Debevoise Insight: Roundup of Recent Anti-Money Laundering Guidance and Advisories

July 20, 2022

The Financial Crimes Enforcement Network ("FinCEN"), joined at times by other federal government agencies, has issued a series of advisories and guidance of importance to financial institutions.[1] In this Debevoise In Depth, we review recent FinCEN issuances concerning developments in customer due diligence ("CDD"), emerging fraudulent schemes impacting consumers, and attempts to evade sanctions or export controls.

FinCEN and Federal Banking Agencies Issue Statement on Customer Due Diligence

On July 6, 2022, FinCEN and the federal banking agencies issued a joint statement reinforcing their position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing or other illicit financial activity.[2] The agencies noted that, although the Federal Financial Institutions Examination Council's Bank Secrecy Act/Anti-Money Laundering Examination Manual contains sections on certain customer types (*e.g.*, independent automated teller machine owners or operators, charities and nonprofit organizations, and nonbank financial institutions), the inclusion of these sections is meant to provide background information and is not meant to signal that certain customer types should be considered "uniformly higher risk." The joint statement does not establish new supervisory expectations or alter existing anti-money laundering ("AML") requirements.

---

[1] We thank Tara Holzer for her help in drafting this Debevoise In D epth.

[2] FinCEN, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration and Office of the Comptroller of the Currency, Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence (July 6, 2022), *available* here.

FinCEN and BIS Urge Financial Institutions to Be Vigilant for Potential Russian and Belarusian Export Control Evasion Attempts

On June 28, 2022, FinCEN and the Commerce Department's Bureau of Industry and Security ("BIS") issued a joint alert urging financial institutions to remain vigilant against efforts by individuals or entities to evade BIS export controls implemented in connection with Russia's invasion of Ukraine.[3] Since February 24, 2022, BIS has implemented a series of export controls targeting Russia's defense, aerospace, maritime and energy production sectors in an attempt to sequester Russia from the technologies and other items required to sustain its military activity in Ukraine, as well as export controls targeting luxury goods used by Russian elites. The United States has also placed restrictions on Belarus in response to its enabling of Russia's war effort.

BIS requires a license prior to export to Russia or Belarus of certain commodities due to their potential end use to further military and defense activities. Examples of such commodities include aircraft parts/equipment, antennas, breathing systems, cameras, GPS systems, inertial measurement units, integrated circuits, oil field equipment, sonar systems, spectrophotometers, test equipment, thrusters, underwater communications, vacuum pumps, water fabrication equipment and wafer substrates.

Financial institutions may have visibility into various aspects of export-related financial activities. Banks, credit card operators and foreign exchange dealers often are involved in providing financing, processing payments or performing other services associated with international trade. FinCEN advises any financial institutions with customers in maritime or export/import industries to rely on their internal risk assessments in employing risk mitigation measures, including CDD. Further, FinCEN cautions financial institutions directly involved in providing trade finance for exporters that they may have access to information relevant to identifying potentially suspicious activity, including customers' end-use certificates, export documents or other more extensive documentation associated with letters of credit-based trade financing. FinCEN suggests that such financial institutions may also have information about other parties involved in their clients' transactions through payment transmittal orders or SWIFT messages. If financial institutions identify suspicious activity, they have an obligation to file suspicious activity reports ("SARs") and should take care to include the information FinCEN identified above.

To encourage vigilance in monitoring possible export control evasion and the filing of SARs, FinCEN and BIS provided a list of transactional and behavioral red flag indicators

[3] FinCEN and BIS, 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, FIN-2022-Alert003 (June 28, 2022), *available* here.

of export control evasion that may be helpful in determining whether an identified activity may be connected to export control evasion (in addition to other appropriate risk-based customer and transactional due diligence). We recommend that clients review the list of red flags carefully to determine if any of them have been identified in their day-to-day business. The alert concluded with a reminder of relevant Bank Secrecy Act ("BSA") reporting obligations for U.S. financial institutions in connection with suspicious activity.

FinCEN Issues Statement to Clarify How to Apply a Risk-Based Approach to CDD on ATM Operators

On June 22, 2022, FinCEN issued a statement reminding banks that independent automated teller machine ("ATM") owner or operator customers are not necessarily all on the same playing field in terms of posing money laundering, terrorist financing or other illicit financial activity risk.[4] In its statement, FinCEN stresses that banks that operate in compliance with BSA/AML regulatory requirements and reasonably manage and mitigate risks related to unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to independent ATM owner or operator customers.

In the aftermath of FinCEN's 2016 customer due diligence rule ("CDD Rule"), FinCEN notes that some independent ATM owners and operators reported difficulty in obtaining and maintaining access to banking services, which would jeopardize the financial services provided, particularly to persons in underserved markets. The CDD Rule requires banks to adopt risk-based procedures for CDD that enable them to (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[5] In each case, the procedures should be proportionate to the risks presented by each customer. Although the CDD Rule does not require banks to conduct additional or unique due diligence on independent ATM owner or operator customers, FinCEN suggests that some information may be useful for banks in making determinations concerning independent ATM owner or operator customers' money laundering and terrorism financing risk profiles. Such information may include organizational structure information, operational information (*i.e.*, policies, procedures, and internal controls) and source of funds information, among other information.

---

[4] FinCEN, Statement on Bank Secrecy Act Due Diligence for Independent ATM Owners or Operators (June 22, 2022), *available* here.

[5] *See e.g.*, 31 CFR 1020.210(a)(2)(v) (imposing CDD obligations on banks).

FinCEN Issues Advisory on Elder Financial Exploitation; Urges Financial Institutions to Aid in Combatting Growing Threat

On June 15, 2022, FinCEN issued an advisory alerting financial institutions to the rising trend of elder financial exploitation ("EFE").[6] EFE involves the illegal or improper use of an older adult's funds, property or assets, often through theft or scams. In particular, the advisory highlights new EFE typologies and red flags identified since FinCEN first issued an advisory on the subject in 2011.

In 2021, financial institutions filed 72,000 SARs relating to EFE, representing an increase of approximately 16% from the number of SARs filed in 2020. Further, the Consumer Financial Protection Bureau ("CFPB") estimates that the dollar value of suspicious transactions linked to EFE increased approximately 31% from 2019 to 2020—the largest year-to-year increase since 2013. Per FinCEN, financial institutions are in a unique position to detect possible EFE through their relationships with older customers.

EFE schemes typically involve either (i) theft of an older adult's assets, funds or income by a trusted person, or (ii) scams, involving the transfer of money to a stranger or imposter for a promised benefit or good that the older adult does not receive. In cases involving elder theft, trusted persons may use deception, intimidation or coercion against older adults in order to access, control and misuse their finances. In elder scams, criminals (who have no relationship to the victim) defraud victims into sending payments and disclosing personally identifying information under false pretenses or for a promised benefit or good the victims will never receive. These scammers may contact older adults via phone, email, text message, mail, social media, dating apps and websites or in-person communication and may pose as government officials, law enforcement agencies, technical or customer support representatives, social media connections or family, friends or other trusted persons in order to establish trust with older adults. They often request that victims make payments through wire transfers at money services businesses but are increasingly requesting payments via alternative means, like prepaid access cards, gift cards, money orders, tracked delivery of cash and high-value personal items through the U.S. Postal Service, ATM deposits, cash pick-up at the victim's houses and convertible virtual currency ("CVC"). In both cases, the potential for re-victimization is high, with many older adults experiencing further financial loss, isolation and emotional or physical abuse long after the initial exploitation.

To aid in identifying, preventing and reporting suspected EFE, FinCEN provides a list of transactional and behavioral red flag indicators of EFE and associated payments. We recommend that clients review the list of red flags carefully to determine if any has been

---

[6] FinCEN, Advisory on Elder Financial Exploitation, FIN-2022-A002 (June 15, 2022), *available* here.

identified in their day-to-day business. The alert concluded with a reminder of relevant BSA reporting obligations for U.S. financial institutions in connection with suspicious activity.

FinCEN Issues Advisory on Kleptocracy and Foreign Public Corruption

On April 14, 2022, FinCEN urged financial institutions to concentrate their efforts on detecting the proceeds of foreign public corruption. FinCEN's advisory details typologies and potential indicators of kleptocracy[7] and other forms of foreign public corruption, namely bribery, embezzlement, extortion and the misappropriation of public assets.[8] The advisory also highlights a few red flag indicators to guide financial institutions in preventing, detecting and reporting suspicious transactions associated with kleptocracy and foreign public corruption.[9] Such indicators are consistent with the BSA's mandated risk-based approach to compliance and require an assessment of the relevant facts and circumstances of each transaction in question. For a more detailed discussion of this guidance, see our client update from earlier this year.[10]

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

Following the U.S. government's imposition of sanctions on Russian elites and their proxies, FinCEN issued an alert on March 16, 2022 to highlight the importance of identifying and quickly reporting suspicious transactions involving real estate, luxury goods and other high-value assets.[11] FinCEN identified these assets as being a useful method of storing value as a means of exchange or investment, therefore making such assets attractive tools for those looking to evade sanctions. The alert provides financial institutions with guidance on identifying suspicious transactions under the following categories of assets as well as reminders concerning BSA reporting obligations.

---

7 Kleptocracy involves the theft by corrupt public officials of the public's wealth for personal gain and use of power and access to state-owned resources for personal benefit. Kleptocrats launder proceeds of their corruption through a variety of means, including through shell companies or by purchasing various high-value assets (*e.g.*, real estate, yachts, private jets and high-value art).

8 FinCEN, Advisory on Kleptocracy and Foreign Public Corruption, FIN-2022-A001 (Apr. 14, 2022), *available* here.

9 *Id.* at 8 and 9.

10 Debevoise Client Update, FinCEN Issues Advisory on Kleptocracy and Foreign Public Corruption (Apr. 20, 2022), *available* here.

11 FinCEN, FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and Their Family Members, FIN-2022-Alert002 (Mar. 14, 2022), *available* here.

- ***Real Estate.*** Sanctioned Russian elites and their proxies may use shell companies, trusts or offshore funds to purchase real estate as a vehicle for storing wealth or laundering illicit gains due to its high value, appreciation potential and potential for shielding a property's ultimate beneficial owner.

- ***Artworks.*** The art market is an attractive market for money laundering by illicit actors. Sanctioned Russian elites may use shell companies and intermediaries to shield their identities in buying, holding or selling artworks. Artwork is also easily moved and concealed, and is subjective in value, making it even more vulnerable to sanctions evasion.

- ***Precious Metals, Stones and Jewelry ("PMSJs").*** PMSJs are portable, highly valuable and practical replacements for currency. Because the underlying commodity (*e.g.*, gold) is legal, PMSJs are ideal for concealing illicit wealth. Additionally, Russia is a major exporter of PMSJs (including gold and diamonds), so sanctioned Russian elites and their proxies may easily attempt to evade trade restrictions in trading PMSJs for currency or funds.

- ***Other High-Value Assets.*** Sanctioned Russian elites and their proxies are known for purchasing and selling other high-value assets like yachts or luxury cars. Therefore, the U.S. government is focused on enforcing sanctions against such property.

In addition to the guidance above, FinCEN highlighted the U.S. government's and its partners' efforts to identify, freeze and seize assets belonging to sanctioned Russian elites and their proxies through a series of international and domestic task forces:

- ***Russian Elites, Proxies, and Oligarchs (REPO) Task Force***, designed to ensure the effective implementation of Russia-related sanctions imposed by the United States, Australia, Canada, the European Commission, France, Germany, Italy, Japan and the United Kingdom.

- ***Task Force KleptoCapture***, dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures imposed by the United States and its allies and partners in connection with Russia's invasion of Ukraine.

- ***Kleptocracy Asset Recovery Rewards Program***, supporting U.S. government programs and investigations aimed at restraining, seizing, forfeiting or repatriating stolen assets linked to foreign government corruption and corresponding proceeds, with initial rewards focused on recovery of assets stolen by Russian elites and their proxies and associates.

- ***Kleptocracy Asset Recovery Initiative***, used by the U.S. government to identify, seize and recover kleptocrats' and other corrupt individuals' assets.

FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts

On March 7, 2022, FinCEN issued an alert advising all financial institutions to be vigilant for potential efforts to evade the expansive sanctions and other U.S.-imposed restrictions implemented in connection with Russia's invasion of Ukraine.[12] To guide financial institutions in identifying suspected sanctions evasion activity, FinCEN's alert dictated a series of red flags in the following categories: (1) sanctions evasion attempts using the U.S. financial system, (2) sanctions evasion using convertible virtual currency ("CVC") and (3) possible ransomware attacks and other cybercrime.

- ***Sanctions Evasion Attempts Using the U.S. Financial System.*** Sanctioned Russian and Belarusian actors may seek to evade sanctions through non-sanctioned Russian and Belarusian financial institutions and/or financial institutions in third countries. Various actors could seek to perpetrate such sanction evasion activities, including CVC exchangers and administrators within or outside of Russia that retain some access to the international financial system.

- ***Sanctions Evasion Using CVC.*** AML and sanctions compliance obligations apply to CVC transactions just as they do to fiat currency. Although large-scale sanctions evasion using CVC by the Russian government is not necessarily practicable, sanctioned persons, illicit actors and their related networks may attempt to use CVC and similar anonymizing tools to evade U.S. sanctions and protect their assets globally.

- ***Possible Ransomware Attacks and Other Cybercrime.*** Russian-related ransomware campaigns can pose significant dangers to financial institutions.

Federal Agencies Launch Joint Effort to Alert Online Daters and Social Media Users of Romance Scams That Have Cost Americans Millions

On February 7, 2022, the Commodity Futures Trading Commission ("CFTC"), the CFPB, the Department of Homeland Security's Immigration and Customs Enforcement, the

---

[12] FinCEN, FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts, FIN-2022-Alert001 (Mar. 7, 2022), *available* here.

U.S. Postal Inspection Service and FinCEN announced a collaborative effort to alert the public to romance scams that target victims largely through dating apps or social media.[13] Titled *Dating or Defrauding?*, the initiative aims to educate members of the public on how to recognize scams before they give any money or assets and provides steps for individuals to take if they are victimized.

While romance scams are not themselves new, new types of scams are emerging, with perpetrators targeting new audiences through online dating apps, social media and messaging apps. According to the Federal Trade Commission, reported romance frauds increased a whopping 48% from 2020 through the third quarter of 2021. Over the past few months, the *Dating or Defrauding?* awareness campaign launched public outreach through social media, local and national media outreach and public-private partnerships in an effort to curtail these types of frauds.

* * *

Please do not hesitate to contact us with any questions.

[13] CFTC, Press Release, Federal Agencies Launch Joint Effort to Alert Online Daters and Social Media Users of Romance Scams That Have Cost Americans Millions, Release No. 8491-22 (Feb. 7, 2022), *available* here.

WASHINGTON, D.C.


Satish M. Kini
smkini@debevoise.com


Robert T. Dura
rdura@debevoise.com


Aseel M. Rabie
arabie@debevoise.com

NEW YORK


Zila Reyes Acosta-Grimes
zracosta@debevoise.com