



# FINANCIAL INTELLIGENCE AUTHORITY

P. O. Box GM 959  
Gablewoods Mall Post Office  
Sunny Acres  
Castries  
St. Lucia, W.I.

Tel: (758) 451-7126  
Fax: (758) 453-6199  
E-mail: slufia@candw.lc

---

---

## Circular No. 001/2023

Date: May 9, 2023

To: All Reporting Entities

Re: FinCEN Alerts Regarding Real Estate Investment by Russian Elites, Oligarchs and their Proxies.

The Financial Crimes Enforcement Network (FinCEN) of the USA has recently issued an advisory which highlights the sanctions evasion-related risks posed by sanctioned Russian elites and their proxies, and their illicit investments in the US commercial real estate sector.

The Financial Intelligence Authority (FIA) recognizes that the misuse of real estate investments by Russian actors could extend beyond US borders and into our local real estate market. We therefore find it prudent to share this FinCEN advisory to alert you of the heightened risk to which your entity may be exposed.

As such, you are reminded of your statutory obligations to develop and implement appropriate policies, procedures and internal controls for the purpose of detecting and preventing your entity from being used to facilitate money laundering and other financial crime.

Please be guided accordingly.

Yours Sincerely,

.....  
**Paul Thompson**  
**Director**



# FinCEN

# ALERT

FIN-2023-Alert002

January 25, 2023

## FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies

The Financial Crimes Enforcement Network (FinCEN) is issuing this alert to all financial institutions<sup>1</sup> regarding potential investments in the U.S. commercial real estate (CRE) sector by sanctioned Russian elites, oligarchs, their family members, and the entities through which they act (collectively, “sanctioned Russian elites and their proxies”).<sup>2</sup> In March 2022, FinCEN issued an alert on the risk of sanctions evasion by sanctioned Russian elites and their proxies involving high-value assets, including both residential and commercial real estate.<sup>3</sup> This alert specifically highlights sanctions evasion-related vulnerabilities in the CRE sector and is based on a review of Bank Secrecy Act (BSA) reporting indicating that sanctioned Russian elites and their proxies may exploit them to evade sanctions.<sup>4</sup>

### 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-2023-RUSSIACRE**”.

1. See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. Here “commercial real estate” refers to property that is used for investment or income-generating purposes rather than as a residence by the owner. While this definition covers properties typically thought of as “commercial” (office buildings, retail stores, hotels, etc.), multifamily housing such as apartment buildings also qualify as commercial real estate under this definition. See Congressional Research Service, “[COVID-19 and the Future of Commercial Real Estate Finance](#),” Oct. 19, 2020, at pp. 1-2. FinCEN has previously defined residential real estate as “real property (including individual units of condominiums and cooperatives) designed principally for the occupancy of from one to four families.” See FinCEN, “[Frequently Asked Questions: Geographic Targeting Orders Involving Certain Real Estate Transactions](#),” Oct. 26, 2022.
3. See FinCEN, “[FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members](#),” Mar. 16, 2022 (“Luxury Goods Alert”).
4. FinCEN has been following money laundering and illicit finance risks in the CRE market for many years and issued a report on CRE-related Suspicious Activity Reports as early as 2006. See FinCEN, “[Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis](#),” Dec. 2006. See also FinCEN, “[Commercial Real Estate Financing Fraud: Suspicious Activity Reports by Depository Institutions January 1, 2007-December 31, 2010](#),” Mar. 2011. In 2021, FinCEN issued an advance notice of proposed rulemaking seeking comment on potential regulations to address money laundering and illicit finance risks in real estate, including in the CRE market. See FinCEN, “[Advance Notice of Proposed Rulemaking \(ANPRM\) on Anti-Money Laundering Regulations for Real Estate Transactions](#),” 86 Fed. Reg. 69589, 69594 Dec. 8, 2021 (“Real Estate ANPRM”). Further, recent civil forfeiture complaints by the U.S. Department of Justice have also highlighted the risks of money laundering and illicit finance in the CRE sector. See, e.g., U.S. Department of Justice, “[United States Files Civil Forfeiture Complaint for Proceeds of Alleged Fraud and Theft from PrivatBank in Ukraine](#),” Jan. 20, 2022 (“Civil Forfeiture Complaint”). As these cases have demonstrated, vulnerable parts of this market include not only luxury or high-end CRE properties in large cities, but also CRE properties used for a variety of common uses and which may be located throughout the United States.

Further, and in light of Russia’s continuing war of aggression against Ukraine, this alert is part of a sustained effort by FinCEN to urge financial institutions to remain vigilant in identifying and promptly reporting suspected sanctions evasion by sanctioned Russian elites and their proxies.<sup>5</sup> The U.S. Department of the Treasury, acting through the Office of Foreign Assets Control (OFAC), has imposed wide-ranging sanctions on certain Russian elites, their proxies, and others who have provided support for Russia’s brutal war in Ukraine.<sup>6</sup> As such, the alert complements ongoing U.S. government efforts to isolate sanctioned Russian persons from the international financial system. It is also part of a broader effort by the Department of the Treasury to effectively implement the U.S. Strategy on Countering Corruption by seeking to increase transparency in U.S. real estate transactions and prevent corrupt elites and other illicit actors from hiding their ill-gotten wealth in the U.S. real estate market.<sup>7</sup>

This alert provides financial institutions with guidance on identifying potential sanctions evasion activity in the CRE sector by providing potential red flags and typologies related to this activity. It also reminds financial institutions of their BSA reporting obligations and, for certain institutions, their customer due diligence (CDD) obligations. FinCEN has derived the typologies and red flags below from its analysis of BSA data, open-source reporting, and information from law enforcement partners.

## **Sanctions Evasion Risks and Vulnerabilities in the Commercial Real Estate Market**

FinCEN assesses that sanctioned Russian elites and their proxies are likely attempting to exploit several vulnerabilities in the CRE market in order to evade sanctions. The CRE market presents unique challenges for financial institutions in detecting sanctions evasion. First, CRE transactions routinely involve highly complex financing methods and opaque ownership structures that can make it relatively easy for bad actors to hide illicit funds in CRE investments. For example, CRE transactions nearly always involve private companies or institutional investors as the buyer and/or seller. As such, trusts, shell companies, pooled investment vehicles, or other legal entities are regularly used on both sides of CRE transactions. The standard use of such legal entities in CRE deals is typically due to the high value of the properties (ranging from the low millions of dollars to the billions of dollars) and the need for buyers and sellers to limit their legal, tax, and financial liability. In addition, several layers of legal entities are frequently involved as CRE buyers or

- 
5. See FinCEN, [“FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts,”](#) Mar. 7, 2022, for additional information regarding potential Russian sanctions evasion. See also Luxury Goods Alert, *supra* footnote 3 and FinCEN and the U.S. Department of Commerce, [“FinCEN and the U.S. Department of Commerce’s Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts,”](#) June 28, 2022.
  6. For a list of sanctioned Russian elites and their proxies, see U.S. Department of the Treasury, Office of Foreign Assets Control, Sanctions Programs and Information, [Sanctions List Updates](#).
  7. See White House, [U.S. Strategy on Countering Corruption](#), Dec. 2021, at p. 22. FinCEN has also issued, renewed, and expanded geographic targeting orders (GTOs) related to real estate in certain counties of the United States. See, e.g., FinCEN Press Release, [“FinCEN Renews and Expands Real Estate Geographic Targeting Orders,”](#) Oct. 26, 2022; see also FinCEN, [“Advisory to Financial Institutions and Real Estate Firms and Professionals,”](#) Aug. 22, 2017.

sellers, and they may be domiciled in offshore jurisdictions. Further, these legal entities often have a large number of investors behind them and, as a result, it can be difficult for a financial institution to identify all of the beneficial owners. As discussed further below and based on BSA reporting, sanctioned Russian elites and their proxies may seek to further obfuscate their involvement in a CRE transaction by decreasing their percentage of ownership in an investment below the threshold set by a bank’s CDD protocols.

Other features of CRE present opportunities for those engaged in illicit finance schemes, including sanctioned Russian elites and their proxies. For instance, the relative stability of the CRE market and the high value of CRE properties provide them with an easy way to store large amounts of wealth.<sup>8</sup> In addition, there is the potential for steady income that CRE properties can generate for their owners.

Foreign investors also make up a large percentage of U.S. CRE transactions. The lack of transparency in the CRE market and the stability of returns in this market may have attracted a significant number of illicit actors among those foreign investors in recent years, including sanctioned Russian elites and their proxies. According to one study of 2021 U.S. CRE transactions, 8.4 percent of those surveyed reported that they closed a sale with a foreign client residing abroad, and this figure was above 10 percent for several years prior to the pandemic.<sup>9</sup>

Some features of the CRE market discussed here are generally based on legitimate business decisions, but they can make it challenging for financial institutions to identify the underlying source or sources of funds and whether politically exposed persons (PEPs) or corrupt elites are involved.<sup>10</sup> For instance, since the use of multiple legal entities is common in CRE transactions, financial institutions should not underestimate the potential for this practice to be part a larger scheme of illicit financial activity such as sanctions evasion.

---

8. As noted in the 2022 National Money Laundering Risk Assessment, money laundering and terrorist financing risks “are compounded in transactions involving commercial real estate, as there are additional types of purchasing options and financing arrangements available for parties seeking to build or acquire property worth hundreds of millions of dollars.” U.S. Department of the Treasury, [“National Money Laundering Risk Assessment,”](#) Feb. 2022, at p. 58.

9. See National Association of REALTORS® (NAR), [“Commercial Real Estate International Business Trends,”](#) Feb. 2022. The survey responses included 1,200 NAR commercial members.

10. As prior guidance for banks from FinCEN and the federal bank regulators has stated, the term “politically exposed person” excludes U.S. public officials and refers to “foreign individuals who are or have been entrusted with a prominent public function, as well as their immediate family members and close associates. By virtue of this public position or relationship, these individuals may present a higher risk that their funds may be the proceeds of corruption or other illicit activity.” See FinCEN and Federal Banking Agencies, [“Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons,”](#) Aug. 21, 2020. The guidance clarifies that PEPs should not automatically be viewed as higher risk and the level of risk varies. Accordingly, “the level and type of CDD should be commensurate with the risks presented by the PEP relationship” and consistent with the financial institution taking a risk-based approach to BSA compliance.



## Typologies Associated with Possible Money Laundering and Sanctions Evasion in the CRE Market

FinCEN has identified methods of potential sanctions evasion in the CRE market that sanctioned Russian elites and their proxies may be exploiting. These typologies and the red flag indicators in the following section represent only a sampling of typologies and indicators of possible sanctions evasion or other illicit activity. They should not be considered an exhaustive list. Moreover, financial institutions should be aware that other bad actors engaged in various types of illicit financial activity, such as money laundering, may use these or other methods to invest in CRE.<sup>11</sup>

### *The Use of Pooled Investment Vehicles in CRE*

CRE investors seeking to evade sanctions, including sanctioned Russian elites and their proxies, may use pooled investment vehicles,<sup>12</sup> including offshore funds, in order to avoid CDD and beneficial ownership protocols established by financial institutions, thereby allowing them to evade detection.<sup>13</sup> In many cases, owing to the number of investors involved in a fund, an individual investor will own less than 25 percent of the fund and their ownership interest will therefore fall below the threshold for beneficial ownership screening by banks that work with funds in CRE financing.<sup>14</sup> Even if banks lower their threshold below 25 percent to 10 percent, which is common with respect to financial institutions' CDD requirements for high-risk customers, investors seeking to evade sanctions may lower their interest in a fund to just below that threshold to avoid the bank's detection. These investors may in fact be general partners that have actual control of the fund, but their ownership interest will fall under a bank's bespoke CDD ownership threshold.

- 
11. In one of the most prominent cases, Ihor Kolomoisky and Gennadiy Boholiubov, who owned PrivatBank, one of Ukraine's largest banks, allegedly embezzled and defrauded the bank of billions of dollars and used anonymous shell companies to launder the misappropriated funds into CRE and businesses across the United States. *See* Civil Forfeiture Complaint, *supra* footnote 4.
  12. For purposes of this alert, the term "pooled investment vehicle" refers to a broader range of entities than those covered under the definition provided by 31 CFR § 1010.380(f)(7) (effective Jan. 1, 2024) which provides a definition of "pooled investment vehicle" as either: (i) an investment company under section 3(a) of the Investment Company Act of 1940, or (ii) a company not covered by such definition due to the exclusions in sections 3(c)(1) or 3(c)(7) and that are identified (or will be identified) by name on the Form ADV that its investment adviser files with the Securities and Exchange Commission (SEC). According to the SEC, a pooled investment vehicle is "an entity—often referred to as a fund—that an adviser creates to pool money from multiple investors. Each investor makes an investment in the fund by purchasing an interest in the fund entity, and the adviser uses that money to make investments on behalf of the fund. Investors generally share in the profits and losses in proportion to their interest in the fund." *See* SEC, "[The Jargon from A to Z](#)."
  13. Although many pooled investment vehicles are exempted under the CDD regulations, pooled investment vehicles are not excluded categorically from all aspects of 31 CFR 1010.230. Coverage will depend to a significant extent on who manages or advises the vehicle and whether the vehicle is registered as a security on a public exchange.
  14. Pursuant to the CDD Rule, a beneficial owner includes any individual owning, directly or indirectly, 25 percent or more of the equity interests of a legal entity customer. *See* 31 CFR § 1010.230(d)(1).

### *The Role of Shell Companies and Trusts*

Sanctioned Russian elites and their proxies may use shell companies<sup>15</sup> and trusts, whether based in the United States or in other jurisdictions, in order to conceal their ownership stake in a CRE property. Particularly in high-value CRE properties, many layers of legal entities and trusts may be involved, and they may be spread across multiple jurisdictions around the world. These features can make it difficult for BSA-regulated financial institutions to identify the beneficial owners of these entities.<sup>16</sup> Furthermore, legitimate businesses (*e.g.*, real estate development or asset management companies) will also frequently, even if unwittingly, be part of CRE ownership structures involved in a sanctions evasion scheme, creating an additional challenge for financial institutions in identifying the bad actors.

### *The Involvement of Third Parties*

The use of third parties to invest in CRE on behalf of a criminal or corrupt actor is a common tactic for laundering money and engaging in other illicit finance schemes in the CRE space. Sanctioned Russian elites and their proxies may use relatives, friends, or business associates to set up the legal entities to invest in CRE projects, or they may create trusts through which to invest in the properties and to hold the assets. When analyzing trusts for which a sanctioned person was at any time the grantor/settlor, trust protector, trustee, or beneficiary, financial institutions should take particular care to ensure that sanctioned persons do not have a present, future, or contingent property interest in the trust.<sup>17</sup>

### *Inconspicuous CRE Investments That Provide Stable Returns*

Sanctioned Russian elites and their proxies also may seek to avoid detection by investing in CRE projects that are less likely to be noticed by the general public or that would potentially draw unwanted attention. These CRE projects can vary tremendously in kind, but they need not be high-end or luxury properties and could include CRE in the multifamily housing, retail, office, industrial, or hotel sectors. In many cases, sanctions evaders may seek out inconspicuous investments so long as they provide stable returns.

Furthermore, there are no central geographic hubs where sanctioned Russian elites and their proxies may be focusing their U.S. CRE investments. As a result, it is just as likely that attempted sanctions evasion is occurring in the CRE markets in small- to mid-size urban centers and throughout the United States as it is to take place in the largest cities.

---

15. FinCEN's recently issued final rule on beneficial ownership reporting requirements, which implements part of the Corporate Transparency Act, notes that "[s]hell companies are typically non-publicly traded corporations, limited liability companies, or other types of entities that have no physical presence beyond a mailing address, generate little to no independent economic value, and generally are created without disclosing their beneficial owners." See FinCEN, [Beneficial Ownership Information Reporting Requirements](#), 87 Fed. Reg. 59,501 (Sept. 30, 2022).

16. The final rule on beneficial ownership reporting is designed to enhance the transparency of such entities. This rule applies to both domestic corporate entities and foreign corporate entities that are registered to do business in the United States. See *id.* at 59,498.

17. Here "property interest" has the same meaning as that provided in the definition at 31 CFR § 589.331.

## The Role of Financial Institutions in CRE Transactions

Various types of financial institutions with regulatory obligations under the BSA are involved in CRE transactions and should apply a risk-based approach to identifying and reporting potential sanctions evasion by sanctioned Russian elites and their proxies. For example, banks<sup>18</sup> frequently work with market participants that are seeking financing for CRE projects, including developers, private investment vehicles, and various other types of companies.<sup>19</sup> Banks are also one of the BSA-regulated financial institutions with CDD obligations, requiring them to verify the beneficial owners of legal entity customers.<sup>20</sup> Banks therefore may be in a position to identify and report suspicious activities associated with sanctioned Russian elites and their proxies including PEPs, among banks' CRE-related customers.

Insurance companies are another type of financial institution with obligations under the BSA,<sup>21</sup> and they play a significant role in CRE financing. At year-end 2021, insurers held \$556.7 billion in CRE debt.<sup>22</sup> Insurance companies may in some cases be in a position to determine whether their CRE-related activities have exposure to sanctioned Russian elites and their proxies.

Furthermore, the CRE market frequently involves loan syndication, which may include banks, life insurers, and other types of BSA-regulated financial institutions. As noted at the end of this alert, Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another on suspected money laundering or terrorist activities under a safe harbor that offers protections from liability.<sup>23</sup> FinCEN strongly encourages this information sharing to occur with respect to potential CRE-related sanctions evasion by sanctioned Russian elites and their proxies, including during the process in which loans are developed and structured.<sup>24</sup>

---

18. See 31 CFR § 1010.100(d).

19. A 2019 study found that banks and thrifts held 39 percent of outstanding CRE debt. See Congressional Research Service, "[COVID-19 and the Future of Commercial Real Estate Finance](#)," Oct. 19, 2020.

20. See 31 CFR § 1010.230(f).

21. See 31 CFR Part 1025.










22. See National Association of Insurance Commissioners, "[Capital Markets Special Report](#)," Aug. 5, 2022.

23. See FinCEN, "[Section 314\(b\) Fact Sheet](#)," Dec. 2020.

24. Even if a bank or other financial institution does not participate in voluntary information sharing under Section 314(b), financial institutions must adhere to their obligations under the BSA and, if appropriate, report suspected sanctions evasion or other illicit activity discovered in the CRE loan syndication process.

## Financial Red Flags Involving Commercial Real Estate

Financial institutions should be vigilant in monitoring, detecting, and reporting suspicious activity that may be indicative of sanctions evasion in the CRE market. As part of this effort, FinCEN encourages financial institutions to consider the following red flags. Since 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 The use of a private investment vehicle that is based offshore to purchase CRE and that includes PEPs or other foreign nationals (particularly family members or close associates of sanctioned Russian elites and their proxies) as investors.
-  2 When asked questions about the ultimate beneficial owners or controllers of a legal entity or arrangement, customers decline to provide information.
-  3 Multiple limited liability companies, corporations, partnerships, or trusts are involved in a transaction with ties to sanctioned Russian elites and their proxies, and the entities have slight name variations.
-  4 The use of legal entities or arrangements, such as trusts, to purchase CRE that involves friends, associates, family members, or others with a close connection to sanctioned Russian elites and their proxies.
-  5 Ownership of CRE through legal entities in multiple jurisdictions (often involving a trust based outside the United States) without a clear business purpose.
-  6 Transfers of assets from a PEP or Russian elite to a family member, business associate, or associated trust in close temporal proximity to a legal event such as an arrest or an OFAC designation.
-  7 Implementation of legal instruments (*e.g.*, deeds of exclusion) that are intended to transfer an interest in CRE from a PEP or Russian elite to a family member, business associate, or associated trust following a legal event such as an arrest or an OFAC designation of that person.
-  8 Private investment funds or other companies that submit revised ownership disclosures to financial institutions showing sanctioned individuals or PEPs that previously owned more than 50 percent of a fund changing their ownership to less than 50 percent.
-  9 There is limited discernable business value in the CRE investment or the investment is outside of the client's normal business operations.



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

*Suspicious Activity Reporting*

*Other Relevant BSA Reporting*

*USA PATRIOT ACT Section 314(b) Information Sharing Authority*

### Suspicious Activity Reporting

A financial institution is required to file a Suspicious Activity Report (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; is intended or conducted 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.<sup>25</sup> All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.<sup>26</sup>

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.<sup>27</sup> 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.<sup>28</sup> 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 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.

### SAR Filing Instructions

FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this alert by including the key term "**FIN-2023-RUSSIACRE**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

25. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

26. See 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

27. 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).

28. *Id.* See also FinCEN, "[Suspicious Activity Report Supporting Documentation](#)," June 13, 2007.

*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).<sup>29</sup>*

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.<sup>30</sup>

### **Other Relevant BSA Reporting Requirements**

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements to provide information in connection with the subject of this alert. These include obligations related to the Currency Transaction Report (CTR),<sup>31</sup> Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),<sup>32</sup> Report of Foreign Bank and Financial Accounts (FBAR),<sup>33</sup> Report of International Transportation of Currency or Monetary Instruments (CMIR),<sup>34</sup> Registration of Money Services Business (RMSB),<sup>35</sup> and Designation of Exempt Person (DOEP).<sup>36</sup> These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

- 
29. 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.
30. 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).
31. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than \$10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. See 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
32. A report filed by a trade or business that receives currency in excess \$10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/IRS form when not otherwise required to be reported on a CTR. See 31 CFR § 1010.330; 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.
33. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding \$10,000 at any time during the calendar year. See 31 CFR § 1010.350; FinCEN Form 114.
34. A form filed to report the transportation of more than \$10,000 in currency or other monetary instruments into or out of the United States. See 31 CFR § 1010.340.
35. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. See 31 CFR § 1022.380.
36. A report filed by banks to exempt certain customers from currency transaction reporting requirements. See 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-2023-RUSSIACRE” in the “Comments” section of the report.

### Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.<sup>37</sup> Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.<sup>38</sup> Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign PEPs.

#### *Senior foreign political figures and due diligence obligations for private banking accounts*

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.<sup>39</sup> Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.<sup>40</sup>

37. See 31 CFR § 1020.210(b)(5), 1023.210(b)(5), 1024.210(b)(4), and 1026.210(b)(5).

38. See 31 CFR § 1010.230; 31 CFR § 1010.650(e)(1) (defining “covered financial institution”).

39. See 31 CFR § 1010.620. The definition of “covered financial institution” is found in 31 CFR § 1010.605(e)(1). The definition of “private banking account” is found in 31 CFR § 1010.605(m). The definition of “non-U.S. person” is found in 31 CFR § 1010.605(h).

40. See 31 CFR § 1010.620(c).

*Anti-money-laundering/countering-the-financing-of-terrorism (AML/CFT) program and correspondent account due diligence requirements*

Financial institutions are reminded of AML/CFT program requirements, and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.<sup>41</sup> As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of a money services business (MSB) must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.<sup>42</sup>

**Information Sharing**

Information sharing among financial institutions is critical to identifying, reporting, and preventing sanctions evasion or other illicit financial activity in the commercial real estate sector. 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.<sup>43</sup> 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](mailto:frc@fincen.gov).

41. 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.

42. 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, (Dec. 14, 2004). See also FinCEN, "[Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring](#)," Mar. 11, 2016.

43. See FinCEN, "[Section 314\(b\) Fact Sheet](#)," Dec. 2020.

**FinCEN Alert on Misuse of Commercial Real Estate Investments by Illicit Actors**

- In the year since Russia’s full-scale invasion of Ukraine began, and thanks to international pressure and the economic restrictions that over 30 countries have imposed on Russia, sanctioned Russian elites increasingly have fewer options for moving and hiding their ill-gotten wealth.
- The United States is committed to exposing the channels that Russian elites, oligarchs, and their proxies may use to move or hide funds. Recently, the Financial Crimes Enforcement Network (FinCEN) issued an alert to U.S. financial institutions identifying red flags and typologies in commercial real estate transactions that financial institutions can use to remain vigilant in monitoring, detecting, and reporting suspicious activity that may be indicative of sanctions evasion by sanctioned Russia elites, oligarchs, and their proxies.
- The relative stability of the U.S. commercial real estate market and the high value of commercial real estate properties can provide illicit actors with a way to generate a steady income and store large amounts of wealth.
- Real estate money laundering schemes can involve a wide range of conventional domestic criminals, as well as transnational criminals, including drug cartels and human traffickers, international terrorists, and foreign kleptocrats (i.e., corrupt high-level officials). The purchase of real estate, often combined with methods to conceal a purchaser's identity and source of funds, can allow criminals to integrate ill-gotten proceeds into the legal economy.
- As the United States explained in its 2020 National Strategy for Combating Terrorist and Other Illicit Financing, “[c]riminals with



widely divergent levels of financial sophistication use real estate at all price levels to store, launder, or benefit from illicit funds.” In that report, we identified the risks of laundering illicit proceeds through real estate purchases as a main vulnerability and key action item for strengthening the U.S. framework to counter money laundering and terror financing.

- And, as Secretary of the Treasury Yellen highlighted in March 2023 during the Second Summit for Democracy, “[c]orrupt actors have for decades anonymously stashed their ill-gotten gains in real estate. By one estimate, illicit actors laundered at least \$2.3 billion through U.S. real estate between 2015 and 2020.”
- We assess that sanctioned Russian elites and their proxies are likely attempting to evade sanctions by exploiting vulnerabilities in the U.S. and international commercial real estate markets. Commercial real estate transactions routinely involve highly complex financing methods and opaque ownership structures that diminish transparency in a way that can allow bad actors to hide illicit funds in commercial real estate investments.
- We ask you to share FinCEN’s alert with your financial and real estate sectors and to consider issuing your own alert.
- We thank you for your cooperation and support in the global fight against illicit finance and for preventing sanctions evaders and criminals from hiding or profiting from their ill-gotten wealth.