



# FinCEN

# ALERT

FIN-2022-Alert001

March 7, 2022

## FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts

The Financial Crimes Enforcement Network (FinCEN) is alerting all financial institutions<sup>1</sup> to be vigilant against efforts to evade the expansive sanctions and other U.S.-imposed restrictions implemented in connection with the Russian Federation’s further invasion of Ukraine.<sup>2</sup> The United States is committed to supporting Ukraine, and, along with key U.S. partners and allies around the globe, has imposed unprecedented economic pressure measures on Russia and Belarus. This alert provides select red flags<sup>3</sup> to assist in identifying potential sanctions evasion activity and reminds financial institutions of their Bank Secrecy Act (BSA) reporting obligations, including with respect to convertible virtual currency (CVC).

### Suspicious Activity Report (SAR) filing request

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

**“FIN-2022-RUSSIASANCTIONS”**

It is critical that all financial institutions, including those with visibility into CVC flows, such as CVC exchangers and administrators—generally considered money services businesses (MSBs)<sup>4</sup> under the BSA—identify and quickly report suspicious activity associated with potential sanctions evasion, and conduct appropriate risk-based customer due diligence or, where required, enhanced due diligence (see *Reminder of Relevant BSA Obligations* below). FinCEN also strongly encourages all financial institutions to make full use of their ability to share information consistent with Section 314(b)<sup>5</sup> of the USA PATRIOT Act,<sup>6</sup> and consider how the use of innovative tools and solutions may assist in identifying hidden Russian and Belarusian assets.<sup>7</sup>

1. See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. For relevant U.S. Department of the Treasury Office of Foreign Asset Control (OFAC) actions against the Russian Federation and the Republic of Belarus, see [OFAC Recent Actions | U.S. Department of the Treasury](#). For additional information on compliance with OFAC obligations, see the *Summary of Relevant OFAC Compliance Obligations* section of this alert. For relevant U.S. Department of Commerce Bureau of Industry and Security actions, see [U.S. Department of Commerce](#). For relevant U.S. Department of State actions, see [U.S. Department of State](#). For other relevant U.S. government measures and actions, see [The White House](#).
3. Many of the red flag indicators highlighted in this alert were previously identified in other FinCEN advisories and represent only a sampling of indicators of possible sanctions evasion activity and should not be considered an exhaustive list. Further, because no single financial red flag indicator is determinative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.
4. See FinCEN Guidance, [“Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,”](#) (May 9, 2019).
5. See 31 CFR § 1010.540.
6. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”)* (Pub. L. 107–56).
7. See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, FinCEN, National Credit Union Administration, and Office of the Comptroller of the Currency, [“Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing,”](#) (December 3, 2018).

## Overview of Recent Treasury Actions Responding to the Further Invasion of Ukraine

Since February 2022, and in response to Russia's further invasion of Ukraine, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has taken several significant sanctions actions related to the Russian financial services sector pursuant to Executive Order (E.O.) 14024,<sup>8</sup> including: a determination by the Secretary of the Treasury with respect to the financial services sector of the Russian Federation<sup>9</sup> that authorizes sanctions against persons determined to operate or to have operated in that sector; correspondent or payable-through account and payment processing prohibitions on certain Russian financial institutions; the blocking of certain Russian financial institutions; expanding sovereign debt prohibitions to apply to new issuances in the secondary market; prohibitions related to new debt and equity for certain Russian entities; and a prohibition on transactions involving certain Russian government entities, including the Central Bank of the Russian Federation.<sup>10</sup> OFAC also imposed sanctions on Russian Federation President Vladimir Putin, and Minister of Foreign Affairs Sergei Lavrov.<sup>11</sup> In a related action, OFAC designated certain Belarusian persons, including financial institutions, due to Belarus' support for, and facilitation of, the invasion.<sup>12</sup> Most recently, OFAC and the U.S. Department of State intensified pressure on Russia by sanctioning numerous Russian elites and their family members, identifying certain property of these persons as blocked, and sanctioning Russian intelligence-directed disinformation outlets and defense-related firms.<sup>13</sup> The United States has been clear that it will continue to impose severe economic costs on Russia if it does not change course. Please continue to consult OFAC's website<sup>14</sup> for additional information on sanctions actions.

### Sanctions Evasion Attempts Using the U.S. Financial System

As a result of these actions, sanctioned Russian and Belarusian actors may seek to evade sanctions through various means, including through non-sanctioned Russian and Belarusian financial institutions and financial institutions in third countries. Sanctions evasion activities could be conducted by a variety of actors, including CVC exchangers and administrators within or outside Russia, that retain at least some access to the international financial system. FinCEN encourages financial institutions to review FinCEN's previous publications, which provide indicators relevant

8. See [Executive Order 14024 of April 15, 2021, Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation](#).

9. See [Determination Pursuant to Section 1\(a\)\(i\) of Executive Order 14024](#) (February 22, 2022).

10. See [OFAC Frequently Asked Question 966](#) (March 2, 2022). See also, Treasury Press Release, "[U.S. Treasury Targets Belarusian Support for Russian Invasion of Ukraine](#)," (February 24, 2022).

11. See U.S. Department of the Treasury (Treasury) Press Release, "[U.S. Treasury Imposes Sanctions on Russian Federation President Vladimir Putin and Minister of Foreign Affairs Sergei Lavrov](#)," (February 25, 2022). In a related action, the U.S. Department of State imposed [sanctions](#) on Russian Minister of Defense Sergei Shoigu and First Deputy Minister of Defense and Chief of the General Staff of the Armed Forces of the Russian Federation Valery Gerasimov.

12. See Treasury Press Release, "[U.S. Treasury Targets Belarusian Support for Russian Invasion of Ukraine](#)," (February 24, 2022).

13. See Treasury Press Release, "[Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors](#)," (March 3, 2022).

14. See [OFAC Recent Actions | U.S. Department of the Treasury](#).

to foreign political corruption and efforts by corrupt senior foreign political figures, their families, and their associates (together often referred to as foreign “politically exposed persons” (PEPs)), or associated entities and financial facilitators, to evade U.S. sanctions or otherwise hide their assets.<sup>15</sup>

### Select Red Flag Indicators<sup>16</sup>

- 1 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.
- 2 Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.
- 3 Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.<sup>17</sup>
- 4 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.
- 5 Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.
- 6 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).
- 7 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.

---

15. See, e.g., FinCEN, [“Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators”](#) (June 12, 2018). See also FinCEN, [“Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption,”](#) (April 17, 2008); and FinCEN, The SAR Activity Review, Issue 19, [“In Focus: Foreign Corruption; Sections 4 and 5,”](#) (May 2011). See also Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, FinCEN, National Credit Union Administration, and Office of the Comptroller of the Currency, [“Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons,”](#) (August 21, 2020). For examples of other nation-state sanctions evasion red flags, see also FinCEN, [“Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System,”](#) (October 11, 2018) and FinCEN, [“Advisory on North Korea’s Use of the International Financial System,”](#) (November 2, 2017).




16. *Id.*

17. See FinCEN [“Advisory to Financial Institutions and Real Estate Firms and Professionals,”](#) (August 22, 2017).

## Sanctions Evasion Using CVC

Anti-money laundering/countering the financing of terrorism/counter proliferation (AML/CFT/CP) and sanctions compliance obligations apply to CVC transactions, just as they do to transactions involving fiat currency. While large scale sanctions evasion using CVC by a government such as the Russian Federation is not necessarily practicable, sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use CVC and anonymizing tools to evade U.S. sanctions and protect their assets around the globe, including in the United States. CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons.

### Select Red Flag Indicators<sup>18</sup>

-  8 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 AML/CFT/CP deficiencies,<sup>19</sup> and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious.
-  9 A customer's transactions are connected to CVC addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List.
-  10 A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction with AML/CFT/CP deficiencies, particularly for CVC entities and activities, including inadequate "know-your-customer" or customer due diligence measures.

## Possible Ransomware Attacks and Other Cybercrime




FinCEN reminds financial institutions about the dangers posed by Russian-related ransomware campaigns.<sup>20</sup> FinCEN encourages financial institutions to refer to previous FinCEN and OFAC publications and other relevant recent resources noting Russian and other ransomware and cybercrime activities for a range of indicators to help detect, prevent, and report potential suspicious activity.

18. See FinCEN, "[Advisory on Illicit Activity Involving Convertible Virtual Currency](#)," (May 9, 2019).

19. See FinCEN, "[Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies](#)," (October 26, 2021).

20. See "[Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments](#)," (November 8, 2021); FinCEN Report, "[Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data between January 2021 and June 2021](#)," (October 15, 2021); and FinCEN, "[Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#)," (June 30, 2021). For ongoing information on other cybersecurity issues relevant to this alert, see also the Cybersecurity and Infrastructure Security Agency's "[Shields Up](#)" and "[StopRansomware](#)".

Select Red Flag Indicators<sup>21</sup>

-  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.

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

*Suspicious Activity Reporting  
Other Relevant BSA Reporting  
Due Diligence*

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

**Suspicious Activity Reporting**

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions evasion.<sup>22</sup> All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.<sup>23</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>24</sup> Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an

21. *Id.* See also, FinCEN, [“Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 \(COVID-19\) Pandemic,”](#) (July 30, 2020); FinCEN, [“Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes,”](#) (July 16, 2019); FinCEN, [“Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime,”](#) (October 25, 2016).

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

23. See 31 U.S.C. § 5312(a)(2) and 31 U.S.C. § 5318(g)(3). All financial institutions with SAR filing requirements (see footnote 22) also may file a SAR regardless of the amount involved (if any) or if the transaction is only attempted.

24. 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).



appropriate law enforcement or supervisory agency.<sup>25</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.

SARs and OFAC Sanctions

Longstanding FinCEN guidance<sup>26</sup> provides clarity regarding when a financial institution must satisfy its obligation to file a SAR on a transaction involving a designated person when also filing a blocking report with OFAC. Relatedly, ransomware attacks and payments on which financial institutions file SARs should also be reported to OFAC at [OFAC\\_Feedback@treasury.gov](mailto:OFAC_Feedback@treasury.gov) (see *Summary of Relevant OFAC Obligations*) if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment.

**SAR Filing Instructions**

FinCEN requests that financial institutions reference this alert by including the key term “**FIN-2022-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 activities highlighted in this alert.

*Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the FinCEN Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).<sup>27</sup>*

It is critical that financial institutions (including CVC exchanges) identify and immediately report any suspicious transactions associated with ransomware attacks. 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.”<sup>28</sup> Financial institutions must subsequently file a

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

26. See FinCEN, The SAR Activity Review, Issue 8, Section 5 “[Revised Guidance on Filing Suspicious Activity Reports Relating to the Office of Foreign Assets Control List of Specially Designated Nationals and Blocked Persons](#),” pp. 38-40, (April 2005), which states, “[t]o the extent that the financial institution is in possession of information not included on the blocking report filed with [OFAC], a separate [SAR] should be filed with FinCEN including that information. This guidance also does not affect a financial institution’s obligation to file a [SAR] even if it has filed a blocking report with [OFAC], to the extent that the facts and circumstances surrounding the [OFAC] match are independently suspicious and are otherwise required to be reported under the existing FinCEN regulations. In those cases, the [OFAC] blocking report would not satisfy a financial institution’s [SAR] filing obligation....When a financial institution files a reject report on a transaction, the financial institution is obligated to file a [SAR] to the extent that the facts and circumstances surrounding the rejected funds transfer are suspicious.”

27. 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.

28. See *e.g.*, 31 CFR § 1020.320(b)(3) (Banks), 31 CFR. § 1022.320(b)(3) (Money Services Businesses), and 31 CFR § 1025.320(b)(3) (Insurance Companies).

SAR using FinCEN’s BSA E-filing System, providing as much of the relevant details around the activity as available at that time. Amended SARs should be filed to include additional information related to the same activity that is learned later; completely new activity should be filed in a new “initial” SAR filing.

Financial institutions also should include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields (42-44) on the SAR. Any data or information that helps identify the activity as suspicious can be included as an indicator. Examples 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.

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

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this alert.<sup>29</sup> These include obligations related to the Currency Transaction Report (CTR),<sup>30</sup> Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),<sup>31</sup> Report of Foreign Bank and Financial Accounts (FBAR),<sup>32</sup> Report of International Transportation of Currency or Monetary Instruments (CMIR),<sup>33</sup> Registration of Money Service Business (RMSB),<sup>34</sup> and Designation of Exempt Person (DOEP).<sup>35</sup> These standard reporting requirements may not have an obvious connection to Russia-related illicit finance, but may ultimately prove highly useful to law enforcement.

- 
29. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer’s foreign bank and financial accounts) to FinCEN “that are highly useful in criminal, tax, or regulatory investigations, risk assessments, or proceedings; or intelligence or counterintelligence activities, including analysis, to protect against terrorism.” 31 U.S.C. § 5311.
  30. A report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than \$10,000, in aggregate per business day. 31 CFR § 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
  31. A report filed by any U.S. person engaged in a trade or business on the receipt of more than \$10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 CFR § 1010.330 and 31 CFR § 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
  32. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds \$10,000 at any time during the calendar year, as specified in 31 CFR § 1010.350 and FinCEN Form 114.
  33. Each person (i.e., an individual or legal entity), as defined in 31 CFR § 1010.100(mm), that transports, ships, or mails more than \$10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 CFR § 1010.340.
  34. Report for a business required to register with FinCEN as a money services business, as defined in 31 CFR § 1010.100(ff), or renewing the registration. 31 CFR § 1022.380.
  35. Report for banks, as defined in 31 CFR § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311.

## Due Diligence

### Due diligence obligations (senior foreign political figures)

Financial institutions should establish risk-based controls and procedures that include reasonable steps to ascertain the status of an individual as a foreign PEP and to conduct scrutiny of assets held by such individuals.<sup>36</sup>

FinCEN's Customer Due Diligence (CDD) Rule requires banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.<sup>37</sup> Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign PEPs.

### Enhanced due diligence obligations for private banking accounts

In addition to these general risk-based due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, certain U.S. financial institutions must implement a due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.<sup>38</sup>

### General obligations for correspondent account due diligence and AML programs

Banks, brokers or dealers in securities, mutual funds, and FCM/IBs also are reminded to comply with their general due diligence obligations for correspondent accounts under 31 CFR § 1010.610(a), in addition to their general AML program obligations under 31 U.S.C. § 5318(h) and its implementing regulations (which apply to all U.S. financial institutions).<sup>39</sup> MSBs have parallel requirements with respect to foreign agents or foreign counterparties, as described in FinCEN Interpretive Release 2004-1, which clarifies that the AML program regulation requires MSBs to establish adequate and appropriate policies, procedures, and controls commensurate with the risk of money laundering and the financing of terrorism posed by their relationship with foreign agents or foreign counterparties.<sup>40</sup>

36. See 31 CFR § 1010.620(c).

37. See 31 CFR § 1010.230.

38. See 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).

39. 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.

40. See FinCEN, "[Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties](#)," Interpretive Release 2004-1, 69 FR 239, December 14, 2004. See also FinCEN, "[Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring](#)," (March 11, 2016).



## Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving sanctions evasion, ransomware/cyber attacks, and laundering of the proceeds of corruption. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.<sup>41</sup> FinCEN strongly encourages such voluntary information sharing.

## Summary of Relevant OFAC Compliance Obligations

Pursuant to any OFAC sanctions, all property and interests in property of blocked persons that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. Equally, 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. Violations of U.S. sanctions regulations can subject those responsible to civil and criminal penalties, to include monetary fines and imprisonment.

### Executive Order 14024

In the context of the OFAC sanctions issued in response to the further invasion of Ukraine, E.O. 14024 permits the United States to impose blocking and short-of-blocking sanctions. OFAC has issued several directives under E.O. 14024 specifying certain prohibitions relating to persons determined to be subject to the applicable directive. OFAC expects all U.S. persons to review the sanctions lists maintained by OFAC, including the Specially Designated Nationals and Blocked Persons List (SDN List), the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List), and the Non-SDN Menu-Based Sanctions List (NS-MBS List), to determine which of these sanctions are applicable.

In addition, E.O. 14024 specifically allows for the targeting of persons engaged in deceptive or structured transactions or dealings to circumvent any United States sanctions, including through the use of digital currencies or assets or the use of physical assets. Anyone facilitating any Russian (or any other) efforts at sanctions evasion should understand that OFAC sanctions compliance obligations apply equally to transactions involving CVC and those involving traditional fiat currencies. OFAC has taken enforcement actions against CVC-related companies that engaged in prohibited activity because they failed to conduct sufficient screening of available geolocation information to prevent users in sanctioned jurisdictions from accessing and using their platforms.

41. For further guidance related to the 314(b) Program, see FinCEN, "[Section 314\(b\) Fact Sheet](#)," December 20, 2020.

## F I N C E N   A L E R T

---

For additional information on the general application of OFAC sanctions with regards to CVC, please review OFAC's related [guidance](#). For any other questions about E.O. 14204 sanctions, to report a ransomware attack or payment involving a potential sanctions nexus, or for more information on OFAC sanctions more broadly, contact [OFAC\\_Feedback@treasury.gov](mailto:OFAC_Feedback@treasury.gov).

### 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).