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).