability and accountability for violations of federal securities laws. For example, the SEC brought actions against:

1

Special purpose acquisition company ("SPAC") Stable Road Acquisition Company, its sponsor SRC-NI, CEO Brian Kabot, its proposed merger target Momentus, Inc., and Momentus founder and CEO Mikhail Kokorich. According to the SEC's order, Momentus—an early-stage space transportation company—repeatedly lied to investors about the state of its propulsion technology by claiming that it had been "successfully tested" in space. In reality, Momentus' only in-space test had failed to achieve its primary mission of demonstrating the technology's commercial viability. The SEC further found that Stable Road and its CEO Brian Kabot repeated Momentus's false claims and failed to conduct appropriate due diligence to satisfy its obligations to investors. As a result, Stable Road filed inaccurate registration statements and proxy solicitations with the SEC. In a settlement reached with Momentus, Stable Road, SRC-NI, and Kabot individually, the SEC imposed monetary penalties totaling nearly $8.04 million and a requirement that Momentus and Stable Road provide private investors with the right to terminate their subscription agreements prior to the shareholder vote to approve the so-called reverse merger. Separate litigation involving Kokorich was initiated by the SEC in federal District Court alleging that he violated the antifraud provisions of U.S. securities laws and aided and abetted Momentus's violations of the same provisions.

2

Wells Fargo Bank CEO and Chairman John G. Stumpf and the former head of Wells Fargo Community Bank Carrie l. Tolstedt for misleading investors about the success of Wells Fargo Community Bank, its core business operation. According to the SEC's complaint against Tolstedt filed in federal District Court, Tolstedt participated in touting Wells Fargo Community Bank's "cross-sell metric" by which it repeatedly reported on the successful sale of other Wells Fargo products to existing retail customers who reputedly "needed, wanted, and used" the Bank's other services. Contrary to these representations, Wells Fargo Community Bank opened millions of accounts or sold products that were unauthorized or fraudulent, and others that were not needed or simply unwanted by retail banking customers. The unused accounts and products were a critical factor in Wells Fargo Community Bank's reported cross-sell metric for many years. Despite knowing that the cross-sell metric was based on rampant sales misconduct, Tolstedt repeatedly provided misleading subcertifications as to the accuracy of Wells Fargo Community Bank's quarterly and annual reports to shareholders.

Separately, the SEC initiated and settled a related action against Wells Fargo Bank CEO and Chairman John Stumpf for his unreasonable reliance on Wells Fargo Community Bank's assurances that minimized the scope of the sales practices problem that precipitated the SEC's investigation. In turn, Stumpf authorized and participated in the filing of misleading SEC reports—including quarterly and annual filings (Form 10-Qs and 10-Ks respectively)—that touted the success of Wells Fargo Community Bank's "cross-sell" initiative under the false pretense that such products were needed, wanted and indeed even valued by its retail customers. As a consequence of his oversight failure and approval of inaccurate and misleading reports that were ultimately filed with the SEC, Stumpf was personally ordered to pay a civil monetary penalty in the amount of $2.5 million, and to cease from committing or causing any additional violations of Sections 17(a)(2) and (3) of the Securities Act.

3

The former CEO and CFO of employee benefits administration company WageWorks, Inc. for making false and misleading statements that resulted in improper recognition of revenue related to a contract with a large public-sector client. Under an action and settlement reached with the SEC, WageWorks's CEO—Joseph Jackson—and its CFO—Colm Callan—admitted that they improperly pressured the company's internal accounting team to recognize $3.6 million in revenue resulting from certain disputed development and transition work with the public sector client. As a consequence, the SEC's order found that WageWorks's former executives violated Sections 17(a)(2) and (3) of the Securities Act and misled the company's own auditors when they knowingly

submitted inaccurate financial reports for FY 2016. Despite restating its financial statements in 2019 to account for the erroneous entry, the SEC found that Jackson and Callan failed to share important information about WageWorks's ability to collect a significant receivable. As a consequence of their actions, the SEC imposed a monetary penalty of $75,000 against Jackson and a $100,000 penalty against Callan. Jackson further agreed to reimburse WageWorks for $1,929,740—representing the incentive-based compensation he received from the sale of WageWorks's stock—while Callan agreed to reimburse WageWorks to the tune of $157,000.

Other Enforcement Actions and Settlements:

The single largest resolution reached by the SEC for FY 2021 involved financial powerhouse Goldman Sachs, for violations of the FCPA in connection with the 1Malaysia Development Berhad ("1MDB") scheme. According to the SEC's order, beginning in 2012, senior employees formerly affiliated with Goldman Sachs enlisted a third-party intermediary to bribe high-ranking government officials in Malaysia and Dubai to obtain significant business from 1MDB—a Malaysian-owned government investment fund. The SEC estimates that Goldman Sachs utilized the intermediary to obtain $6.5 billion in bond offerings. Goldman Sachs was ordered to pay over $1 billion in disgorgement and civil monetary penalties. The resolution of the principal case against Goldman Sachs itself follows the SEC's 2019 decision to charge former Goldman Sachs Group Inc. managing director Tim Leissner individually for his complicity in the 1MDB scheme, which resulted in personal disgorgement of $43.7 million.

An enforcement action brought by the SEC against telecommunications giant AT&T and three of its executives also gained considerable media attention. In March 2021, the SEC sued AT&T for selective disclosure of nonpublic material information to a handful of analysts in direct violation of Regulation FD. According to the SEC's complaint filed in federal District Court, AT&T learned in March 2016 that a steeper-than-expected decline in its first quarter smartphone sales would cause its revenue to fall short of analysts' expectations for the quarter. Thereafter, three of AT&T's senior investor relations executives—Christopher Womack, Michael Black, and Kent Evans—made private one-on-one phone calls to analysts at approximately twenty different firms to disclose internal sales data and the impact of that data of internal revenue metrics despite the fact that this type of non-public material was subject to limitations on selective disclosure. While the case has yet to be resolved, the SEC's complaint seeks to permanently enjoin AT&T and its three investor relations executives from future violations of selective disclosure prohibitions and impose civil monetary penalties on all of the defendants pursuant to Section 21(d)(3) of the Exchange Act.

2022 and Beyond:

2021 represented the SEC's formal entrée into the emerging arenas of cryptocurrency, DeFi, and the Dark Web—long considered implausible for the SEC given its current fiscal constraints and lack of technological savvy. The SEC proved the critics wrong by not only embarking on significant investigations in these areas, but also continuing to utilize sophisticated analytics to detect fraud in suspected trades under the aegis of its much-touted Earnings Per Share ("EPS") Initiative.

If recent comments by the Acting Director of the SEC's Division of Examination are any indication, the SEC will continue to embark into unchartered territory unimpeded, including the market for investment products with environmental, social and governance ("ESG") goals. Rapid growth in demand for investment products with ESG foci present a real risk for investors given a lack of consensus about its real meaning and the nature of both institutional and investor objectives. Compliance professionals should also expect the Examination Division to conduct more through audits of registered investment advisers to private funds that focus on the liquidity and disclosure of financial risks, as well as potential conflicts of interest. Finally, the Enforcement Division anticipates active coordination with financial services firms to identify and proactively address issues related to endpoint security, data loss, remote access, use of third-party communications systems, and vendor management. Although much of the activity of the Examination Division in FY 2021 has been concentrated on the repercussions of moves away from LIBOR, registrants should expect the Division to be more active in FY 2022 in other areas as well.

Proposed rulemaking in FY 2022 is also anticipated to accelerate, as the SEC outlined in a June 11, 2021 press release forthrightly providing the public with its regulatory agenda. In particular, the SEC has and will continue to focus on creating disclosure rules related to climate risk, human capital, workplace diversity, and cybersecurity risk; market structure modernization within equity, treasury and fixed-income markets; transparency involving stock buybacks, short sale disclosures, securities-based swap ownership, and the stock loan market; enhancing shareholder participation; and regulating special purpose acquisition companies ("SPACs").

The Agencies: DOJ

Because the DOJ is our primary federal law enforcement agency and is empowered to handle all criminal prosecutions and civil suits in which the United States has an interest, this white paper could not possibly cover every development at that agency. Below are a few notable events not fully covered in other sections of this paper.

New Leadership:

With Attorney General Merrick Garland and Deputy Attorney General Lisa Monaco at the helm of the DOJ, the somewhat fragmented and inconsistent nature of the Trump Administration's enforcement of the law was replaced by an emphasis on professionalizing the Department overall and reinvigorating many initiatives that were perceived as being relegated to the periphery during Trump's tenure as President. Although decisive action was considerably delayed as the Senate postponed consideration of both nominations, Garland and Monaco seemed poised by the end of FY 2021 to implement an aggressive reform agenda.

On October 28, 2021, Monaco delivered remarks to the American Bar Association's ("ABAs") 36th National Institute on White Collar Crime. In that speech, Monaco highlighted the DOJ's efforts to "strengthen the way [the Department] respond[s] to corporate crime." Although emphasizing that any changes to the DOJ's priorities were a matter of "degree and not of kind," Monaco announced that the DOJ would increasingly seek to hold individuals accountable for their actions—not just the institutions those individuals represent. As Monaco plainly stated, "[a]ccountability starts with the individuals responsible for criminal conduct." To that end, Monaco directed the DOJ to restore prior guidance making it clear that to be eligible for cooperation credit, companies implicated in potential criminal activity must furnish the DOJ with all non-privileged information about the individuals involved or responsible for the misconduct at issue—regardless of position, status or seniority. Because even the most peripheral actors in underlying misconduct can be valuable sources of information to the DOJ, artificial determinations by company counsel that an individual was not "substantially involved" in the misconduct are no longer sufficient. In short, the DOJ now expects companies to come completely clean.

Monaco's ABA speech also put companies on notice that all prior misconduct would be considered when determining what an appropriate resolution constitutes for organizations implicated in criminal activity. Previously, the DOJ's own prosecutorial guidance—the Principles of Federal Prosecution of Business Organizations—artificially constrained a prosecutor's ability to consider misconduct dissimilar to the criminal activity at issue. Monaco emphasized that prosecutors will now be required to consider the full criminal, civil and regulatory records of any company when deciding what resolution is appropriate for a company facing a criminal investigation.

Finally, Monaco's October 2021 remarks emphasized that, to the extent the appointment of corporate monitors was previously disfavored, that policy would be rescinded under the Biden Administration. As we noted in last year's comprehensive enforcement recap, the use of corporate monitors had stagnated in recent years, with organizations having essentially free reign over their own remediation efforts, with minimal oversight or follow up by federal prosecutors. That era seems to have ended abruptly. In addition to granting prosecutors the full discretion to determine whether a corporate monitorship is appropriate, the DOJ will now zealously pursue companies that violate the provisions of both Non-Prosecution Agreements ("NPAs") and Deferred Prosecution Agreements ("DPAs"). Too often viewed as a proverbial 'get out of jail free pass,' Monaco was clear that significant resources would be devoted to implementing a zero-tolerance policy for companies that violate the terms of NPAs and DPAs.

Focus On Corporate Crime:

DOJ seemingly made good on Deputy Attorney General Lisa Monaco's renewed commitment to individual and institutional accountability in the same month as her speech to the ABA, by filing and settling an action against Credit Suisse Group AG—a global financial institution with headquarters in Switzerland and various subsidiaries in Europe (including the United Kingdom). According to a criminal information filed against Credit Suisse in the United States District Court for the Eastern District of New York, between 2013 and March 2017, Credit Suisse, through its subsidiary Credit Suisse Securities (Europe) Ltd. ("CSSEL") used U.S. wires and the U.S. financial system to defraud investors in securities related to a Mozambican state-owned entity, Empresa Moçambicana de Atum, S.A. ("EMATUM"), which Mozambique founded to develop a state-owned tuna fishing project. Credit Suisse made numerous materially false representations and omissions relating to the use of loan proceeds, kickback payments made to CSSEL bankers, and the existence of other debt owned by Mozambique to Credit Suisse. Significantly, Credit Suisse affirmatively represented to investors that all loan proceeds would be used for the tuna fishing project. In fact, these loan proceeds were diverted for unlawful purposes—including $50 million in kickbacks paid to CSSEL bankers themselves and $150 million in bribes paid to Mozambiquan

state officials. More egregiously, Credit Suisse admitted that "prior to and during the EMATUM financing," it identified significant red flags concerning the potential for bribery and corruption in connection with the contractor that supplied boats and equipment for EMATUM but decided to continue with the transaction anyway.

Under the terms of a DPA reached with the DOJ, Credit Suisse agreed to the imposition of a $247 million criminal penalty, with approximately $175 million being paid to the United States Treasury. As part of the same DPA, Credit Suisse agreed to an event study to calculate the proximate fraud loss for the victims of its criminal conduct, and ultimately, the amount of restitution Credit Suisse will pay to those victims. Parallel settlements were reached by Credit Suisse with the SEC as well as the UK's Financial Conduct Authority ("FCA").

The Agencies: CFTC

The Commodity Futures Trading Commission's ("CFTC") Division of Enforcement aims to protect the public and preserve market integrity by detecting, investigating, and prosecuting violations of the Commodity Exchange Act ("CEA") and the Commission's own regulations. As of the date of this report, although no statistics were immediately available from CFTC for the previous fiscal year, several notable actions were initiated by the Enforcement Division as follows:

1

In March 2021, the CFTC obtained a judgment against Benjamin Reynolds (a UK national), in the sizeable sum of **$571 million** for operating an illicit Bitcoin trading scheme. According to court filings, between May 2017 and October 2017, Reynolds used a public website and various social media accounts to solicit at least 22,190.542 in Bitcoin, valued at approximately $143 million from more than 1,000 customers worldwide including 169 individuals in the United States. Reynolds falsely represented to customers that his business—Control-Finance Limited, a United Kingdom based entity—was trading their Bitcoin deposits in virtual currency markets and generating "guaranteed" trading profits for all customers. According to the CFTC, Reynolds in fact, made no such trades and earned no profits on his customers' behalf, but rather converted the funds for his own personal use. As a consequence, the victims of Reynolds's fraud lost most, if not all, of their Bitcoin deposits. Under a final judgment entered by the United States District Court for the Southern District of New York, Reynolds was ordered to pay a civil monetary penalty of $429,000,000 and restitution of $142,986,589 to his victims. Reynolds was also permanently restrained, enjoined, and prohibited from directly or indirectly, with respect to the sale of any commodity in interstate commerce, using or employing any artifice to defraud; making or attempting to make any misleading statement of material fact or omitting to state a material fact; and engaging or attempting to engage in any act, practice, or course of business which would operate as fraud or deceit upon any person.

2

In April 2021, the CFTC successfully sued David Gilbert Saffron, an Australian citizen residing in Nevada and Los Angeles, and his company Circle Society, Corp., a Nevada organized and operated legal entity, for cryptocurrency fraud and misappropriation. In a consolidated complaint filed against both Saffron and Circle Society, the CFTC successfully alleged that from December 2017, Saffron fraudulently solicited and accepted at least $15,815,967 worth of Bitcoin and U.S. dollars from at least 179 individuals to trade off-exchange binary options on foreign currencies and cryptocurrency pairs. Saffron created and used Circle Society to perpetrate his fraud and induced the general public to invest in his scheme, by making false claims of its trading expertise and guaranteeing outrageous rates of return of up to three hundred percent. The CFTC determined that rather than using the funds as intended, Saffron misappropriated the funds by maintaining them in his own personal cryptocurrency wallet and using some of the funds to pay participants with the funds of others in the manner of a Ponzi scheme. Despite repeated demands, the majority of participants have been unable to obtain a return of their funds from Saffron or Circle Society, Corp. The District Court's final judgment calls for Saffron and Circle Society—jointly and severally—to pay restitution of $14,831,280 to all defrauded pool participants, disgorgement of $15,815,967, and a civil monetary penalty of $1,484,128—a total of approximately $32 million.

3

In August 2021, the CFTC entered into a consent order with five companies—HDR Global Trading Limited, 100x Holding Limited, ABS Global Trading Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited—charged with operating the BitMEX cryptocurrency trading platform. Pursuant to the consent order, the BitMEX entities agreed that they violated the Commodity Exchange Act ("CEA") by operating as Futures Commission Merchants ("FCM") without CFTC registration by accepting bitcoin to margin digital asset derivative transactions and by acting as a counterparty to leveraged retail commodity transactions. In addition, according to the consent order, between approximately November 2014 and October 1, 2020, the BitMEX entities offered leveraged trading of cryptocurrency derivatives to retail and institutional customers in the United States and abroad through an online platform. Customers in the United States and elsewhere placed orders directly through BitMEX's online platform, with the BitMEX itself acting as a counterparty to certain transactions. As such, the BitMEX entities admitted to additional violations of the CEA by operating a facility to trade or process swaps without being approved as Designated Contract Markets ("DCM") or Swap Execution Facilities ("SEF"). Adding insult to injury, the BitMEX entities also wholly failed to implement appropriate Anti-Money Laundering ("AML") protocols and Know Your Customer ("KYC") procedures that would have enabled them to identify and bar customers based in the United States from accessing and utilizing the BitMEX trading platform. As a result

of the BitMEX entities' collective misconduct, the court ordered the payment of a $100 million civil monetary penalty with a $50 million offset for amounts paid by the entities to the Financial Crimes Enforcement Network ("FinCEN").

Looking Forward:

CFTC has increasingly devoted its resources and attention to enforcing the CEA and its implementing regulations in the emerging market for digital currency. Indeed, much of the CFTC's focus in the previous year has been related to pursuing unregistered—and at times entirely fraudulent—individuals and entities involved in the trading of digital commodities such as cryptocurrency and related swaps and derivatives. The sheer value of these digital assets—by some accounts, worth an estimated $3 trillion as a whole—makes it all but certain that the CFTC will continue to make enforcement in this area a top priority for 2022 and beyond.

OFAC Sanctions and Regulations

The United States Department of the Treasury's Office of Foreign Asset Control ("OFAC") is the agency statutorily responsible for the administration of comprehensive, selective, country and industry-specific trade sanctions imposed consistent with U.S. foreign policy. Among other things, OFAC administers sanctions targeting adversarial countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security and economic stability of the United States. In calendar year 2021, OFAC entered into a number of settlements with primarily institutional actors found to have violated multiple sanctions regulations. In total, OFAC brought twenty enforcement actions against domestic and foreign institutions found to have violated U.S. sanctions regulations and imposed $20,896,739.22 in monetary penalties. These actions included, but are not limited to:

1

A $1,385,901.40 settlement with Payoneer Inc., a publicly traded New York-based online money transmitter, for apparent violations of multiple sanctions programs. According to OFAC, Payoneer processed 2,201 payments for parties located in jurisdictions subject to comprehensive and selective sanctions, including the Crimea Region of the Ukraine, Iran, Sudan, Syria, and 19 payments on behalf of sanctioned persons on OFAC's List of Specially Designated Nationals and Blocked Persons ("SDN List"). Notably, OFAC found that Payoneer's gross sanctions program deficiencies—including the lack of protocols with respect to the screening, testing, auditing and review of transactions—enabled prohibited persons to engage in approximately $793,950.70 worth of transactions. In imposing a sizable monetary penalty on Payoneer, Inc., OFAC found that weak algorithms allowed names contained on the SDN List not to be

flagged by its own filter. Moreover, Payoneer failed to screen for Business Identifier Codes ("BICs") even when associated SDN List entries contained them. Finally, and perhaps most egregiously, Payoneer knowingly permitted flagged and pended payments to be released automatically without review during periods of significant backlog. Among other things, OFAC noted that the sheer scope of the misconduct at issue—spanning six different sanctions programs—justified the imposition of a sizable penalty.

2

An $8,572,500 settlement with French bank Union de Banques Arabes et Françaises ("UBAF") that facilitates trade finance between Europe, the Middle East, North African, and sub-Saharan Africa. Under a settlement agreement reached with OFAC in January 2021, UBAF admitted to operating U.S. dollar accounts on behalf of sanctioned Syrian financial institutions and indirectly conducting business through the U.S. financial system. While the majority of the apparent violations involved the processing of internal transfers on behalf of the sanctioned entities followed by corresponding funds transfers through a U.S. bank, additional transactions involved "back-to-back" letters of credit or other trade finance transactions—all of which were processed through a U.S. bank. In all, UBAF was found to violated U.S. sanctions regulations 127 times. Even so, OFAC determined that UBAF's violations were "non-egregious and voluntarily self-disclosed."

3

A $2,329,991 settlement with Bank of China (UK) Limited ("BOC UK") for violations of the now-defunct Sudan sanctions program, which prohibited the exportation, indirectly or directly, to the nation of Sudan of any goods, technology or services from the United States. OFAC found that between September 4, 2014 and February 24, 2016, BOC UK exported financial services from the United States by processing a total of 111 commercial transactions worth $40,599,184 through the U.S. financial system on behalf of parties in Sudan. Although OFAC found that BOC UK had "demonstrated a reckless disregard for U.S. sanctions requirements by processing transactions through the U.S. financial system for entities in Sudan despite having account and transaction information indicating [a] Sudanese connection," it also found that BOC UK had no prior sanctions history, self-reported to OFAC, and cooperated fully with its investigation into the Sudan sanctions violations. Importantly, BOC UK also committed to taking remedial measures, including conducting an annual enterprise-wide sanctions risk assessment by business line, centralizing customer due diligence firm-wide to strengthen internal controls, and enhancing policies and procedures to better address U.S. sanctions regulations.

Looking Ahead:

Increasingly, key policymakers are relying on the levers of U.S. sanctions programs to further foreign policy and national security objectives by targeting the assets of individuals and entities designated on OFAC's SDN list and aggressively pursuing reports of comprehensive and targeted sanctions violations. A noticeable uptick in sanctions activity across the federal government this year involved the People's Republic of China. In conjunction with the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), OFAC took decisive action against a number of entities and individuals identified as affiliated with China's civil-military fusion initiative, to prohibit U.S. persons generally from dealing with these foreign actors, including exporting more sensitive U.S.-origin technology to potential adversaries. 2022 is likely to see more aggressive efforts by the Biden Administration to deal with China—which now includes Hong Kong—as a viable threat to the national security and economic interests of the United States.

Anti-Money Laundering, Bank Secrecy Act, and Fraud Recovery Developments

First, A Few Notable Events:

The DOJ's Money Laundering and Asset Recovery Section ("MLARS") was active in 2021, with an emphasis on traditional areas of money laundering activity, the recovery of illegally obtained COVID-19 funds, and the return of misappropriated digital assets (cryptocurrency) to victims of fraud.

Among the more noteworthy actions resolved by MLARS in 2021 was with Swiss Bank Julius Baer & Co. Ltd. ("BJB"). According to documents filed in federal court, BJB admitted to conspiring to launder over $36 million in bribes through the United States to soccer officials associated with the Fédération Internationale de Football Association ("FIFA") and other international soccer organizations. These bribes were paid by various sports marketing companies in furtherance of a scheme to obtain exclusive broadcasting rights to soccer matches. Under a three-year DPA reached with the DOJ, BJB admitted to conspiring to commit money laundering and agreed to pay more than $79 million in penalties—including a fine of $43,320,000 and forfeiture of $36,368,400—to resolve the criminal information filed against it. The principal individuals associated with the scheme—namely, former BJB relationship manager Jorge Luis Arzuaga and Alejandro Burzaco, the controlling executive of a sports media and marketing company based in Argentina—pled guilty to various criminal charges including racketeering conspiracy in 2017 and 2015, respectively.

MLARS also aggressively pursued the return of illegally obtained COVID-19 funds. In December 2021, for instance, the DOJ announced that it had secured a conviction of a Texas woman for defrauding the Paycheck Protection Program ("PPP") to the tune of $1.9 million. According to documents filed in federal court and evidence presented at trial, Lola Shalewa Barba Kasali, the owner of two small businesses in Houston, falsely represented the number of her employees and related payroll expenses when she made multiple applications for PPP relief. In support of these applications, Kasali submitted falsified tax records and successfully obtained over $3.8 million in PPP proceeds. In concert with its law enforcement partners, the DOJ successfully obtained the forfeiture of the proceeds and Kasali was convicted of

two counts of making false statements to a financial institution and two counts of bank fraud. Kasali is scheduled to be sentenced in February 2022 and faces up to thirty years in prison on each count.

In the same month, MLARS—in conjunction with the U.S. Attorney's Office for the Southern District of California—initiated an action to return over $150 million in embezzled funds to Sony. According to a civil forfeiture complaint filed in federal court, an employee of Sony Life Insurance Ltd. in Japan—Rei Ishii—diverted $154 million to a personal account he controlled at a bank in La Jolla, California by falsifying transaction instructions when Sony attempted to transfer monies between its financial accounts. Ishii then converted the funds to cryptocurrency in the form of Bitcoin. Based on a seizure warrant authorized in June 2021, law enforcement was able to trace multiple Bitcoin transfers and identify that approximately 3,879.16 Bitcoins had been transferred to a specific Bitcoin address and subsequently stored in an offline cryptocurrency "cold wallet."

New DOJ Initiatives Announced:

In October 2021, the DOJ announced two new major departmental initiatives—namely, the Civil–Cyber Fraud Initiative and the National Cryptocurrency Initiative. Under the Civil-Cyber Fraud Initiative, the DOJ announced that it would concentrate resources into False Claims Act ("FCA") recovery from contractors that misrepresent the nature of cybersecurity services sold to the U.S. government. The National Cryptocurrency Initiative—in which MLARS will play the dominant role—will dedicate departmental resources to prosecuting cryptocurrency exchanges and other related entities (including so-called "mixing and tumbling services" that mix digital assets with other funds to prevent tracing) that permit the use of digital assets to facilitate criminal activity such as money laundering, illegal or unregistered money services, and "dark markets" for illegal drugs, weapons, malware and other hacking tools. The head of the National Cryptocurrency Initiative Team will report directly to the Assistant Attorney General in the DOJ's Criminal Division—and will lead a team comprised of prosecutors drawn from MLARs, the Computer Crime and Intellectual Property Section ("CCIPS"), and Assistant United States Attorneys detailed from multiple offices across the nation.

2022 and Beyond:

The emergence of newer, more sophisticated methods to facilitate money laundering has and will continue to prompt federal agencies to respond in kind (albeit on a reactive basis as opposed to a proactive one) with enforcement efforts like the DOJ's aggressive Cryptocurrency Initiative. We anticipate that while prosecutors will continue to focus on more conventional means by which criminal activity is funded, an equal emphasis will be placed on emerging technologies and the use of digital assets to conceal illicit activity.

Additionally, we expect that investigations and subsequent prosecutions of individuals and institutions involved in defrauding the federal government's COVID relief efforts to increase dramatically in 2022, as the pandemic begins to wane, and preliminary leads turn into full-scale investigations.

Conclusion & Key Takeaways

Although the new Administration got off to a slow start in 2021—largely due to partisan politics on Capitol Hill that impeded its ability to fill key positions within Treasury, DOJ and elsewhere—there were indications that, at the end of the 2021 calendar year, the Biden Administration was poised to take a more aggressive approach to holding individuals and companies accountable for criminal activity.

In concert with Deputy Attorney General Lisa Monaco's remarks to the ABA's White Collar Crime Institute (mentioned elsewhere in the context of this recap), the White House itself issued its comprehensive Strategy on Countering Corruption pursuant to the President's earlier Executive Order designating the fight against global corruption as an urgent national security priority of the United States. That strategy is predicated on five essential pillars: (1) modernizing, coordinating, and resourcing U.S. government efforts to fight corruption; (2) curbing illicit finance; (3) holding corrupt actors personally accountable for their actions; (4) preserving and strengthening the existing multilateral anti-corruption architecture; and (5) improving diplomatic engagement and leveraging foreign assistance resources to achieve anti-corruption policy goals.

Adding credence to the fifth pillar of the Biden Administration corruption strategy is the fact that the United States has increasingly cooperated on a multilateral basis with foreign regulatory agencies—including but not limited to, the UK's Financial Conduct Authority—to investigate and prosecute fraud in the financial markets. We anticipate that such efforts will continue with the breadth and scope of international cooperation increasing as the focus pivots to the enforcement of the FCPA and other international anti-bribery and corruption laws and regulations with a cross-border dimension.

As such, all compliance officers—but particularly those employed by international organizations—should ensure that their anti-bribery and corruption protocols and FCPA compliance programs are in line with current DOJ and SEC guidance.

DOJ's announcement in March 2021 that it would concentrate its efforts on recovering ill-gotten proceeds from the massive federal stimulus program directed at providing relief to individuals and businesses adversely impacted by COVID-19 is expected to generate even more significant returns in 2022. In the spring of 2021, the DOJ reported that it had initiated cases against 474 defendants in attempts to recover over $569 million in COVID relief funds. This included filing actions in fifty-six federal district courts

around the nation. Although no statistics were immediately available for the totality of FY 2021 as of the date of this report, based on DOJ's previous press release, we anticipate that the number of COVID-19 related enforcement actions to be substantial. We predict that 2022 will be an even bigger year for federal prosecutors as preliminary investigations mature and additional criminal charges and asset forfeiture suits are initiated.

Compliance officers should be prepared to face additional government scrutiny regarding the use of COVID-19 funds, including those legally obtained. The key to avoiding federal investigation and prosecution is to keep meticulous records involving the application, provision, and use of any COVID-19 relief funds obtained by an organization.

Whistleblower activity across responsible agencies—which in 2021 continued to generate significant leads and resulted in numerous successful enforcement actions—is only likely to increase in 2022 and beyond as the government further incentivizes cooperation in corporate malfeasance investigations. **In this vein, compliance officers should ensure that current internal reporting policies and procedures are aligned with both government expectations and industry best practices.** But mere implementation of an internal reporting mechanism is insufficient. **To avoid having matters escalate outside of the organization, it is critical that companies diligently investigate and document all reported infractions of the law and violations of the company's code of ethics or conduct.** It is simply a fact that employees whose concerns are relegated to the periphery are exponentially more likely to report to external regulators, increasing legal costs for the organization overall, and resulting in substantial criminal and/or civil penalties for deficient reporting and follow up procedures.

Finally, we anticipate that 2022 will continue to see aggressive government efforts to combat fraud in the digital currency markets. Both CFTC and DOJ have taken the lead in prosecuting individuals responsible for cryptocurrency fraud and recovering substantial amounts for unwitting victims. DOJ's new Cryptocurrency Initiative is likely to yield even more investigations, prosecutions, and recoveries. In addition, given the Biden Administration's seemingly negative view of the digital asset market—indeed, many public statements by Administration officials have often mischaracterized the cryptocurrency market as facilitating criminal activity—we anticipate that additional regulation of the cryptocurrency market itself will emerge. **Businesses involved in the offering, trading, and mixing of digital assets like cryptocurrency should ensure that they comply with all applicable statutes and regulations—including the CEA, its implementing regulations, and Anti-Money Laundering laws.**

Diligent

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS provider, serving more than one million users from over 25,000 organizations around the globe. Our modern GRC platform ensures boards, executives and other leaders have a holistic, integrated view of audit, risk, information security, ethics and compliance across the organization. Diligent brings technology, insights and confidence to leaders so they can build more effective, equitable and successful organizations.

For more information or to request a demo:

Email: **info@diligent.com** • Visit: **diligent.com**