FIN-2022-Alert002 March 16, 2022

FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members

Suspicious Activity Report (SAR) filing request:

FinCEN requests financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**FIN-2022-RUSSIALUXURY**"

The Financial Crimes Enforcement Network (FinCEN) is issuing a second[1] alert on the importance of identifying and quickly reporting suspicious transactions[2] involving real estate, luxury goods, and other high-value assets of sanctioned Russian elites and their family members and those through which they act (collectively, "sanctioned Russian elites and their proxies").[3] This alert provides select red flags[4] to assist financial institutions[5] in identifying suspicious transactions, and reminds financial institutions of their Bank Secrecy Act (BSA) reporting obligations. This alert also complements other recent coordinated U.S. Government actions related to luxury goods, and highlights the establishment of U.S. and international task forces and programs designed to freeze and seize the assets of sanctioned Russian actors.[6]

Because real estate, luxury goods, and other high-value assets can be used as a store of value, a medium of exchange, or an investment, sanctioned Russian elites and their proxies may use such assets to evade expansive U.S. and other sanctions and restrictions imposed in response to the

1. *See* FinCEN's first Alert, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," (March 7, 2022) for additional information regarding potential Russian and Belarusian sanctions evasion.
2. *See* 31 U.S.C. § 5318(g); 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
3. Luxury goods can include high-end watches, luxury vehicles, yachts and planes, high-end apparel, high-end alcohol, jewelry, and other goods frequently purchased by Russian elites. *See* White House Fact Sheet, "FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia," (March 11, 2022). Other high-value assets can include physical works of art, precious stones (such as diamonds) and metals (such as gold) among other similar items. *See* U.S. Department of the Treasury (Treasury), "National Money Laundering Risk Assessment," (February 2022), at pp. 58-63.
4. The red flags highlighted in this alert are derived from FinCEN's analysis of Bank Secrecy Act (BSA) reporting or publicly cited sources, and represent only a sampling of indicators of possible sanctions evasion or other illicit activity and should not be considered an exhaustive list. Further, because no single financial red flag 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.
5. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
6. *See* White House "Joint Statement by the G7 Announcing Further Economic Costs on Russia," (March 11, 2022). *See* also U.S. Department of Justice Press Release, "Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture," (March 2, 2022).

Russian Federation's (Russia) invasion of Ukraine.[7] Accordingly, on March 1, 2022, the President announced the U.S. Government's intent to identify and freeze the assets of sanctioned Russian elites and family members, including their yachts, luxury apartments, money, and other ill-gotten gains.[8] The President then signed an Executive Order (E.O.) on March 11, 2022,[9] which among other things, banned the import into the United States of goods from several important sectors of the Russian economy, and prohibits the exportation from the United States or by U.S. persons of certain luxury goods to Russia. In parallel, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued a new round of sanctions targeting Russian and Kremlin elites,[10] and the U.S. Department of Commerce restricted the export of luxury goods to Russia and Belarus, and to certain Russian and Belarusian oligarchs and malign actors located worldwide.[11]

Real Estate

Sanctioned Russian elites and their proxies may seek to evade sanctions through the purchase and sale of commercial or high-end residential real estate.[12] 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. Sanctioned Russian elites and their proxies may purchase or maintain real estate through shell companies or trusts, possibly using funds or assets held in offshore jurisdictions, or may liquidate real estate owned in countries with sanctions against Russia and its elites. FinCEN issued

7. For relevant U.S. Department of the Treasury (Treasury) Office of Foreign Assets Control (OFAC) actions against Russia and the Republic of Belarus, *see* OFAC Recent Actions | U.S. Department of the Treasury. For additional information on compliance with OFAC obligations, *see Summary of Relevant OFAC Compliance Obligations* section of FinCEN's Alert of March 7, 2022 (*supra* Note 1). For relevant U.S. Department of Commerce Bureau of Industry and Security actions, *see* Bureau of Industry and Security | U.S. Department of Commerce. For relevant U.S. Department of State actions, *see* U.S. Department of State. For other relevant U.S. Government measures and actions, *see* The White House.
8. *See* White House, State of the Union Address, (March 1, 2022). *See also*, White House, "FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice," (March 3, 2022).
9. *See* White House, "Executive Order on Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression," (March 11, 2022); White House, "FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia," (March 11, 2022); "Joint Statement by the G7 Announcing Further Economic Costs on Russia," (March 11, 2022).
10. *See* Treasury Press Release, "Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine," (March 11, 2022).
11. *See* U.S. Department of Commerce (Commerce) Press Release, "Commerce Restricts the Export of Luxury Goods to Russia and Belarus and to Russian and Belarusian Oligarchs and Malign Actors in Latest Response to Aggression Against Ukraine," (March 11, 2022). *See also*, Commerce Bureau of Industry and Security, Red Flag Indicators.
12. *See* FinCEN "Advisory to Financial Institutions and Real Estate Firms and Professionals," (August 22, 2017) and Treasury, "National Money Laundering Risk Assessment," (February 2022), at pp. 58-61. *See also*, FinCEN "Advanced Notice of Proposed Rulemaking (ANPRM) on Anti-Money Laundering Regulations for Real Estate Transactions," 86 FR 69589 (December 8, 2021), at pp. 69590 and 69596; and FinCEN Assessment, "Money Laundering in the Commercial Real Estate Industry," (December 2006).

renewed and expanded Geographic Targeting Order (GTO)[13] requirements in high-risk U.S. locations that often see significant real estate money laundering activity.[14]

Select Red Flags

1. The purchase, sale, donation, or legal ownership transfer of high-value real estate in the name of a foreign legal entity, shell company, or trust, especially if the transaction: (i) is far above or below fair market value, (ii) involves all-cash transfers, or (iii) is funded by a third party with a known nexus to sanctioned Russian elites and their proxies.
2. The use of legal entities or arrangements that may have a nexus to sanctioned Russian elites and their proxies to hide the ultimate beneficiary or the origins or source of the funds.
3. Changes, without an apparent business reason, to the transaction patterns of a firm located in a country other than the United States, Russia, Belarus, and Ukraine, where the new transactions involve convertible virtual currency and Russian-related investments or firms.
4. A Russian individual or entity requests a wire transfer from a non-U.S. (particularly non-Russian) bank to pay for an all-cash purchase, especially if the wired funds come from an account held by an individual or entity other than the original requestor.
5. The dilution of equitable interest held in real property by sanctioned Russian elites and their proxies, by the addition of, or the transfer of real estate to, an individual not affiliated with the buyer or seller.
6. The maintenance, purchase, or termination of real estate insurance by persons with a known nexus to sanctioned Russian elites and their proxies.

13. The Director of FinCEN may issue an order that imposes certain additional recordkeeping and reporting requirements on one or more domestic financial institutions or nonfinancial trades or businesses in a geographic area. 31 U.S.C. § 5326(a); 31 CFR § 1010.370; and Treasury Order 180-01 (July 1, 2014). *See also* FinCEN Press Release, "FinCEN Renews Real Estate Geographic Targeting Orders for 12 Metropolitan Areas," (October 29, 2021). The GTOs require U.S. title insurance companies to identify the natural persons behind shell companies used in all-cash purchases of residential real estate over $300,000 in several U.S. metropolitan areas.
14. *See* Treasury, "National Money Laundering Risk Assessment," (February 2022), at p. 59.

Artworks

Several qualities inherent to art, the high-value art market, and market participants may make the art market[15] attractive for money laundering by illicit actors, including sanctioned Russian elites.[16] Shell companies and intermediaries are frequently used to purchase, hold, or sell artworks, as well as to remit and receive payments, allowing sanctioned persons to obscure their identities and hide their activity.[17] The mobility, concealability, and subjective value of artwork further exacerbate its vulnerability to sanctions evasion.

Select Red Flags

7. The use of shell companies and trusts, and/or third-party intermediaries, including art dealers, brokers, advisers, or interior designers, with a nexus to sanctioned Russian elites and their proxies, to purchase, hold, or sell art on a client's behalf.

8. Transactions involving sanctioned Russian elites and their proxies, and large amounts of cash, especially in currencies not typically used in the art market.

9. Artwork-related transactions involving persons with suspected ties to sanctioned Russian elites and their proxies who (i) are not concerned with recouping their initial investment or paying a substantially higher price than the notational value of the work, and/or (ii) conduct transactions that exceed the expected sales value of the work.

10. The purchase, maintenance, or termination of insurance policies to protect the market value or provide cash payments for the loss, theft, or destruction of privately held or donated high-value artwork linked to sanctioned Russian elites and their proxies.

Precious Metals, Stones, and Jewelry (PMSJs)

Dealers in PMSJs, such as gold and diamonds, are advised that sanctioned Russian elites and their proxies may attempt to use PMSJs to evade sanctions. In addition to being valued for a variety of legitimate industrial, personal consumption, and investment purposes, PMSJs are portable, highly

15. The art market includes auction houses, art galleries, online marketplaces and social media sites, certain non-profits, art finance service providers, and art storage facilities. *See* Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," (February 4, 2022), at pp. 11-19.
16. *See* Treasury, "National Money Laundering Risk Assessment," (February 2022), at pp. 58-63. *See also*, FinCEN, "FinCEN Informs Financial Institutions of Efforts Related to Trade in Antiquities and Art," (March 9, 2021); Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," (February 4, 2022), and OFAC, "Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork," (October 30, 2020). For a case study documenting how certain Russian elites appear to have used transactions involving high-value art to evade sanctions imposed on them by the United States in response to Russia's 2014 invasion of Ukraine and annexation of Crimea, *see* United States Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, "The Art Industry and U.S. Policies that Undermine Sanctions," (July 29, 2020).
17. *See* OFAC, "Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork," (October 30, 2020).

valuable, and practical replacements for currency, making them ideal for concealing illicit wealth without increased scrutiny, because the underlying commodity is legal.[18]

As Russia is a major exporter of many of these materials, including diamonds and gold, sanctioned Russian elites and their proxies also may attempt to evade trade restrictions[19] on PMSJs to obtain needed currency or funds. On February 24, 2022, OFAC expanded Russia-related debt and equity restrictions to additional key aspects of Russia's economy, including applying them to the Russian diamond mining company Alrosa, the world's largest diamond mining company and responsible for 90 percent of Russia's diamond mining capacity.[20]

Select Red Flags

11 Transactions involving PMSJ trading companies, particularly in Asia, and firms with a nexus to sanctioned Russian elites and their proxies.

12 High-value or frequent transactions involving mining operations with opaque and complex corporate structures, that are or have been owned or controlled by sanctioned Russian elites or their proxies.

Other High-Value Assets

Sanctioned Russian elites and their proxies are known to purchase or sell other high-value assets, such as luxury yachts and vehicles. U.S. sanctions regulations block property of sanctioned Russian elites, and such property may also be subject to European sanctions. As a result, enforcement of sanctions against such property is an important U.S. priority, and violations of sanctions will be aggressively enforced. Over the past several weeks, various European governments, consistent with their sanctions regimes and legal frameworks, have made high-profile seizures of luxury yachts owned by sanctioned Russian elites, such as Alisher Usmanov.[21] Usmanov is one of Russia's wealthiest billionaires with vast holdings across multiple sectors of the Russian economy as well as

18. *See* Treasury, "National Money Laundering Risk Assessment," at p. 61; *see also* FinCEN, "Financial Threat Analysis: Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data," noting that "[p]ayments for wildlife shipping can be masked as payment to gold, diamonds, or precious metals dealers or to precious metal trading business [. . .] [and that] gold, diamonds, and other precious metals might be used to facilitate payment as trade for wildlife or to conceal proceeds of wildlife trafficking," (December 20, 2021), at p. 12, and FinCEN, "FinCEN Calls Attention to Environmental Crimes and Related Financial Activity," noting that illegal mining often involves extraction of various metals, stones, and materials, including gold, silver, iron, coal, diamonds, emeralds, and rare earths, in violation of the law, and is often associated with other crimes or criminal groups, (November 18, 2021), at p. 7.
19. *See* White House Press Release, "FACT SHEET: United States, European Union, and G7 to Announce Further Economic Costs on Russia," (March 11, 2022). The President's Executive Order of March 11, 2022, prohibits the import of non-industrial diamonds into the United States.
20. *See* Treasury Press Release, "U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs," (February 24, 2022).
21. *See, e.g.*, White House, "FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice," (March 3, 2022).

internationally.[22] On March 3, 2022, OFAC sanctioned Usmanov, among other targets, and blocked his yacht and aircraft.[23] Similarly, on March 11, 2022, OFAC re-designated Viktor Feliksovich Vekselberg and identified his yacht and aircraft as blocked property.[24] Vekselberg is a prominent Russian businessman with an estimated net worth exceeding $6 billion who has maintained close ties with leading Russian Government officials, including Russian President Vladimir Putin and former Russian President Dmitry Medvedev.[25]

Select Red Flags

13. The sudden transfer, including through sales, by sanctioned Russian elites and their proxies of ownership in high-value assets and goods.

14. The involvement of legal entities, such as shell companies, with a nexus to sanctioned Russian elites and their proxies, that are falsely posing as well-known entities and operating in jurisdictions other than the well-known entity's jurisdiction and geographic sphere of business.

15. The involvement of a common set of (i) financial institutions, (ii) individuals, or (iii) addresses to facilitate luxury goods-related transactions, that may have a nexus to sanctioned Russian elites and their proxies.

16. The involvement of law firms based in global and offshore financial centers that have historically specialized in Russian clientele or in transactions associated with sanctioned Russian elites and their proxies.

17. The involvement of transportation service companies that have been owned by, or have a nexus to, sanctioned Russian elites and their proxies, and that may be used to transport luxury goods and obfuscate their movement.

22. *See* Treasury Press Release, "Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors," (March 3, 2022). *See also*, White House, "FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice," (March 3, 2022).
23. *Id*. As a result, U.S. persons are generally prohibited from engaging in any transactions related to Usmanov, his property, or any entity owned 50 percent or more by Usmanov, unless authorized or exempt; this includes engaging in transactions or activities involving Usmanov's yacht or aircraft, such as maintenance, the hiring of operating personnel, or payment of docking or landing fees.
24. *See* Treasury Press Release, "Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine," (March 11, 2022).
25. *See* Treasury Press Release, "Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity," (April 6, 2018). *See also* Treasury Press Release, "Treasury Sanctions Kremlin Elites, Leaders, Oligarchs, and Family for Enabling Putin's War Against Ukraine," (March 11, 2022).

U.S. and International Efforts to Identify, Freeze, and Seize Assets Belonging to Sanctioned Russian Elites and Their Proxies

The U.S. Government and its partners and allies have established international and domestic task forces dedicated to identifying blocked assets as well as enforcing sanctions, export restrictions, and economic pressure measures imposed by the United States and our partners and allies.

Russian Elites, Proxies, and Oligarchs (REPO) Task Force

On March 16, 2022, the U.S. Department of the Treasury and the U.S. Department of Justice launched the multinational Russian Elites, Proxies, and Oligarchs (REPO) Task Force with counterparts from Australia, Canada, the European Commission, France, Germany, Italy, Japan, and the United Kingdom.[26] The initial concept of the REPO Task Force was announced on February 26, 2022, to ensure the effective implementation of those jurisdictions' Russia-related sanctions.[27] The REPO Task Force is intended to share information to take concrete actions, including sanctions, asset freezing, and civil and criminal asset seizure, and criminal prosecution.

Task Force KleptoCapture

Additionally, on March 2, 2022, the Attorney General announced the formation of Task Force "KleptoCapture". Task Force KleptoCapture is an interagency U.S. law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions, and economic countermeasures that the United States has imposed, along with allies and partners, in response to Russia's unprovoked military invasion of Ukraine.[28]

Kleptocracy Asset Recovery Rewards Program

Lastly, in conjunction with this Alert, the Department of the Treasury announced the launch of the Kleptocracy Asset Recovery Rewards Program.[29] The rewards program supports U.S. Government programs and investigations aimed at restraining, seizing, forfeiting, or repatriating stolen assets linked to foreign government corruption and the proceeds of such corruption. The program's initial rewards will target the recovery of assets stolen by elites and their associates linked to the Russian Government.

26. *See* Treasury and U.S. Department of Justice Press Release, "U.S. Departments of Treasury and Justice Launch Multilateral Russian Oligarch Task Force," (March 16, 2022).
27. *See* White House, "Joint Statement on Further Restrictive Economic Measures," (February 26, 2022).
28. *See* Justice Press Release, "Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture," (March 2, 2022).
29. *See* Section 9703 of William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283. The statute authorizes the Secretary of the Treasury and the Attorney General, in consultation with relevant Federal departments and agencies, to pay a reward to qualified individuals for information leading to the restraining, seizure, forfeiture or repatriation of stolen assets linked to foreign government corruption held at U.S. financial institutions or that come within the United States or within the possession or control of any U.S. persons. *See* Teasury, "Kleptocracy Asset Recovery Rewards Program," (March 16, 2022).

Kleptocracy Asset Recovery Initiative

The Department of Justice also has the Kleptocracy Asset Recovery Initiative which the U.S. Government uses to identify, seize, and recover the assets of kleptocrats and other corrupt individuals.[30]

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.[31] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[32]

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.[33] 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.[34] 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

30. 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).
31. *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.
32. *See* 31 U.S.C. § 5318(g)(3).
33. *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), 1030.320(d).
34. *Id*. *See also* FinCEN, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or Anti-Money Laundering (AML) 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[35] 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 **"FIN-2022- RUSSIALUXURY"** 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.

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).[36]

35. *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," (April 2005), at pp. 38-40, 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."
36. 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.

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.[37]

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.[38] These include obligations related to the Currency Transaction Report (CTR),[39] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[40] Report of Foreign Bank and Financial Accounts (FBAR),[41] Report of International Transportation of Currency or Monetary Instruments (CMIR),[42] Registration of Money Service Business (RMSB),[43] and Designation of Exempt Person (DOEP).[44] These standard reporting requirements may not have an obvious connection to Russia-related illicit finance, but may ultimately prove highly useful to law enforcement.

37. *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), 1030.320(d)(1)(ii)(A)(2).
38. 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).
39. 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.
40. 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 and 31 CFR § 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
41. 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.
42. 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.
43. 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.
44. 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.

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 **"FIN-2022-RUSSIALUXURY"** 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.[45]

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.[46] 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.[47]

General obligations for correspondent account due diligence and AML 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 program obligations under 31 U.S.C. § 5318(h) and its implementing regulations (which apply to all U.S. financial institutions).[48] 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

45. *See* 31 CFR § 1010.620(c).
46. *See* 31 CFR § 1010.230.
47. *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).
48. *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.

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.[49]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving sanctions evasion, ransomware/cyber attacks, and laundering of the proceeds of corruption. 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.[50] FinCEN strongly encourages such voluntary information sharing.

For Further Information

Questions or comments regarding the contents of this alert should be sent to the FinCEN Regulatory Support Section at frc@fincen.gov.

49. *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).
50. For further guidance related to the 314(b) Program, *see* FinCEN, "Section 314(b) Fact Sheet," December 20, 2020.