THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Assistant Attorney General Kenneth A. Polite Jr. Delivers Remarks at NYU Law's Program on Corporate Compliance and Enforcement (PCCE)

New York, NY ~ Friday, March 25, 2022

Remarks as Prepared for Delivery

I have been fortunate in my career to have served as a prosecutor, as a defense attorney, and to work as a chief compliance officer of a Fortune 500 company. The detection and prevention of criminal conduct has been a constant across these three roles. Perhaps the most challenging of the three roles has been serving in compliance.

I know the resource challenges. The challenges you have accessing data. The relationship challenges. The silo-ing of your function. You are called upon to be a resource for information, an enforcer of law and policy, and somehow the primary architect of your company's ethical culture. I have seen first-hand how a strong compliance program can ward off misconduct and empower ethical employees. Although I am the head of the Criminal Division, I believe that enforcement, while a critical tool, is not our only one. I believe that the number of prosecutions we bring is not necessarily the most accurate measure of our success.

Having served in these three positions, I know that your compliance role is perhaps the most impactful, because you have a direct role in utilizing the most effective tool in addressing crime – you are trying to prevent it in the first place. That is why we closely evaluate corporate compliance programs during our corporate investigations and after our corporate resolutions, and give significant credit to companies that build strong controls to detect and prevent misconduct.

Today, I want to describe in detail about how we evaluate corporate compliance programs to ensure that companies are designing and implementing effective compliance systems and controls, creating a culture of compliance, and promoting ethical values. As our Evaluation of Corporate Compliance Programs guidance makes clear, we expect an effective corporate compliance program to be much more than a company's policies, procedures, and internal controls. We expect companies to implement compliance programs that: (1) are well designed, (2) are adequately resourced and empowered to function effectively, and (3) work in practice.

First, when we say that we expect a company's compliance program to be well designed, we closely examine the company's process for assessing risk and building a program that is tailored to manage its specific risk profile. We want to see whether the company has implemented policies and procedures that are designed to address the key risk areas identified in its risk assessments, and that those policies and procedures are easily accessible and understandable to the company's employees and business partners. We want to know how the company is training employees, management, and third-parties on the risk areas and responsibilities applicable to those individuals. Policies, training, and other processes should address relevant high-risk elements of the company's business model, such as third-party relationships or mergers and acquisitions. We want to see that the company has established a process for reporting violations of law or company policy that encourages employees to speak up without fear of retaliation, and that those reports are taken seriously, appropriately documented, investigated, and—if substantiated—remediated.

Second, when we are evaluating whether a compliance program is adequately resourced and empowered to function effectively, we want to know more than dollars, headcount, and reporting lines. We will review the qualifications and expertise of key compliance personnel and other gatekeeper roles. We want to know if compliance officers have adequate access to and engagement with the business, management, and the board of directors. We seek to

understand whether and how a company has taken steps to ensure that compliance has adequate stature within the company and is promoted as a resource. A company's commitment to promoting compliance and ethical values at all levels—from the chief executive on down to middle and lower-level managers—is critical.

Third, we want to see evidence that the compliance program is working in practice. We look at whether the company is continuously testing the effectiveness of its compliance program, and improving and updating the program to ensure that it is sustainable and adapting to changing risks. We want to know that a company can identify compliance gaps or violations of policy or law. Equally importantly, we want to see how the company addresses the root causes of these gaps or violations and finds ways to improve its controls and prevent recurrence of issues. We want to see examples of compliance success stories— the discipline of poor behavior, the rewarding of positive behavior, the transactions that were rejected due to compliance risk, positive trends in whistleblower reporting, and the partnerships that have developed between compliance officers and the business. We are also interested in how a company measures and tests its culture—at all levels of seniority and throughout its operations—and how it uses the data from that testing to embed and continuously improve its ethical culture.

There is a separate question of whether a company is demonstrating an ethical culture in practice. Do employees feel empowered to bring issues and questions to the management's attention? Are managers and compliance officers providing ethical advice to salespeople even though such advice may mean loss of business? Just as we use data analytics to detect and combat criminal schemes, we urge corporations to consider what data analytic tools they can use to monitor compliance with laws and policies within their operations and to ferret out wrongdoing when it occurs.

In addition, whether and how the company responds to prior misconduct speaks to its commitment to compliance and an ethical culture. Companies that have effectively deployed capabilities to conduct independent monitoring and testing of all elements of their compliance program, not just their financial controls—for example, testing effectiveness of training, communications, and compliance culture—and made improvements to the compliance program as a result, set themselves apart. I know that many of you are working at or on behalf of companies to help them design and implement compliance programs, and some of you may be making compliance presentations to our prosecutors in the future. On a practical level, when communicating with us, it is important to demonstrate how a compliance program has been upgraded to address the root cause of the misconduct, and how it is being tested and updated to ensure that it is sustainable and adaptable to changing risk.

We prefer not to hear a 'check-the-box' presentation from outside counsel. We like to see the Chief Compliance Officer leading the compliance presentation and demonstrating knowledge and ownership of the compliance program. Not for show, but because we want to empower these teams. Other senior management should also participate, taking ownership of their role in the compliance program and demonstrating commitment to compliance. Based on what we learn about the company's compliance program, we determine whether an independent compliance monitor should be imposed. We believe that monitorships are effective tools for strengthening corporate compliance programs in companies where there were compliance weaknesses that resulted in criminal conduct. Monitors can be allies to compliance officers in making recommendations that create lasting, sustainable change in corporate culture.

As the Deputy Attorney General discussed last October, we can expect to see the Department imposing independent corporate monitors whenever it is appropriate in order to satisfy our prosecutors that a company is living up to its compliance and disclosure obligations under a non-trial resolution.

When a monitorship is imposed, we follow the Criminal Division's well-settled selection procedures. When proposing their three monitor candidates to the Division, we encourage companies to not only ensure that the candidates are eminently qualified with deep compliance experience but also that the candidates are diverse both in terms of their types of experience as well as background, in keeping with the Department's commitment to diversity, equity, and inclusion. Monitors, of course, are not appropriate in every case. For example where a company:

- has invested—not just from a financial perspective, but from a concerted commitment from the top down—in implementing a strong compliance program;
- has been able to test its controls and demonstrate they are effective;
- has made relevant updates to its program to adapt to changing risks;

- and has cultivated a strong culture of compliance and ethical values, our prosecutors may decide not to impose a monitor.

To ensure that we are equipped with the resources to make these determinations, we have prioritized building a wealth of compliance expertise among our prosecutors and dedicating resources to strengthen our abilities to assess the effectiveness of compliance programs. We recently revamped the Fraud Section's former Strategy, Policy, and Training Unit into the Corporate Enforcement, Compliance, and Policy (CECP) Unit to align the name with the Unit's mission, and we've announced new management comprised of prosecutors and former compliance and defense lawyers with deep experience in compliance, monitorships, and corporate enforcement matters. We plan to add additional capability to the Unit. This Unit has responsibility for many aspects of the Fraud Section's corporate criminal enforcement practice.

When a company comes in to make a compliance presentation to the Fraud Section, it will face tough and probing questions from our compliance specialists. The CECP Unit also provides training on compliance and monitorship matters to prosecutors within and outside the Fraud Section, and works on policy issues. Having these resources helps us to use a consistent approach when evaluating whether a monitor is appropriate. It also allows us to employ appropriate compliance obligations to ensure corporations are maintaining effective compliance programs post-resolution. When we determine that a monitor is not necessary, that does not mean that the company's obligations to continue to test, improve, and demonstrate the effectiveness of its compliance program end when the resolution is papered. Companies without a monitor are still required to comply with ongoing obligations and report to the Department regarding the status of compliance obligations.

Our CECP attorneys review work plans and self-reports and continue to evaluate a company's progress—both in reviewing and testing its compliance program and in making the appropriate enhancements to ensure that, at the end of the term of the resolution agreement, the corporation has an effective and sustainable corporate compliance program that is designed to detect and prevent recurrence of criminal misconduct. We are holding companies accountable for failing to comply with their obligations under our corporate resolutions—including obligations to implement an effective compliance program, cooperate, or report allegations of misconduct.

Companies face consequences for violating our agreements, which can and have involved breaches and extensions of the agreements, including extensions of monitorships. Just as we propose charges based on the particular facts and circumstances of a given case, so too with breaches of corporate resolutions: we tailor our proposed sanctions to the nature of any breach, to address the particular facts and circumstances at bar. Whether it's a corporate guilty plea or an extension of a monitorship, we will pursue appropriate punishments. Our message is clear – companies that make a serious investment in improving their compliance programs and internal controls will be viewed in a better light by the Department. Support your compliance team now or pay later.

Chief Compliance Officers and their functions should have true independence, authority, and stature within the company. In order to further empower Chief Compliance Officers, for all of our corporate resolutions (including guilty pleas, deferred prosecution agreements, and non-prosecution agreements), I have asked my team to consider requiring both the Chief Executive Officer and the Chief Compliance Officer to certify at the end of the term of the agreement that the company's compliance program is reasonably designed and implemented to detect and prevent violations of the law (based on the nature of the legal violation that gave rise to the resolution, as relevant), and is functioning effectively. In certain resolutions, we will require additional certification language.

As you are aware, when a monitor is imposed pursuant to a resolution, we do not require companies themselves to also provide annual self-reports on the state of their compliance programs since the monitor provides annual reports to the government. However, in instances where a monitor is not imposed and a company is required to provide annual self-reports on the state of their compliance programs, we will consider requiring that the CEO and the CCO will also have to certify that all compliance reports submitted during the term of the resolution are true, accurate, and complete. By taking this step, we are ensuring that Chief Compliance Officers receive all relevant compliance-related information and can voice any concerns they may have prior to certification. I have been in your CCO role. Again, I know the challenges.

Today’s announcement is not punitive in nature. No, it is a new tool in your arsenal to combat those challenges. It is the type of resource that compliance officials, including myself, have wanted for some time, because it makes it clear that you should and must have appropriate stature in corporate decision-making. It is intended to empower our compliance professionals to have the data, access, and voice within the organization to ensure you, and us, that your company has an ethical and compliance focused environment.

A final word, connecting our emphasis on strengthening compliance to some of our recent policy announcements. When you are asked about your compliance program and whether its adequately creating, maintaining, and supporting an ethical culture, the question again goes to individual accountability. We want to know about your investment in compliance, not simply because we want you to hire more consultants or buy more sophisticated training software. No, as a former Chief Compliance Officer who now serves as the head of the Criminal Division, I want to know whether you are doing everything you can to ensure that when that individual employee is facing a singular ethical challenge, he has been informed, trained, and empowered to choose right over wrong. Or if he makes the wrong choice, you have a system that immediately detects, remediates, disciplines, and then adapts to ensure that others do not follow suit. That is how powerful a role you have in improving our world. Embracing that calling, today and every day.

I look forward to working with you, individually and collectively, in preventing and combatting criminality in the workplace and our world at large. Thank you, and have a wonderful conference.

Speaker:
Assistant Attorney General Kenneth A. Polite, Jr.

Component(s):
Criminal Division

Updated March 31, 2022

THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations

Washington, DC ~ Thursday, June 16, 2022

Remarks as Prepared for Delivery

Good afternoon. It's great to be with you. I'm glad to be joining you virtually although I wish I were there in person. Thank you for inviting me to speak with you today – this is a terrific gathering and a great forum, particularly for women leading investigations and enforcement work around the world. I'm especially glad to be joining this discussion among a broad group of practitioners, in house counsel and regulators.

I want to use my time with you all to speak about trends in the department's approach to corporate criminal enforcement, with a particular focus on sanctions enforcement. Before I get to sanctions let me start by updating you on some of the department's most recent work when it comes to corporate criminal enforcement – it has been a very active time.

In the span of the last month and a half, the department's investigators and prosecutors have:

- Charged the founder of Archegos and three other executives with racketeering and fraud related to market manipulation that caused more than $100 billion in market cap losses when Archegos collapsed; and
- The department announced four corporate guilty pleas — by Allianz Global Investors, Glencore International AG, Glencore Ltd. and Fiat Chrysler — who collectively agreed to pay over $7 billion in criminal penalties.

Between these five cases, we have charged 12 individuals, including a CEO, a CFO, three portfolio managers and three traders. While the number of charged defendants and penalty size alone don't tell the whole story, the department is committed to a data-driven assessment of our work on corporate criminal enforcement, to identify what works and what does not.

When it comes to corporate criminal enforcement, our mission is to enforce the criminal laws that govern corporations, executives, officers and others, in order to protect jobs, guard savings and maintain our collective faith in the economic engine that fuels this country. We will hold those that break the law accountable and we will promote respect for the laws designed to protect investors, consumers and employees.

Our resolve is strengthened by another accelerating trend: corporate crime increasingly implicates national security in ways that are all-too-relevant to this group and in this current moment.

Corporations that pay bribes and kickbacks to foreign governments, that pay terrorist groups for protection, or that launder funds for sanctions evaders – they profit from crimes at the expense of our collective peace and prosperity.

Today, the geopolitical landscape is more challenging and complex than ever. The most prominent example is of course Russia's invasion of Ukraine – which is nothing less than a fundamental challenge to international norms, sovereignty and the rule of law that underpins our society. Our collective security and prosperity face further challenges from other countries, such as those that sponsor the rampant theft of trade secrets, subject ethnic minority groups to forced labor or prop up regimes through institutional corruption.

Increasingly, you and your clients are on the front lines in responding to these geopolitical realities. We recognize that the complicated geopolitical environment forces companies to constantly make tough and sometimes costly decisions.

As advisors to the companies and institutions confronting this landscape, you can help your clients navigate this terrain and make the right decisions in this complex environment. The department wants to support those that do — such as the many companies who have made the tough and costly decision to depart from Russia in recent months.

To use the vernacular of national security lawyers, our goal is not only to hold people accountable, but to disrupt these threats using all the tools available to us. And we continue to develop new tools to do so every day. Just last week, the department announced the issuance of seizure warrants for two U.S. manufactured luxury jets owned by a Russian oligarch — the first such warrants issued based on violations of commerce regulations governing the reexport of U.S. aircraft to Russia. We will continue to develop creative tools to hold people, regimes and companies accountable.

An all-tools approach to corporate criminal enforcement includes enlisting the private sector to help watch out for misconduct within companies. For those truly committed to promoting a corporate culture that values and invests in compliance — rather than begrudges or under-resources it — the department stands ready to work with you to do what we can to promote and reward such cultures.

One tool that is increasingly prominent at the intersection of national security challenges and corporate criminal enforcement is the department's work on sanctions enforcement.

For years, the department has targeted sanctions evasion — so we're by no means starting on a blank canvas. Three sanctions cases in the last decade have each involved over $1 billion in collective civil and criminal penalties.

But what you have seen in the last few months is something completely different. The United States has shown leadership in galvanizing broad, multilateral networks to meet today's challenges. The scope of the sanctions imposed on Russia by the United States and its allies and partners are of a new order of magnitude. Recognizing the critical need to enforce these sanctions with unprecedented intensity, the department launched Task Force KleptoCapture to pursue Russian sanctions evasion, particularly by oligarchs and other cronies who have propped up and enabled the Russian regime responsible for the unjustified and unprovoked aggression against Ukraine. We are pouring resources into sanctions enforcement, and you have seen and will continue to see results.

But it's not just the war in Ukraine that has prompted a new level of intensity and commitment to sanctions enforcement. We have turned a corner in our approach. Over the last couple of months, I've given notice of that sea change by describing sanctions as "the new FCPA."

The growth of sanctions enforcement follows the path that the FCPA traveled before it. Both FCPA and sanctions enforcement are relevant to an expanding number of industries. They have extended beyond just U.S. actions to an increasingly multilateral enforcement regime. And they both reward companies that develop the capacity to identify misconduct within the organization, and then come forward and voluntarily disclose that misconduct to the department. Let me expand on each of those points.

First, sanctions enforcement is relevant to an expanding number of industries. Sanctions have been considered by some as a concern mainly for banks and financial institutions. As companies grapple with the fallout of Russian aggression and the new intensity of sanctions enforcement, though, they are recognizing that the risk of sanctions violations cuts across industries and geographic regions.

For any multinational corporation — indeed, for any business with an international supply chain — sanctions should be at the forefront of its approach to compliance. Every company needs to be pressure-testing its sanctions compliance program, for instance through risk assessments, technology upgrades and industry benchmarking. Every board of directors of such a company should be inquiring whether it is conducting necessary oversight of the company's sanctions controls. Every corporate officer should be committed to ensuring they have the programs, culture, personnel and counsel to identify problem areas and navigate the rapidly changing landscape. And for anyone who seeks to evade sanctions, the warning is simple: the Justice Department is coming for you.

Our sanctions enforcement is also more and more a multinational team sport. Just as the last decade saw the world of FCPA enforcement expand to foreign partners and counterparts, the months and years ahead will see the department's sanctions teams work hand-in-glove with civil and law enforcement agencies across the world. The multilateralization of

our sanctions work follows the same trajectory as our FCPA history, which grew from a largely unilateral effort by the United States to a worldwide movement to combat international corruption.

From Spain to Fiji, we have relied on local counterparts in our early successes against Russian sanctions evasion, and we will continue to need similar partnerships. The Attorney General and I frequently speak with counterparts in partner countries about our collective work on sanctions, including with our friends in the United Kingdom.

In addition to our own KleptoCapture task force, the department is working cooperatively with our international partners through the multilateral Russian Elites, Proxies, and Oligarchs (REPO) Task Force — an international collaboration between the United States and European Union to cooperate at an unprecedented level on multilateral sanctions enforcement to isolate international actors undermining the world's security, stability and international norms. Such partnerships are sure to continue and expand.

The multilateral growth in FCPA and sanctions enforcement has also allowed us to go after those who profit from corruption and crime around the world — whether they are sanctions-evading oligarchs or office-holding bribe recipients. Working with our partners, we can ensure that corrupt regimes will be held responsible — whether we're seizing yachts or freezing slush funds.

Finally, we aim for our sanctions enforcement to incentivize companies to come forward and voluntarily disclose discovered misconduct. As with the FCPA, the department — through the National Security Division I had the privilege to lead earlier in my career — has a self-disclosure program to address potential criminal sanctions violations. We drew on the model from the FCPA with this self-disclosure program and since the relevant NSD guidelines were revised in 2019, the number of voluntary self-disclosures is increasing.

The National Security Division continues to refine the program, and last year the department had its first resolution under its Voluntary Self-Disclosure program. That resolution — involving SAP — rewarded the company for its self-disclosure and cooperation with no fine and only disgorgement of the revenue the company earned. Contrast the form of that resolution to the four recent corporate guilty pleas over the last month or so, which carried collective criminal penalties of nearly $7 billion. The math is simple: self-disclosure can save a company hundreds of millions of dollars.

For any company that thinks it may have a sanctions problem, I have a clear, unequivocal message for you: pick up the phone and call us. Do not wait for us to call you.

In closing, you can expect to see more action in sanctions enforcement, both by the U.S and by our international partners. And I hope and expect to see a new level of sophistication and resource commitment to sanctions compliance at companies across the globe. Thank you for having me today.

Speaker:
Lisa O. Monaco, Deputy Attorney General

Component(s):
Office of the Deputy Attorney General

Updated June 16, 2022

FinCEN ADVISORY

FIN-2022-A001 April 14, 2022

Advisory on Kleptocracy and Foreign Public Corruption

FinCEN urges financial institutions to focus efforts on detecting the proceeds of foreign public corruption, a priority for the U.S. government.

SAR Filing Request:
FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**CORRUPTION FIN-2022-A001**" and selecting SAR field 38(m). Additional guidance on filing SARs appears near the end of this advisory.

Corruption includes the abuse of authority or official position to extract personal gain. Corruption corrodes public trust; hobbles effective governance; undercuts development efforts; contributes to national fragility, extremism, and migration; and provides authoritarian leaders a means to undermine democracies worldwide.[5]

Introduction

Last year, President Biden established the fight against corruption as a core national security interest.[1] The proceeds of foreign public corruption travel across national borders and can affect economies and political systems far from the origin of the proceeds.[2] Foreign public corruption disproportionately harms the most vulnerable in societies, often depriving these populations of critical public services. In the United States, the proceeds of foreign public corruption can distort our markets, taint our financial system, and can erode public trust in government institutions.[3] Foreign public corruption can also violate U.S. law.[4]

Kleptocratic regimes and corrupt public officials may engage in bribery, embezzlement, extortion, or the misappropriation of public assets, among other forms of corrupt behavior, to advance their strategic, financial, and personal goals. In doing so, they may exploit the U.S. and international financial systems to launder illicit gains, including through the use of shell companies, offshore financial centers, and professional service providers who enable the movement and laundering

1. *See* White House, "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest," (June 3, 2021) (Memo on Establishing Fight Against Corruption). The 2022 U.S. National Money Laundering Risk Assessment reiterates corruption as a primary money laundering threat and provides the financial sector information on risks related to foreign and domestic corruption. For more information, *see* Treasury, "National Money Laundering Risk Assessment," (February 2022).
2. *Id*.
3. On June 30, 2021, the Financial Crimes Enforcement Network (FinCEN) issued the first national anti-money laundering and countering the financing of terrorism (AML/CFT) priorities (the "Priorities"), identifying corruption as one of the most significant AML/CFT threats currently facing the United States. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021), at p. 3; *see also*, FinCEN Press Release, "FinCEN Issues First National AML/CFT Priorities and Accompanying Statements," (June 30, 2021).
4. *See, e.g.*, the Foreign Corrupt Practices Act of 1977, 15 USC §§ 78dd-1, et seq.
5. *See* Memo on Establishing Fight Against Corruption, *supra* Note 1.

A ***kleptocracy*** is a government controlled by officials who use political power to appropriate the wealth of their nation for personal gain, usually at the expense of the governed population.

A ***kleptocrat*** uses their position and influence to enrich themselves and their networks of corrupt actors.

of illicit wealth, including in the United States and other rule-of-law-based democracies.[6] These practices harm the competitive landscape of financial markets and often have long-term corrosive effects on good governance, democratic institutions, and human rights standards.[7]

Russia is of particular concern as a kleptocracy because of the nexus between corruption, money laundering, malign influence and armed interventions abroad, and sanctions evasion. Corruption is widespread throughout the Russian government and manifests itself as bribery of officials, misuse of budgetary resources, theft of government property, kickbacks in the procurement process, extortion, and improper use of official positions to secure personal profits.[8] Russia's further invasion of Ukraine, for example, highlights foreign public corruption perpetrated by kleptocratic regimes like that of Russian President Vladimir Putin.[9] Russia's actions in Ukraine are supported and enabled by Russia's elites and oligarchs who control a majority of Russia's economic interests.[10] These individuals have a mutually beneficial relationship with President Putin that allows them to misappropriate assets from the Russian people while helping President Putin maintain his tight control on power.[11] Oligarchs are believed to be directly financing off-budget projects that include political malign influence operations and armed interventions abroad.[12] The U.S. government has imposed sanctions on many of these individuals and the businesses and state-owned entities they

6. *See* White House, "U.S. Strategy on Countering Corruption," (December 2021).
7. FinCEN has published several advisories highlighting corruption by foreign governments and officials. *See* FinCEN Advisory, "Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators," (June 12, 2018) (FinCEN Advisory on Human Rights and Corruption); *see also*, "Updated Advisory on Widespread Public Corruption in Venezuela," (May 3, 2018); "Advisory to Financial Institutions on the Risk of Proceeds of Corruption from Nicaragua," (October 4, 2018), and "Advisory to Financial Institutions on Political Corruption Risks in South Sudan," (September 6, 2017).
8. *See* U.S. Department of State (State), Bureau of Democracy, Human Right and Labor Report, "Russian 2020 Human Rights Report," (March 30, 2021), at p. 53.
9. *See* State, "International Narcotics Control Strategy Report Volume II," (March 2021), at p. 159 and the Helsinki Commission Report, "Corruption in Russia: An Overview," (October 23, 2017), at pp. 1-2.
10. It is estimated that the top 1 percent of Russians holds 58 percent of Russia's total wealth, and much of the wealth of these ultra-wealthy elite stems from businesses linked to the Russian state. For additional information, *see* Congressional Research Service Report, "Russia: Domestic Politics and Economy," (September 9, 2020) (Russia CRS Report), at p. 16. *See also*, U.S. Department of the Treasury (Treasury) Press Releases (Treasury Press Releases), "Treasury Prohibits Transactions with Central Bank of Russia and Imposes Sanctions on Key Sources of Russia's Wealth," (February 28, 2022); "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," (March 3, 2022); and "Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine," (March 11, 2022).
11. *See* CRS Report, *supra* Note 10, at p. 6.
12. *See* CRS Report, *supra* Note 10, at p. 17.

control as part of U.S. efforts to hold President Putin and his supporters accountable for Russia's further invasion of Ukraine, and to restrict their access to assets to finance Russia's destabilizing activities globally.[13]

This advisory provides financial institutions with typologies and potential indicators associated with kleptocracy and other forms of foreign public corruption, namely bribery, embezzlement, extortion, and the misappropriation of public assets.

The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open-source reporting, and information from law enforcement partners.

Typologies of Kleptocracy and Foreign Public Corruption

Wealth Extraction

Foreign public corruption can take many forms, including bribery, extortion, embezzlement, or misappropriation of public funds and assets. This corruption can occur at every level of government. For instance, in Russia, President Putin has allowed the resources of the Russian people to be siphoned off by oligarchs and elites, who amassed their fortunes through their

13. *See* Treasury Press Releases, *supra* Note 10. *See also*, FinCEN Alerts, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," (March 7, 2022) (FinCEN Alert on Russian Sanction Evasion); and "FinCEN Alert on Real Estate, Luxury Goods, and Other High Value Assets Involving Russian Elites, Oligarchs, and their Family Members," (March 16, 2022) (FinCEN Alert on Real Estate and High Value Assets involving Russian Elites). In addition to imposing financial sanctions against corrupt actors, the U.S. government has a number of tools to counter public corruption, kleptocracy, foreign malign influence, and foreign bribery across the globe. The Foreign Corrupt Practices Act (FCPA) makes it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. *See* 15 U.S.C. §§ 78dd-1, *et seq.* U.S. anti-money laundering laws prohibit transactions involving offenses against a foreign nation of extortion; bribery of a public official; or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official. *See* 18 U.S.C. § 1956(c)(7)(B)(ii) and (iv). Title 31 also prohibits, among other things, concealing, falsifying, or misrepresenting to a financial institution a material fact concerning a senior foreign political figure's control of assets in certain high-value transactions. *See* 31 U.S.C. § 5335. The Department of Justice (DOJ) and federal law enforcement, through specialized prosecutorial and investigative units, as well as through U.S. Attorneys' Offices, investigate and prosecute foreign corruption and related conduct, and seek recovery of foreign corruption proceeds for the benefit of the people harmed by such acts. For more information, *see generally*, DOJ, Foreign Corrupt Practices Act. DOJ's Kleptocracy Asset Recovery Initiative facilitates the recovery and return of corruption proceeds to the benefit of people harmed by corrupt acts. For more information, *see generally*, DOJ, Money Laundering and Asset Recovery Section (MLARS). Additionally, DOJ recently created Task Force KleptoCapture that focuses specifically on enforcing recent economic actions against Russia. For more information, *see* DOJ Press Release, "Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture," (March 2, 2022). On March 16, 2022, Treasury and the DOJ launched the multinational Russian Elites, Proxies, and Oligarchs (REPO) Task Force with counterparts across the globe. For more information, *see* Treasury and DOJ Press Release, "U.S. Departments of Treasury and Justice Launch Multilateral Russian Oligarch Task Force," (March 16, 2022). The Department of Commerce's Bureau of Industry and Security (BIS) regulate the export and import of critical and sensitive technologies paramount to U.S. national security. For more information, *see generally*, Bureau of Industry and Security | U.S. Department of Commerce. Treasury recently created the Kleptocracy Asset Recovery Reward Program. For more information, *see* Treasury, "Kleptocracy Asset Recovery Rewards Program," (March 16, 2022).

personal connections to Putin and the abuse of state-owned entities and assets.[14] This activity is not unique to Russia, however. Kleptocratic activities throughout the world are often associated with other criminal behavior, such as human rights abuses.[15]

Bribery and Extortion

Bribery schemes often involve payments to foreign government officials by persons and entities to obtain or retain business, or for other benefits.[16] Such schemes, which generally benefit both parties involved, may be employed to influence political outcomes, secure lucrative contracts with governments or state-owned enterprises, gain access to natural resources, or obtain fraudulent documents such as passports or visas, among other purposes. In certain situations, however, parties can be coerced and extorted by corrupt public officials to pay bribes in order to gain access to or continue their operations in the country of concern. Bribes and extortion payments can be made through third-party facilitators, as well as through legal entities that are controlled by family members and close associates, to conceal the ultimate beneficiary of the payment. In many cases, the payments are laundered through a network of shell companies, offshore financial centers, or professional service providers. Financial accounts into or from which bribes are deposited or withdrawn are sometimes established outside of a public official's country of residence to evade detection and financial institutions' sanctions screening and anti-money laundering/countering the financing of terrorism (AML/CFT) controls.

Bribery schemes with a U.S. nexus may be prosecuted in the United States under a range of laws, including the Foreign Corrupt Practices Act (FCPA).[17] Information provided by financial institutions through Suspicious Activity Reports (SARs) assists U.S. law enforcement in identifying and prosecuting these activities.

- **Bribery involving Russian state-owned entity:** In November 2019, the former president of Transportation Logistics Inc. (TLI), a Maryland-based transportation company, was found guilty after a federal trial for his role in a scheme to bribe an official at a subsidiary of Russia's State Atomic Energy Corporation and on related fraud and conspiracy charges. According to the evidence presented at trial, the defendant, Mark Lambert, participated in a scheme to bribe Vadim Mikerin, a Russian official at JSC Techsnabexport (TENEX), a subsidiary of Russia's State Atomic Energy Corporation and the sole supplier and exporter of

14. *See* White House Press Release, "Background Press Call by Senior Administration Officials on New Economic Costs on Russia," (April 6, 2022). *See also*, "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," (March 3, 2022).
15. *See* Russia CRS Report, *supra* Note 10, at p. 16.
16. *See* the Foreign Corrupt Practices Act of 1977, 15 USC §§ 78dd-1, *et seq*.
17. The FCPA's anti-bribery provisions apply broadly to three categories of persons and entities: (1) "issuers" and their officers, directors, employees, agents, and stockholders acting on behalf of an issuer; (2) "domestic concerns" and their officers, directors, employees, agents, and stockholders acting on behalf of a domestic concern; and (3) certain persons and entities, other than issuers and domestic concerns, acting while in the territory of the United States. For further information, *see generally*, DOJ, Foreign Corrupt Practices Act. *See also*, "A Resource Guide to the U.S. Foreign Corrupt Practices Act," a joint publication by the DOJ and the U.S. Securities and Exchange Commission.

Russian Federation uranium and uranium enrichment services to nuclear power companies worldwide, in order to secure contracts with TENEX. Lambert conspired with others at TLI to pay bribes to Mikerin through offshore bank accounts associated with shell companies, at Mikerin's direction. In order to conceal the bribes, Lambert and his co-conspirators caused fake invoices to be prepared, purportedly from TENEX to TLI, which described services that were never provided, and then Lambert and others caused TLI to wire the corrupt payments for those fictitious services to shell companies in Latvia, Cyprus, and Switzerland.[18]

- **Bribery Scheme in Brazil:** Odebrecht S.A., a global construction conglomerate based in Brazil, admitted in its guilty plea agreement with DOJ that it paid $788 million in bribes to or for the benefit of government officials in 12 countries, including Angola, Argentina, Brazil, Colombia, Dominican Republic, Ecuador, Guatemala, Mexico, Mozambique, Panama, Peru, and Venezuela between 2001 and 2016. Braskem S.A., a Brazilian petrochemical company, also admitted to paying approximately $250 million to Odebrecht to use to pay bribes to politicians and political parties in Brazil as well as at least one official at Petróleo Brasileiro S.A., the state-controlled oil company of Brazil. The criminal conduct was directed by the highest levels of the company, with the bribes paid through a complex network of shell companies, off-book transactions, and off-shore bank accounts. In all, this conduct resulted in corrupt payments and/or profits totaling approximately $3.336 billion. In April 2021, the former president of Braskem S.A. pled guilty to bribery charges and agreed to pay $2.2 million in forfeiture.[19]

Misappropriation or Embezzlement of Public Assets

Misappropriation or embezzlement of public assets broadly encompass the theft, diversion, or misuse of public funds or resources for personal benefit or enrichment.[20] These assets may involve government funds, services, contracts, or publicly owned natural resources, among others. Public officials or their associates may exploit or deceive corporations, including financial institutions that seek to do business with the government, into redirecting government resources for their own profit.[21] Embezzlement or misappropriation of public assets can also be tied to a bribery scheme.

18. *See* DOJ Press Release, "Former President of Transportation Company Found Guilty of Violating the Foreign Corrupt Practices Act and Other Crimes," (November 22, 2019).
19. DOJ and the Federal Bureau of Investigation seek information leading to the seizure, restraint, forfeiture, or repatriation of bribes or assets linked to bribes paid by Odebrecht S.A. and Braskem S.A. that are: (1) in an account at a U.S. financial institution, including a U.S. branch of a foreign financial institution; (2) that come within the United States; or (3) that come within the possession or control of any U.S. person. *See* Treasury webpage, "Kleptocracy Asset Recovery Rewards Program," for further details. For details related to the bribery scheme, *see* DOJ Press Release, "Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History," (Dec. 21, 2016). *See also* DOJ Press Release, "Former CEO of Braskem Pleads Guilty to Bribery," (April 15, 2021).
20. *See* Article 17 of the UN Convention Against Corruption, which requires member states to criminalize the intentional "embezzlement, misappropriation or other diversion by a public official for his or her benefit or for the benefit of another person or entity, of any property, public or private funds or securities or any other thing of value entrusted to the public official by virtue of his or her position".
21. *See* FinCEN Advisory on Human Rights and Corruption, supra Note 7 at p. 4.

Several types of procurement, such as in the defense and health sectors, large infrastructure projects, and development and other types of assistance, appear to pose a particularly high risk of being associated with corruption-related money laundering.[22] Below are recent examples of misappropriation or embezzlement of public assets by corrupt public officials:

- **Corruption in Belarus:** The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) recently sanctioned Alyaksandr Ryhorovich Lukashenka, the head of the corrupt government in Belarus whose patronage network benefits his inner circle and regime. Lukashenka, who was originally sanctioned in 2006, has rewarded businessmen close to him with benefits and privileges in exchange for kickbacks to himself and his regime. For example, Lukashenka enacted strategic policies that facilitated tobacco smuggling by U.S. designated Aliaksei Aleksin, granting Aleksin a virtual monopoly over the Belarusian tobacco industry.[23]
- **Corruption in El Salvador:** On December 9, 2021, OFAC designated Martha Carolina Recinos De Bernal. Recinos was the head of a multiple-ministry, multi-million-dollar corruption scheme in El Salvador involving suspicious procurements in the construction of a hospital, in addition to directing various government ministers to authorize several suspicious pandemic-related purchases, including millions of dollars in surgical masks and millions more on hospital gowns from companies with no apparent ties to the healthcare or manufacturing industries. Additionally, Recinos directed a corruption scheme in which government-purchased food baskets intended for COVID-19 relief were diverted for political gain and votes in municipal and legislative elections.[24]

Laundering Illicit Proceeds

Kleptocrats and other corrupt public officials typically use the same methods to launder their illicit gains as those used by other illicit actors, whether drug traffickers or transnational organized crime syndicates.

Shell Companies and Offshore Financial Accounts

Corrupt actors often use shell companies to obscure the ownership and origin of illicit funds.[25] Corrupt actors may also leverage their family members and close associates to create shell companies and open business or personal accounts on their behalf while retaining control of the accounts. These shell companies can be used to facilitate the payment of bribes as well as the illicit movement of funds stemming from the misuse of state assets and government contracts.[26]

22. *See generally*, Financial Action Task Force (FATF) Report, "Specific Risk Factors in Laundering the Proceeds of Corruption," (June 2012).
23. *See* Treasury Press Release, "Treasury Sanctions Russians Connected to Gross Human Rights Violations and Corrupt Leader of Belarus," (March 15, 2022).
24. *See* Treasury Press Release, "Treasury Issues Sanctions on International Anti-Corruption Day," (December 9, 2021).
25. *See* Treasury, "National Money Laundering Risk Assessment," (February 2022), at p. 26.
26. *See* FinCEN Advisory on Human Rights and Corruption, *supra* Note 7 at p. 4.

In addition, these shell companies and offshore accounts are frequently established in foreign jurisdictions whose corporate formation regimes and financial sector offer limited transparency to law enforcement, regulators, or financial institutions.[27] From these offshore financial centers, the funds are integrated into the broader financial system through investments and acquisitions.

FinCEN has taken several steps to curb the use of shell companies in the United States. Customer Due Diligence regulations took effect in 2018, requiring certain financial institutions to collect beneficial ownership information of legal entity customers at the time of account opening.[28] More recently, FinCEN has begun implementing the Corporate Transparency Act (CTA), enacted as part of the Anti-Money Laundering Act of 2020. The CTA requires, among other things, that Treasury create a beneficial ownership information database.[29]

Purchase of Real Estate, Luxury Goods and other High-Value Assets

Corrupt officials and others involved in bribery and other forms of corruption often purchase various U.S. assets, such as luxury real estate and hotels, private jets, artwork, and motion picture companies, to launder the proceeds of their corruption.[30] The use of anonymous companies or straw purchasers to acquire high-value assets that maintain relatively stable value is attractive to all types of illicit actors, both domestic and foreign.[31] Real estate may offer an attractive vehicle for storing wealth or laundering illicit gains due to its high value, its potential for appreciation, and the potential use of layered and opaque transactions to obfuscate a property's ultimate beneficial owner.[32] The purchase of real estate in connection with criminal conduct also may include complicit real estate professionals as well as the use of legal entities and nominees to avoid detection.[33]

27. *See* Financial Action Task Force on Money Laundering (FAFT) Report, Laundering the Proceeds of Corruption, (July 2011), at p. 23.
28. *See* FinCEN Press Release, "FinCEN Reminds Financial Institutions that the CDD Rule Becomes Effective Today," (May 11, 2018).
29. The CTA is Title LXIV of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283 (January 1, 2021) (NDAA). Division F of the NDAA is the Anti-Money Laundering Act of 2020, which includes the CTA. Section 6403 of the CTA, among other things, amends the BSA by adding a new Section 5336, Beneficial Ownership Information Reporting Requirements, to Subchapter II of Chapter 53 of Title 31, United States Code. *See also*, FinCEN Press Release, "FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency," (December 7, 2021), and FinCEN Fact Sheet, "Fact Sheet: Beneficial Ownership Information Reporting Notice of Proposed Rulemaking (NPRM)," (December 7, 2021).
30. *See* FBI Congressional Testimony, "Combating Money Laundering and Other Forms of Illicit Finance," (November 29, 2018).
31. *See* Treasury, "National Strategy to Counter Illicit Finance," (February 2020) (Illicit Finance Strategy), at p. 16.
32. *See* Executive Order 14068, "Prohibiting Certain Imports, Exports, and New Investment With Respect to Continued Russian Federation Aggression," (March 11, 2022), and White House, "FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia," (March 11, 2022). *See also*, FinCEN Alert on Real Estate and High Value Assets involving Russian Elites, *supra* Note 13, at p. 2.
33. *See* Illicit Finance Strategy, *supra* Note 31, at p. 17. Additionally, FinCEN recently published an Advance Notice of Proposed Rulemaking on money laundering in the real estate sector. For more information, *see* FinCEN Press Release, "FinCEN Launches Regulatory Process for New Real Estate Sector Reporting Requirements to Curb Illicit Finance," (December 7, 2021). For further information regarding money laundering risks in the real estate sector, *see* FinCEN, "Advisory to Financial Institutions and Real Estate Firms and Professionals," (August 22, 2017) (FinCEN Advisory on Real Estate Firms and Professionals).

- Recently, the U.S. government announced it would work with allies and partners to block President Putin and certain Russian elites' assets in the United States and elsewhere, including their real estate, private jets, and mega yachts.[34] For example, OFAC recently sanctioned the family of Dmitriy Sergeevich Peskov, a close ally of President Putin and lead propagandist and spokesperson for the Russian Federation. Peskov's family is reported to own real estate in Russia and elsewhere valued at more than $10 million, and to have access to a number of luxury vehicles, including private aircrafts and yachts, which they use for travel across the world.[35]

Financial Red Flag Indicators of Kleptocracy and Foreign Public Corruption

FinCEN has identified the following financial red flag indicators to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with kleptocracy and foreign public corruption. Because no single financial red flag indicator is determinative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.

1. Transactions involving long-term government contracts consistently awarded, through an opaque selection process, to the same legal entity or entities that share similar beneficial ownership structures.[36]
2. Transactions involving services provided to state-owned companies or public institutions by companies registered in high-risk jurisdictions.
3. Transactions involving official embassy or foreign government business conducted through personal accounts.
4. Transactions involving public officials related to high-value assets, such as real estate or other luxury goods, that are not commensurate with the reported source of wealth for the public official or that fall outside that individual's normal pattern of activity or lifestyle.
5. Transactions involving public officials and funds moving to and from countries with which the public officials do not appear to have ties.[37]

34. *See* White House, "FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice," (March 3, 2022). *See also*, FinCEN Alert on Real Estate and High Value Assets involving Russian Elites.
35. *See* Treasury Press Release, "Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine," (March 11, 2022).
36. *See generally*, Egmont Group Report, "Public Summary: FIU Tools and Practices for Investigations Laundering of the Proceeds of Corruption," (July 2019), at p. 16.
37. *See* FinCEN Advisory on Human Rights and Corruption, *supra* Note 7, at p. 6.

6. Use of third parties to shield the identity of foreign public officials seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.[38]

7. Documents corroborating transactions involving government contracts (e.g., invoices) that include charges at substantially higher prices than market rates or that include overly simple documentation or lack traditional details (e.g., valuations for good and services).

8. Transactions involving payments that do not match the total amounts set out in the underlying documentation, or that involve vague payment details or the use of old or fraudulent documentation to justify transfer of funds.

9. Transactions involving fictitious email addresses and false invoices to justify payments, particularly for international transactions.

10. Assets held in the name of intermediate legal entities whose beneficial owner or owners are tied to a kleptocrat or his or her family member.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting
Other Relevant BSA Reporting
Due Diligence
USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions evasion.[39] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[40]

38. *See* FinCEN Advisory on Real Estate Firms and Professionals, *supra* Note 33. *See also*, FinCEN Alert on Russian Sanction Evasion, *supra* Note 13.

39. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions with these SAR filing requirements also may file a SAR regardless of the amount involved (if any) or if the transaction is only attempted.

40. *See* 31 U.S.C. § 5318(g)(3).

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[41] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[42] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML/CFT program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SARs and OFAC Sanctions

Longstanding FinCEN guidance[43] provides clarity regarding when a financial institution must satisfy its obligation to file a SAR on a transaction involving a designated person when also filing a blocking report with OFAC. Relatedly, ransomware attacks and payments on which financial institutions file SARs should also be reported to OFAC at OFAC_Feedback@treasury.gov if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment.

SAR Filing Instructions

FinCEN requests that financial institutions reference this alert by including the key term "**CORRUPTION FIN-2022-A001**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.[44]

41. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), and 1030.320(d).
42. *Id*. *See also*, FinCEN, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).
43. *See* FinCEN, The SAR Activity Review, Issue 8, Section 5 "Revised Guidance on Filing Suspicious Activity Reports Relating to the Office of Foreign Assets Control List of Specially Designated Nationals and Blocked Persons," pp. 38-40, (April 2005), which states, "[t]o the extent that the financial institution is in possession of information not included on the blocking report filed with [OFAC], a separate [SAR] should be filed with FinCEN including that information. This guidance also does not affect a financial institution's obligation to file a [SAR] even if it has filed a blocking report with [OFAC], to the extent that the facts and circumstances surrounding the [OFAC] match are independently suspicious and are otherwise required to be reported under the existing FinCEN regulations. In those cases, the [OFAC] blocking report would not satisfy a financial institution's [SAR] filing obligation….When a financial institution files a reject report on a transaction, the financial institution is obligated to file a [SAR] to the extent that the facts and circumstances surrounding the rejected funds transfer are suspicious."
44. For activity involving possible violations of export and import restrictions and other controls related to Russia, as set by the U.S. Department of Commerce's BIS, financial institutions should include the key term "FIN-2022-RUSSIABIS". For relevant actions related to Russia's invasion of Ukraine, *see* Bureau of Industry and Security | U.S. Department of Commerce. *See also*, U.S. Commerce Department's BIS, Red Flag Indicators.

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[45]

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[46]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this alert.[47] These include obligations related to the Currency Transaction Report (CTR),[48] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[49] Report of Foreign Bank and Financial Accounts (FBAR),[50] Report of International Transportation of Currency or Monetary Instruments (CMIR),[51] Registration of Money Services Business (RMSB),[52] and

45. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
46. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2).
47. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer's foreign bank and financial accounts) to FinCEN "that are highly useful in (A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B) intelligence or counterintelligence activities, including analysis, to protect against terrorism;" 31 U.S.C. § 5311(1).
48. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than $10,000, in aggregate per business day. 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
49. A report filed by any U.S. person engaged in a trade or business on the receipt of more than $10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
50. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds $10,000 at any time during the calendar year, as specified in 31 CFR § 1010.350 and FinCEN Form 114.
51. Each person (*i.e.*, an individual or legal entity), as defined in 31 CFR § 1010.100(mm), that transports, ships, or mails more than $10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 CFR § 1010.340.
52. Report for a business required to register with FinCEN as a money services business, as defined in 31 CFR § 1010.100(ff), or renewing the registration. 31 CFR § 1022.380.

Designation of Exempt Person (DOEP).[53] These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this alert, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**CORRUPTION FIN-2022-A001**" in the "**Comments**" section of the report.

Due Diligence

Due diligence obligations (senior foreign political figures)

Financial institutions should establish risk-based controls and procedures that include reasonable steps to ascertain the status of an individual as a senior foreign political figure (along with their families and their associates, together often referred to as foreign "politically exposed persons" (PEPs)) and to conduct scrutiny of assets held by such individuals.[54]

FinCEN's Customer Due Diligence (CDD) Rule requires banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[55] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign PEPs.

Enhanced due diligence obligations for private banking accounts

In addition to these general risk-based due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, certain U.S. financial institutions must implement a due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.[56]

53. Report for banks, as defined in 31 CFR § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311.
54. *See* 31 CFR § 1010.620(c).
55. *See* 31 CFR § 1010.230.
56. *See* 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).

General obligations for correspondent account due diligence and AML/CFT programs

Banks, brokers or dealers in securities, mutual funds, and FCM/IBs also are reminded to comply with their general due diligence obligations for correspondent accounts under 31 CFR § 1010.610(a), in addition to their general AML/CFT program obligations under 31 U.S.C. § 5318(h) and its implementing regulations (which apply to all U.S. financial institutions).[57] MSBs have parallel requirements with respect to foreign agents or foreign counterparties, as described in FinCEN Interpretive Release 2004-1, which clarifies that the AML program regulation requires MSBs to establish adequate and appropriate policies, procedures, and controls commensurate with the risk of money laundering and the financing of terrorism posed by their relationship with foreign agents or foreign counterparties.[58]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving sanctions evasion, ransomware/cyberattacks, and the laundering of the proceeds of corruption, among other illicit activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[59] FinCEN strongly encourages such voluntary information sharing.

For Further Information

Questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

57. *See* 31 CFR §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210.
58. *See* FinCEN, "Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties," Interpretive Release 2004-1, 69 FR 239, (December 14, 2004). *See also*, FinCEN, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring," (March 11, 2016).
59. For further guidance related to the 314(b) Program, *see* FinCEN, "Section 314(b) Fact Sheet," (December 20, 2020).

Davis Polk

DOJ announces compliance certifications to be considered as part of corporate criminal resolutions

March 31, 2022 | Client Update | 9-minute read

In a pair of speeches last week, the Assistant Attorney General of DOJ's Criminal Division emphasized its focus on compliance and announced that he has instructed his prosecutors to consider requiring chief executive officers and chief compliance officers to certify to (1) the accuracy of annual reports submitted pursuant to corporate resolutions, and (2) the effectiveness of their company's compliance program prior to releasing the company from its obligations under a resolution agreement.

Assistant Attorney General (AAG) Kenneth Polite – who oversees many of the Department of Justice's (DOJ) most significant corporate criminal cases relating to the Foreign Corrupt Practices Act (FCPA), financial fraud, anti-money laundering (AML), the Bank Secrecy Act, computer crimes, and health care fraud violations – gave the speeches at the ACAMS AML and Financial Crime Conference in Hollywood, Florida, on March 22 and the NYU Program for Corporate Compliance and Enforcement Conference on Assessing Effective Compliance on March 24.

In particular, he has asked his prosecutors to consider requiring the chief executive officer (CEO) and chief compliance officer (CCO) of the relevant corporate entity to certify that their compliance program is reasonably designed and implemented as part of the close-out of a company's resolution agreement with DOJ. In addition, where the company is required to self-report on its compliance program during the term of the agreement (as opposed to where an independent compliance monitor is imposed), the CEO and CCO may also be required to certify that the annual reports submitted by the company during the term are true, accurate, and complete.

That such certifications may be mandated highlights DOJ's recent emphasis on compliance. Indeed, AAG Polite stated that it was his view that requiring these certifications would help to empower CCOs and ensure that they get the support and resources they need to fully remediate and enhance their companies' compliance programs in the wake of discovering misconduct.

Still, it remains unclear whether the AAG's announcement signals a sweeping policy change to be implemented across all resolution agreements, or if his instruction to "consider" requiring such certifications is intended to be done on a case by case basis.

To be sure, under standard agreements with the Criminal Division, CEOs and CFOs are currently required to certify that the company has met its disclosure obligations at the conclusion of the agreement's term. However, the new requirements proposed by AAG Polite would necessarily inject a heightened level of scrutiny into the certification process and would undoubtedly result in more robust discussions between companies and DOJ to ensure that CEOs and CCOs are not making certifications that DOJ would view as false. Moreover, depending on the language that DOJ ultimately rolls out as part of the certification process, and the type of diligence CEOs and CCOs might be required to undertake in order to meet their compliance obligations, these corporate officers may have an increased risk of personal liability. Accordingly, CEOs and CCOs who submit such certifications would be well served by ensuring that there is sufficient supporting documentation before doing so.

In addition to the announcement on compliance certifications, AAG Polite also provided guidance concerning what is expected of companies presenting to DOJ on their compliance program, as well as DOJ's commitment to adding compliance resources to its own ranks.

Potentially new certification requirement

In his speech, AAG Polite stated that he has asked his prosecutors "to consider requiring both the chief executive officer and the chief compliance officer to certify at the end of the term of an agreement that the company's compliance program is reasonably designed and implemented to detect and prevent violations of the law and is functioning effectively."

In addition, AAG Polite said that in certain resolutions where companies are required to provide annual self-reports to DOJ on the state of their compliance programs (as opposed to monitorships, where the monitor is the one submitting annual reports about the company's compliance program), DOJ "will consider requiring the CEO and the CCO to certify that all compliance reports submitted during the term of the resolution are true, that they are accurate, that they are complete."

AAG Polite drew upon his experience as a CCO, stating that he knows the challenges that compliance officers face with resources, relationships, accessing data, and siloing of the compliance function. This is a theme that AAG Polite has emphasized throughout his tenure, and of note, he is the first former CCO to serve as a senior official in the Department.

According to AAG Polite, the purpose of these new conditions is to "empower" CCOs and compliance programs and to ensure "that chief compliance officers receive all relevant compliance-related info and can voice any concerns they may have prior to certification." He also noted his hope that such additional requirements would result in "our chief compliance officers hav[ing] true independence, true authority and true stature within [their] companies."

Although AAG Polite's announcement proposes consideration of a new type of certification by corporate officers at the end of the term of a resolution agreement, DOJ's Criminal Division already requires the CEO and CFO to certify that the company has satisfied its obligation to disclose allegations and evidence of new misconduct. That certification includes an attestation that the CEO and CFO are duly authorized by the company to sign the certification, and that the certification constitutes "a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the Company to the executive branch of the United States for purposes of 18 U.S.C. § 1001." In other words, the certification exposes the corporate officers and the company to a false statements prosecution if it turns out that the company did not disclose certain allegations or evidence of misconduct. The newly proposed certifications have the potential of requiring far more work and scrutiny by CEOs and CCOs, specifically as it relates to the state of their compliance programs.

Additional compliance focus

In addition to discussing the newly proposed compliance certifications, which was by far the most ground-breaking aspect of his speeches, the AAG also provided insight into what DOJ expects of companies when they present on their compliance programs and highlighted that DOJ's Fraud Section will be adding new compliance expertise and resources.

Although DOJ's Evaluation of Corporate Compliance Programs provides a sampling of questions that DOJ asks companies to evaluate compliance program effectiveness, AAG Polite provided additional examples, particularly revolving around culture. For example, "[d]o employees feel empowered to bring issues and questions to the management's attention? Are managers and compliance officers providing ethical advice to salespeople even though such advice may mean loss of business?"

He also emphasized the importance of coming armed with compliance "success stories," including the discipline of poor behavior, the rewarding of positive behavior, the transactions that were rejected due to compliance risk, positive trends in whistleblower reporting, and the partnerships that have developed between compliance officers and the business. Beating a similar drum, the AAG noted the benefit of using data analytics tools to monitor compliance with laws and policies within company operations to ferret out wrongdoing when it occurs.

AAG Polite also addressed expectations around who should be providing compliance presentations to DOJ, and stressed that DOJ would "like to see the Chief Compliance Officer leading [] compliance presentation[s] and demonstrating knowledge and ownership of the compliance program" instead of a "check-the-box presentation from outside counsel." In fact, he noted that "[o]ther senior management should also participate, taking ownership of their role in the compliance program and demonstrating commitment to compliance."

To aid with this heightened focus on compliance, the AAG announced that DOJ has "prioritized . . . dedicating resources to strengthen [its] abilities to assess the effectiveness of compliance programs" beyond those already embedded in the DOJ Fraud Section's Corporate Enforcement, Compliance, and Policy Unit.

Finally, the AAG reiterated a common theme hit by other DOJ officials over the past few months – that DOJ will hold to account companies that breach existing resolution agreements, but that compliance can mitigate bad outcomes. According to AAG Polite, "companies that make a serious investment in improving their compliance programs and internal controls will be viewed in a better light by the Department. Support your compliance team now or pay later."

Takeaways

Emphasizing compliance: These speeches are consistent with recent messaging by DOJ about the importance of compliance. In recent speeches by the Deputy Attorney General and other DOJ officials, there has been consistent messaging concerning their intent to pursue harsher treatment of corporate wrongdoers, but also a standard refrain about the importance of compliance as a mitigating factor. Sending a similar message, DOJ's Fraud Section, which handles all FCPA matters among other significant financial fraud and healthcare fraud cases, continues to hire additional compliance attorneys who are devoted to evaluating companies' compliance programs, a point that AAG Polite reiterated last week. These messages underscore the importance of companies continuing to enhance their compliance programs prior to, and during, any government investigation in order for companies to achieve the best outcome possible with DOJ (as well as the SEC).

Open questions: There remain a number of open questions related to AAG Polite's remarks. Given that he stated he was directing his prosecutors to "consider" requiring this new certification, under what circumstances and in what types of cases will such certifications be required? Will individual prosecutors be given the discretion to decide, or will there be leadership team directives concerning when to apply such requirements? Will mandated certifications contain a similar "penalty of perjury" clause that would subject CEOs and CCOs to personal liability if DOJ disagrees with their conclusion that the program is "reasonably designed and

implemented to detect and prevent violations of the law and is functioning effectively"? What type of diligence would be required of CEOs and CCOs to meet their certification obligations, and what type of guidance would DOJ provide to companies and corporate officers about its view concerning the state of the compliance program? The answers to these questions will be critical in assessing the feasibility of such certifications and whether CEOs and CCOs will be willing to sign them.

An ambiguous concept likely to lead to a robust discussion with DOJ: Unlike the current disclosure certification (which requires the CEO and CFO to certify that the company has disclosed misconduct raised to its attention), the concept of a "reasonably designed and implemented" compliance program that is "functioning effectively" is not at all clear. Indeed, given the wide range of compliance failings that could exist in a company's compliance program, the specific contours of this concept would be largely subjective absent further clarification from DOJ. To avoid being stuck in a "gotcha" moment where CEOs and CCOs risk being prosecuted for false certifications, detailed and clear communications between DOJ and company counsel concerning the nature and extent of the compliance requirements will be necessary prior to a resolution. Moreover, there is a concern that such new requirements would put senior corporate officials in the very difficult position of certifying to something that, in most cases, they do not have direct knowledge of. DOJ could help to address this concern by having a robust discussion with the company at the end of the resolution agreement term, wherein the company provides a detailed download of its compliance program and DOJ, in turn, provides feedback in real time concerning whether they are skeptical of the ability of the CEO and CCO to sign the certification under the circumstances. If the purpose of the certification is, as AAG Polite stated, to ensure that compliance programs are properly resourced and enhanced, this is exactly the type of discussion that DOJ should welcome.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Uzo Asonye
+1 202 962 7057
uzo.asonye@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Daniel S. Kahn
+1 202 962 7140
daniel.kahn@davispolk.com

Tatiana R. Martins
+1 212 450 4085
tatiana.martins@davispolk.com

Fiona R. Moran
+1 202 962 7137
fiona.moran@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Patrick S. Sinclair
+1 212 450 3343
patrick.sinclair@davispolk.com

Davis Polk

Federal court finds company broadly waived privilege by disclosing investigation findings to DOJ

February 18, 2022 | Client Update | 6-minute read

A recent District of New Jersey ruling in the case involving alleged FCPA violations by two former Cognizant executives demonstrates the potential risks of government downloads. Judge Kevin McNulty found that Cognizant broadly waived privilege when it summarized for DOJ the findings of its internal investigation of potential FCPA violations.

On February 1, 2022, Judge Kevin McNulty of the District of New Jersey issued a key ruling on motions related to subpoenas served by two former Cognizant Technology Solutions Corporation (Cognizant) executives on their former employer and its construction partner. The court's ruling is most notable for its finding that Cognizant broadly waived privilege in summarizing the findings of its internal investigation of potential Foreign Corrupt Practices Act (FCPA) violations to the Department of Justice (DOJ). The court's ruling also hit on a number of other relevant issues, finding that Cognizant's communications with its forensic accounting firm about the internal investigation were privileged; finding that draft press releases were not protected; granting discovery requests to allow for a proper assessment of any *Garrity* issues; and granting a motion to quash filed by Cognizant's India-based construction partner, Larsen & Toubro Construction Company, for lack of personal jurisdiction.

Background

Defendants Gordon Coburn and Steven Schwartz, Cognizant's former President and Chief Legal Officer, respectively, were indicted in February 2019 for violating and conspiring to violate the FCPA's anti-bribery and accounting provisions. According to the indictment, between 2014 and 2016, Coburn and Schwartz engaged in a scheme to bribe government officials in India—where more than half of Cognizant's employees worked—to obtain a planning permit needed for construction of an office campus. DOJ issued a declination letter to Cognizant under the FCPA Corporate Enforcement Policy, citing, among other factors, Cognizant's voluntary self-disclosure,

full cooperation, lack of prior criminal history and full remediation. Coburn and Schwartz, meanwhile, await trial. Although trial is currently scheduled to begin next month, the judge indicated it was likely to be continued to October.

The court's ruling follows numerous interrelated motions to compel compliance with and quash the subpoenas issued by the defendants. The defendants argued that Cognizant effected a subject-matter waiver over a broad category of documents when it disclosed a summary of its investigation findings to DOJ. The waiver, they argued, included "any communications regarding conduct alleged in the indictment and any materials related to Cognizant's internal investigation." Cognizant maintained that it did not waive the privilege over the entire internal investigation as the result of simply cooperating with DOJ or disclosing portions of investigative documents.

District of New Jersey's ruling

Subject-matter privilege waiver

Judge McNulty agreed that Cognizant effectuated a subject-matter waiver of privilege. The court observed that Cognizant had made significant disclosures to the government consisting of "detailed accounts of 42 interviews of 19 Cognizant employees, including Defendants." In support of its finding of a waiver, the court explained that "by disclosing this information to the Government while under threat of prosecution, Cognizant handed these materials to a potential adversary and destroyed any confidentiality they may have had, undermining the purpose of both attorney-client and work-product privileges." As authority for its finding, the court cited *In re Chevron Corp.*, which held that "purposeful disclosure of [] purportedly privileged material to a third-party" may waive attorney-client and work product privileges "if that disclosure undermines the purpose behind each privilege." 633 F.3d 153, 165 (3d Cir. 2011).

With regard to the breadth of Cognizant's privilege waiver, Judge McNulty determined it to be "significant," albeit not quite as expansive as the defendants had contended. First, he found that Cognizant had waived its privilege to all memoranda, notes, summaries or other records of interviews to the extent summaries of the interviews had been provided to the government. Second, he ruled that Cognizant had waived its privilege to underlying documents or communications whose content had been directly conveyed through the summaries. Third, he determined Cognizant had waived its privilege to any documents and communications that were reviewed and formed the basis of any presentation to DOJ.

The recent Cognizant ruling follows other findings of privilege waivers. In *U.S. Securities & Exchange Commission v. Sandoval Herrera*, for example, the court ruled that the company had

waived the work product privilege to 12 sets of interview notes and memoranda that had been disclosed to the SEC during an oral download. *See* 324 F.R.D. 258, 267 (S.D. Fla. 2017).

Additional findings

In addition to his findings on the waiver of privilege related to presentations to DOJ, Judge McNulty ruled on privilege questions about draft press releases and Cognizant's communications with accountants. The court found that drafts of press releases, public disclosures and communications with public relations firms were not privileged. It reasoned that such drafts and communications were neither created for the predominant purpose of legal advice nor to prepare for litigation. It also determined that Cognizant maintained its privilege with respect to its communications with its accounting firm concerning the internal investigation and related updates to DOJ and the Securities and Exchange Commission because they were "closely related to the provision of legal advice."

The court further addressed the scope of the defendants' subpoenas and the question of whether it had jurisdiction over the subpoenas issued to Cognizant's India-based construction partner. The defendants were seeking evidence to support the argument that incriminating statements made during their interviews are inadmissible at trial under *Garrity v. New Jersey* because they were made as a result of state action and coercion. *See* 385 U.S. 493, 495-96 (1967). The court agreed with the defendants that Cognizant should expand the time frame for its document search to include material from prior to their interviews in order to properly capture any potential *Garrity* issue. The court also granted Larsen & Toubro Construction Company's motion to quash because it found a lack of specific jurisdiction. The court relied on the absence of any indication that the company's U.S. offices or employees had any contact with the project at issue. It also rejected the defendants' argument that the parent company purposefully availed itself of the forum by cooperating with DOJ's investigation, which the court said, "shows only voluntary cooperation with federal law enforcement, no more and no less."

Key takeaways

The way in which clients manage the production of potentially privileged materials to government authorities in connection with internal investigations continues to implicate significant risk. Although DOJ, as a matter of policy, is prohibited from punishing a company for failing to provide privileged materials, or rewarding a company for producing such materials, prosecutors nevertheless sometimes request materials that courts have determined to be privileged. The Cognizant case is but the most recent example, and a reminder of the collateral consequences of such a waiver. Clients and their counsel should attempt to engage in a productive dialogue with

prosecutors to ensure they secure cooperation credit without exposing the company to a subject-matter waiver in the process.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Uzo Asonye
+1 202 962 7057
uzo.asonye@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Daniel S. Kahn
+1 202 962 7140
daniel.kahn@davispolk.com

Tatiana R. Martins
+1 212 450 4085
tatiana.martins@davispolk.com

Fiona R. Moran
+1 202 962 7137
fiona.moran@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Patrick S. Sinclair
+1 212 450 3343
patrick.sinclair@davispolk.com