Schulte Roth&Zabel

Alert

Russian Sanctions Update: FinCEN and NYDFS Issue Guidance

April 25, 2022

In response to the ongoing Russia-Ukraine conflict, President Biden has imposed broad sanctions on a multitude of individuals and institutions connected to Russia and Belarus.[1] These sanctions have targeted dozens of individuals, entities, and financial institutions, including the Russian Central Bank, the Russian sovereign wealth fund, large publicly traded Russian banks and corporations, Russia's energy sector, Russian imports and exports, and luxury assets belonging to oligarchs with ties to Russian Federation President Vladimir Putin.[2]

To address these developments, both the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and the New York State Department of Financial Services ("NYDFS") have released guidance outlining the steps that financial institutions and other regulated entities should take to meet their regulatory obligations arising from these sanctions-related developments. FinCEN has also released a related advisory that provides financial institutions with typologies and indicators associated with kleptocracy and other forms of foreign public corruption, which FinCEN identifies as widespread throughout the Russian government.[3] We discuss each of these publications below.

FinCEN Alert on Russian Sanctions Evasion

In a March 7, 2022 alert to all financial institutions (the "Russian Sanctions Evasion Alert"),[4] FinCEN outlines red flag indicators to assist in identifying potential sanctions evasion activity as well as ransomware attacks and other cybercrimes in connection with the Russia-Ukraine conflict. The Russian Sanctions Evasion Alert reiterates financial institutions' reporting requirements under the Bank Secrecy Act ("BSA") and their reporting obligations to the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury, such as filing reports regarding blocked financial accounts, payments or transfers in which an OFAC-designated country, entity or individual has any interest.[5]

---

[1] *See* Schulte Roth & Zabel's prior *Alerts*, *Sanctions Update: U.S. Imposes Sweeping Sanctions Against Russia and Belarus* (Feb. 28, 2022), *available at* https://www.srz.com/resources/sanctions-update-u-s-imposes-sweeping-sanctions-against-russia.html; and *Sanctions Update: US Begins to Roll Out Sanctions Against Russia* (Feb. 22, 2022), *available at* https://www.srz.com/resources/sanctions-update-u-s-begins-to-roll-out-sanctions-against-russia.html.

[2] *See,* e.g., U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors* (Mar. 3, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0628; and Press Release, *U.S. Treasury Guidance on President Biden's Executive Order* (Mar. 8, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0641.

[3] *See* FinCEN, *Advisory on Kleptocracy and Foreign Public Corruption*, FIN-2022-A001 (Apr. 14, 2022) at 2 ("Kleptocracy Advisory"), *available at* https://www.fincen.gov/sites/default/files/advisory/2022-04-14/FinCEN%20Advisory%20Corruption%20FINAL%20508.pdf.

[4] FinCEN, *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts* (Mar. 7, 2022) ("Russian Sanctions Evasion Alert"), *available at* https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf.

[5] *See* 31 CFR § 501.603.

Red Flags Relating to Sanctions Evasion Attempts Using the U.S. Financial System

The Russian Sanctions Evasion Alert cautions regulated financial institutions that sanctioned entities could use non-sanctioned Russian and Belarusian financial institutions and financial institutions in third countries to evade sanctions. Sanctions evasion activities could be conducted by a variety of actors. FinCEN points to the following red flags as indicators of potential sanction evasion activities:

- Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- Use of third parties to shield the identity of sanctioned persons and/or Politically Exposed Persons ("PEPs") seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.
- Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale.
- Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.
- Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[6]
- Non-routine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity over the prior 12 months. For example, the Central Bank of the Russian Federation may seek to use import or export companies to engage in foreign exchange transactions on its behalf and to obfuscate its involvement.

Red Flags Relating to Sanctions Evasion Using CVC

The Russian Sanctions Evasion Alert further warns that sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use convertible virtual currency ("CVC") and other anonymizing tools to evade sanctions. Specifically, CVC exchangers and administrators and other financial institutions may observe transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian and other affiliated persons. FinCEN lists the following red flag indicators of potential customer sanctions evasion attempts using CVC:

- A customer's transactions are initiated from or sent to the following types of Internet Protocol (IP) addresses: non-trusted sources; locations in Russia, Belarus, FATF-identified jurisdictions with anti-money laundering ("AML")/Counter-Financing of Terrorism ("CFT")/Counter-

[6] On March 12, 2022, the following seven Russian banks and their subsidiaries were disconnected from the SWIFT network and other financial messaging operators in compliance with EU Council Regulation 2022/345: Bank Otkritie, Novikombank, Promsvyazbank, Bank Rossiya, Sovcombank, Vnesheconombank, and VTB Bank.

Proliferation deficiencies, and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious.

- A customer's transactions are connected to CVC addresses included in OFAC's Specially Designated Nationals ("SDNs") and Blocked Persons List ("SDN List").
- A customer uses a CVC exchanger or foreign-located money services business ("MSB") in a high-risk jurisdiction with AML/CFT deficiencies, particularly for CVC entities and activities, including inadequate know-your-customer ("KYC") or customer due diligence ("CDD") measures.

Red Flags Relating to Possible Ransomware Attacks and Other Cybercrime

Reiterating the danger of potential Russian cyberattacks, FinCEN warns financial institutions of the following red flag indicators of ransomware and other cybercrime:

- A customer receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs with no apparent related purpose, followed by a transaction off the platform. This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.
- A customer initiates a transfer of funds involving a CVC mixing service.
- A customer has either direct or indirect receiving transaction exposure identified by blockchain tracing software as related to ransomware.

Separately, the Russian Sanctions Evasion Alert stresses that "[i]t is critical that financial institutions (including CVC exchanges) identify and immediately report any suspicious transactions associated with ransomware attacks."[7] FinCEN instructs financial institutions to provide "as much of the relevant details around the activity as available at that time," and reminds them that amended Suspicious Activity Reports ("SARs") should be filed to reflect any additional information later discovered relating to the same underlying activity.[8] When filing SARs related to cyber events and associated transactions, financial institutions are also instructed to "include any relevant technical cyber indicators within the available structured cyber event indicator fields (42-44) on the SAR." Examples of relevant technical cyber indicators include "chat logs, suspicious IP addresses, suspicious email addresses, suspicious filenames, malware hashes, CVC addresses, command and control (C2) IP addresses, C2 domains, targeted systems, MAC address or port numbers."

Reminder of Relevant BSA Obligations

The Russian Sanctions Evasion Alert also reminds regulated financial institutions of their obligations under the BSA, including reporting requirements such as filing BSA reports, including SARs and currency transaction reports; conducting due diligence and enhanced due diligence, where necessary; and information sharing.

[7] Russian Sanctions Evasion Alert at 6 (noting that, for purposes of meeting a financial institution's SAR obligations, FinCEN and law enforcement consider suspicious transactions involving ransomware attacks to constitute "situations involving violations that require immediate attention." *See, e.g.*, 31 CFR § 1020.320(b)(3) (Banks), 31 CFR. § 1022.320(b)(3) (MSBs), and 31 CFR § 1025.320(b)(3) (Insurance Companies)).

[8] Russian Sanctions Evasion Alert at 6-7. FinCEN also notes that "completely new activity should be filed in a new 'initial' SAR filing." *Id*.

- **Suspicious Activity Reporting**. FinCEN reminds financial institutions of their SAR filing obligations and associated requirements to maintain records related to SARs and cooperate with law enforcement and regulatory inquiries related to SAR filings, noting that voluntary SAR filings are subject to existing safe harbor protections. FinCEN also reminds financial institutions that a blocking report filed with OFAC would not satisfy a SAR filing obligation if a financial institution were to identify facts and circumstances surrounding the event that are independently suspicious.[9] FinCEN further provides specific instructions for filing SARs in connection with the activities highlighted in the Russian Sanctions Evasion Alert, requesting that financial institutions include the key term "FIN-2022-RUSSIASANCTIONS" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the Russian Sanctions Evasion Alert. FinCEN also reminds financial institutions of their ability to contact the FinCEN Financial Institutions Toll-Free Hotline.[10]
- **Due Diligence Obligations.** The Russian Sanctions Evasion Alert highlights certain due diligence obligations pertinent to concerns arising from the Russia-Ukraine conflict. FinCEN reminds financial institutions of the following:
    - *Senior foreign political figures*. Financial institutions are required to "establish risk-based controls and procedures," which include taking reasonable steps to make sure that the financial institutions knows whether a senior foreign political figure who nominally or beneficially owns a private banking account is or is not a foreign PEP and to "conduct scrutiny of assets held by such individuals."[11]
    - *Enhanced due diligence requirements for private banking accounts*. Under Section 312 of the USA PATRIOT Act, 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.
    - *General obligations for correspondent account due diligence and AML programs*: Financial institutions are also required to comply with their general due diligence obligations for correspondent accounts, in addition to their general AML program obligations. MSBs are reminded of their risk-based AML program requirements with respect to foreign agents or foreign counterparties.

[9] *See* Russian Sanctions Evasion Alert at 6, citing 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 38-40 ("[t]his 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 . . . [w]hen 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").

[10] FinCEN directs financial institutions wanting to expedite their report to call the FinCEN Financial Institutions Toll-Free Hotline at (866) 556-3974. Any imminent threat, however, should be reported immediately to local-area law enforcement officials. *Id*.

[11] *See Id.* at 8 (citing 31 CFR § 1010.620(c) ("In the case of a private banking account for which a senior foreign political figure is a nominal or beneficial owner, the due diligence program required . . . shall include enhanced scrutiny of such account that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption)").

- **Information Sharing.** Lastly, the Russian Sanctions Evasion Alert strongly encourages the voluntary sharing of relevant information among financial institutions and associations under the safe harbor provision of section 314(b) of the USA PATRIOT Act.[12]

Reminder of Relevant OFAC Obligations

The Russian Sanctions Evasion Alert stresses the legal requirement to report to OFAC "all [blocked] property and interests in property of blocked persons that are in the United States or in the possession or control of U.S. persons" and emphasizes that "all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or otherwise exempted."[13]

FinCEN Alert on High-Value Oligarch Assets

On March 16, 2022, FinCEN issued an additional alert underscoring the importance of identifying and reporting suspicious transactions involving real estate, luxury goods and other high-value assets involving Russian elites, oligarchs, and their family members (the "High-Value Assets Alert").[14]

Red Flags Relating to the Real Estate Market

Warning that "Sanctioned Russian elites and their proxies may seek to evade sanctions through the purchase of commercial or high-end residential real estate," the High-Value Assets Alert highlights a number of red flag indicators of activity designed to evade sanctions:

- The purchase, sale, donation or transfer of legal ownership of high-value real estate in the name of a foreign legal entity, shell company, or trust, especially if the transaction (1) is either far above or below fair market value; (2) involves all-cash transfers; or (3) is funded by a third party with a known nexus to sanctioned Russian individuals.[15]
- The use of legal entities or arrangements to hide the ultimate beneficiary, origins or sources of funds that may have a sanctions nexus.
- Changes to the transaction patterns of a firm located in a country other than the U.S., Russia, Belarus or Ukraine, without an apparent business purpose, where the new transactions involve CVCs and Russian-related investments.
- A request by a Russian individual or entity for a wire transfer from a non-U.S. bank to pay for an all-cash purchase, particularly if the wired funds come from an account held by an individual or entity other than the requestor.

[12] *Id.* at 9.

[13] *Id.*

[14] FinCEN, *Alert on Real Estate, Luxury Goods, and Other High Value Assets Involving Russian Elites, Oligarchs, and their Family Members* (March 16, 2022) ("High-Value Assets Alert"), *available at* https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Elites%20High%20Value%20Assets_508%20FINAL.pdf.

[15] For additional information, see *SRZ Client Alert*, *FinCEN Commences Rulemaking Process to Implement AML Reporting Requirements for Real Estate Sector* (Feb. 11, 2022), *available at* https://www.srz.com/resources/fincen-commences-rulemaking-process-to-implement-aml-reporting.html.

- An attempt to shrink the real property holdings of sanctioned Russian elites and their proxies by bringing in, or transferring real estate to, an individual not affiliated with the buyer or seller.
- The maintenance, purchase or termination of real estate insurance by persons with a known nexus to sanctioned Russian individuals or entities.

Red Flags Relating to the Art Market

The High-Value Assets Alert also addresses the heightened risk of money laundering through the art market. FinCEN notes that the certain qualities of the art market make it particularly attractive to sanctioned Russian oligarchs seeking to launder money and "exacerbate [the art market's] vulnerability to sanctions evasion," such as the "mobility, concealability, and subjective value" of works of art. Accordingly, FinCEN advises regulated entities to be on the lookout for the following:

- The use of shell companies, trusts or third-party intermediaries with a nexus to sanctioned Russian entities to purchase, hold or sell art on a client's behalf.
- Transactions involving sanctioned Russian individuals and large amounts of cash, especially denominated in currencies not typically used in the art market.
- Art-related transactions involving persons with suspected ties to sanctioned Russian individuals who may not be concerned with recouping their investment, pay a substantially higher price than the value of the work or conduct transactions that exceed the expected sales value of the work.
- The maintenance, purchase or termination of insurance policies to protect the market value of the work from loss, theft or destruction.

Red Flags Relating to Other High-Value Assets

- FinCEN cautions that sanctioned Russian oligarchs may use precious metals, stones and jewelry ("PMSJs") to evade sanctions as Russia is a major exporter of many of the materials used to make PMSJs. Regulated entities are advised to pay particular attention to (1) transactions involving PMSJ trading companies and firms with a nexus to sanctioned Russian individuals, and (2) 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 individuals.
- Finally, FinCEN adds that sanctioned Russian individuals have been known to purchase and sell other high-value assets, such as luxury yachts and vehicles.[16] Accordingly, regulated entities should take note of the following: (1) sudden transfers of ownership interests in high-value goods and assets by sanctioned Russian individuals, including through sales; (2) the involvement of legal entities with a nexus to sanctioned Russian individuals "posing as well-known entities and operating in jurisdictions other than the well-known entity's jurisdiction"; (3) the involvement of a common set of individuals, financial institutions or addresses to facilitate transactions for luxury goods; (4) the involvement of law firms that have historically specialized in Russian clientele or in transactions associated with sanctioned Russian individuals; and (5) the involvement of transportation services that have been owned by or have a nexus to sanctioned Russian individuals.

[16] High-Value Assets Alert, *supra*.

FinCEN Advisory on Kleptocracy and Corruption

On April 14, 2022, FinCEN issued an advisory to urge financial institutions to focus their efforts on detecting transactions involving the proceeds of kleptocracy and foreign public corruption (the "Kleptocracy Advisory").[17] The Kleptocracy Advisory provides an overview of typologies associated with kleptocracy and foreign public corruption and potential red flag indicators[18] to help financial institutions identify the proceeds thereof.[19]

Typologies of Kleptocracy and Foreign Public Corruption

Foreign public corruption may involve wealth extraction, such as bribery, extortion, embezzlement or misappropriation or embezzlement of public funds and assets, which can occur at every level of government. The Kleptocracy Advisory highlights that Russian President Vladimir Putin "has allowed the resources of the Russian people to be siphoned off by oligarchs and elites, who amassed their fortunes through their personal connections to Putin and the abuse of state-owned entities and assets."[20] However, FinCEN notes that kleptocratic activities take place globally and often go hand-in-hand with other criminal behavior, such as human rights abuses, and typically employ the same money laundering methods used by other illicit actors such as drug traffickers or transnational organized crime syndicates.[21]

- **Wealth Extraction**
    - *Bribery and Extortion*. Bribery and extortion schemes often involve payments to foreign government officials by persons or entities to obtain or retain business or "influence political outcomes, secure beneficial contracts with governments or state-owned enterprises, gain access to natural resources, or obtain fraudulent documents such as passports or visas, among other purposes."[22] Payments made in furtherance of bribery and extortion can be made through third-party facilitators or legal entities controlled by the ultimate beneficiary's family members and close associates, and are often laundered through shell companies, offshore financial centers or professional service providers. The accounts into which the proceeds are deposited may be located outside the relevant public official's country of residence in order to evade detection and AML/CFT controls.

[17] President Biden established the fight against corruption as a core national security interest in 2021. *See* White House, *Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest* (June 3, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/. On June 30, 2021, FinCEN issued the first AML/CFT priorities, which identified corruption as one of the most significant AML/CFT threats currently facing the United States. *See* FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021) at 3, *available at* https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[18] The typologies and potential red flag indicators provided in the Kleptocracy Advisory are derived from FinCEN's "analysis of [BSA] data, open-source reporting, and information from law enforcement partners." *Id*. at 3.

[19] The Kleptocracy Advisory also provides various examples of enforcement actions. *See, e.g.*, *id.* at 4-5 (former president of Maryland transportation company found guilty of crimes including violations of the Foreign Corrupt Practices Act for participating in a scheme to bribe a Russian official in order to secure contracts with JSC Techsnabexport (TENEX), a subsidiary of Russia's State Atomic Energy Corporation).

[20] *Id*. at 3-4.

[21] *Id*. at 6.

[22] *Id*. at 4.

- *Misappropriation or Embezzlement of Public Assets*. Such schemes involve the "theft, diversion, or misuse of public funds or resources for personal benefit or enrichment."[23] Implicated assets may include government funds, services or contracts or publicly owned natural resources. Public officials or their associates may exploit or deceive corporations and financial institutions interested in doing business with the government into redirecting government resources for their own profit. FinCEN notes that the defense and health sectors and large infrastructure or development projects "appear to pose a particularly high risk of being associated with corruption-related money laundering."

- **Laundering Illicit Proceeds**
  - *Shell Companies and Offshore Financial Accounts*. Corrupt actors frequently rely on shell companies to obscure the ownership and origin of illicit funds, sometimes leveraging family members and close associates to create shell companies and open financial accounts on their behalf. Such shell companies can then be used to facilitate the payment of bribes or move funds gained through corrupt activities such as the misuse of state assets or government contracts. FinCEN notes that shell companies and offshore accounts are often "established in foreign jurisdictions whose corporate formation regimes and financial sector offer limited transparency to law enforcement, regulators, or financial institutions."[24]
  - *Purchase of Real Estate, Luxury Goods and Other High-Value Assets*. Similarly, corrupt actors often purchase high-value U.S. assets such as "luxury real estate and hotels, private jets, artwork, and motion picture companies" to launder illicit proceeds.[25] FinCEN further notes that the purchase of real estate to facilitate such conduct may also implicate complicit real estate professionals as well as involve "the use of legal entities and nominees to avoid detection."[26]

Financial Red Flag Indicators of Kleptocracy and Foreign Public Corruption

FinCEN provides the following financial red flag indicators to help financial institutions detect, prevent and report suspicious activity that may be associated with kleptocracy and foreign public corruption[27]:

- Transactions involving long-term government contracts consistently awarded, through an opaque selection process, to the same legal entity or entities that share similar beneficial ownership structures.
- Transactions involving services provided to state-owned companies or public institutions by companies registered in high-risk jurisdictions.

[23] *Id.* at 5.
[24] *Id.* at 6-7.

[25] *Id.* at 7.

[26] The U.S. government is working with allies and partners to block President Putin and certain Russian elites' assets in the United States and elsewhere, including their real estate, private jets and mega yachts. *Id.* at 8 (citing White House, *FACT SHEET: The United States Continues to Target Russian Oligarchs Enabling Putin's War of Choice* (March 3, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/03/fact-sheet-the-united-states-continues-to-target-russian-oligarchs-enabling-putins-war-of-choice/).

[27] *Id.* at 8.

- Transactions involving official embassy or foreign government business conducted through personal accounts.
- Transactions involving public officials related to high-value assets, such as real estate or other luxury goods, that are not commensurate with the reported source of wealth for the public official or that fall outside that individual's normal pattern of activity or lifestyle.
- Transactions involving public officials and funds moving to and from countries with which the public officials do not appear to have ties.
- Use of third parties to shield the identity of foreign public officials seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.
- Documents corroborating transactions involving government contracts (*e.g.*, invoices) that include charges at substantially higher prices than market rates or that include overly simple documentation or lack traditional details (*e.g.*, valuations for good and services).
- Transactions involving payments that do not match the total amounts set out in the underlying documentation, or that involve vague payment details or the use of old or fraudulent documentation to justify transfer of funds.
- Transactions involving fictitious email addresses and false invoices to justify payments, particularly for international transactions.
- Assets held in the name of intermediate legal entities whose beneficial owner or owners are tied to a kleptocrat or his or her family member.

NYDFS Guidance Relating to Recent Sanctions

On February 25, 2022, the NYDFS released an Industry Letter (the "Industry Letter")[28] to emphasize that entities and individuals subject to NYDFS regulations ("Regulated Entities") should fully comply with U.S. sanctions on Russia, as well as New York State and federal laws and regulations. The Industry Letter clarifies the NYDFS's expectations regarding Regulated Entities' approach to, and the significance of, compliance with cybersecurity, virtual currency and sanctions regulatory requirements.

Cybersecurity

The Industry Letter outlines steps Regulated Entities should take to mitigate cybersecurity risk. These steps include reviewing Regulated Entities' cybersecurity programs and paying particular attention to core cybersecurity hygiene measures, evaluating their incident response and business continuity planning, implementing the NYDFS's June 2021 Ransomware Guidance,[29] conducting a full test of Regulated Entities' ability to restore backups and providing additional cybersecurity guidance to their employees. The Industry Letter cautions that Regulated Entities need to closely track guidance and alerts (as well as follow past issuances) from the Cybersecurity and Infrastructure Security Agency ("CISA") and Information Sharing and Analysis Centers (ISACs). Additionally, the NYDFS expects that regulated entities that do business in Russia or Ukraine will take increased measures to inspect traffic from the region and isolate networks from any Russian or Ukrainian offices from the entity's global

[28] NYDFS, Industry Letter, *Re: Escalating Situation in Ukraine and Impact to Financial Sector* (Feb. 25, 2022) (the "Industry Letter"), *available at* https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220225_ukraine_escalation_impact_financial.

[29] NYDFS, Industry Letter, *Re: Ransomware Guidance* (Jun. 30, 2022), *available at* https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.

network. Finally, the Industry Letter reminds regulated entities that any cybersecurity event that meets the criteria of 23 NYCRR § 500.17(a)[30] must be reported to the NYDFS's Portal[31] within 72 hours of the event, as well as reporting the event to CISA.

Sanctions

To ensure that they continue to refrain from transacting with SDNs, the Industry Letter urges Regulated Entities to sign up on the Treasury Department's website[32] for email updates. The NYDFS reiterates that Regulated Entities are prohibited from engaging in any transactions with persons on the SDN List, unless OFAC has authorized otherwise, through general licenses listed on the OFAC website or by obtaining a separate specific license for a certain transaction. The Industry Letter further outlines particular steps for Regulated Entities to take to ensure their compliance with applicable sanctions laws and regulations:

- Monitor all communications from the NYDFS, the U.S. Department of the Treasury, OFAC and other federal agencies in real-time to ensure that they are compliant;
- Review Transaction Monitoring and Filtering Programs to ensure the implementation of all modifications necessary for the system to remain compliant with current sanctions prohibitions, as well as Part 504 of the Superintendent's Regulations;[33]
- Monitor all transactions, particularly trade finance transactions and funds transfers, to identify and block transactions subject to OFAC sanctions and follow any OFAC instructions regarding blocked funds;
- Continually update the Regulated Entity's OFAC compliance policies and procedures.

Virtual Currency

The Industry Letter also warns that virtual currency transfers may be used to circumvent sanctions prohibitions and that, accordingly, all Regulated Entities engaging in virtual currency business activity must have in place policies and procedures to protect against risks specific to virtual currency, including through the implementation of OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry[34] and the NYDFS "BitLicense" regulation's AML program requirement.[35] The Industry Letter also states that in order to identify potentially sanctioned transactions, Regulated Entities should use virtual currency-specific control measures such as geolocation tools, IP address identification and blockchain analytics to identify information associated with sanctioned individuals and entities.

[30] 23 NYCRR § 500.17(a) (requiring each Regulated Entity to notify NYDFS no later than 72 hours from a determination that a cybersecurity event has occurred, subject to certain conditions and required each Regulated Entity to annually submit certification of compliance to the NYDFS).

[31] The NYDFS Portal can be accessed at https://myportal.dfs.ny.gov/.

[32] *See* https://service.govdelivery.com/accounts/USTREAS/subscriber/new.

[33] 3 NYCRR Part 504 (clarifying the required attributes of a Transaction Monitoring and Filtering Program and requiring that the board of directors or senior officer(s) of each Regulated Entity annually submit to the NYDFS a board resolution or compliance finding confirming the steps taken to ascertain such Regulated Entity's compliance with Part 504).

[34] OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021), *available at* https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

[35] 23 NYCRR § 200.15.

Additionally, on March 2, 2022, New York Governor Kathy Hochul announced that the state was taking "actions to strengthen the [NYDFS's] enforcement of sanctions against Russia, including the expedited procurement of additional blockchain analytics technology," in order to "bolster the [NYDFS's] ability to detect exposure among [NY]DFS-licensed virtual currency businesses to Russian individuals, banks and other entities that the Biden Administration has sanctioned."[36] Quoting NYDFS Superintendent Adrienne A. Harris, Governor Hochul's announcement states:

> We know that bad actors will try to evade sanctions through the transmission of virtual currency, which is why it is imperative that we have the ability to monitor transactions and exposure in real-time. We continue to coordinate closely with federal and other state regulators and communicate with our regulated entities to ensure the full weight of our regulatory regime is brought to bear in the fight to protect Ukraine.

Conclusion

Financial institutions should monitor for and be mindful of any guidance by state and federal regulators to ensure compliance with any sanctions-related rules. For more information about the sanctions issued in connection with the Russia-Ukraine conflict, please see Schulte Roth & Zabel's prior *Alerts* referenced above and on the SRZ website.

Schulte Roth & Zabel's lawyers are available to assist you or address any questions you may have regarding these developments. Please contact the Schulte Roth & Zabel lawyer with whom you usually work, or any of the following attorneys:

Betty Santangelo – New York (+1 212.756.2587, betty.santangelo@srz.com)
Gary Stein — New York (+1 212. 756.2441, gary.stein@srz.com)
Melissa G.R. Goldstein – Washington, DC (+1 202.729.7471, melissa.goldstein@srz.com)
Donald J. Mosher – New York (+1 212.756.2187, donald.mosher@srz.com)
Kara A. Kuchar – New York (+1 212.756.2734, kara.kuchar@srz.com)
Hadas A. Jacobi – New York (+1 212.756.2055, hadas.jacobi@srz.com)
Hannah M. Thibideau – New York (+1 212.756.2382, hannah.thibideau@srz.com)
Angela Garcia – New York (+1 212.756.2359, angela.garcia@srz.com)
Steven T. Cummings – New York (+1 212.756.2251, steven.cummings@srz.com)

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com

[36] NYDFS, *Press Release: Governor Hochul Announces Actions to Strengthen Department of Financial Services Enforcement of Sanctions Against Russia* (Mar. 2, 2022), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20220302.