RAPID RESPONSE BRIEF

SUMMARY OF FINCEN ALERT (FIN-2022-ALERT001) ADVISING INCREASED VIGILANCE FOR POTENTIAL RUSSIAN SANCTIONS EVASION ATTEMPTS

On March 7, 2022, the Financial Crimes Enforcement Network (FinCEN) released an alert (FIN-2022-Alert001) advising financial institutions to increase their vigilance for potential sanctions evasion attempts by Russia and Belarus. The alert serves to remind financial institutions of their reporting requirements, lists potential red flags relating to sanctions evasion, and outlines suspicious activity report (SAR) filing considerations.

This rapid response brief highlights the key points outlined in the alert, to assist financial institutions and cryptoasset providers alike to take all necessary actions, configure their compliance systems, and exercise effective risk management.

FinCEN alert: key takeaways

1. Sanctioned individuals and entities within Russia will likely attempt to evade sanctions by using non-sanctioned financial institutions within Russia and Belarus, financial institutions in third countries, and convertible virtual currency (CVC) exchanges with access to the international financial systems.

2. Red flags relevant to politically exposed persons (PEPs) and foreign political corruption are pertinent in analyzing transactions that are potentially related to sanctions evasion.

3. Due diligence and information sharing are both critical in effectively determining Russian or Belarusian sanctions evasion attempts. All identification of property and interests of property of blocked persons in the US must be reported, while all transactions involving this property or interests are prohibited unless authorized with an OFAC issued license.

4. Virtual currency providers have equal obligations to report potential OFAC compliance risks and sanctions evasion.

5. Financial institutions (FIs) should increase awareness around their due diligence obligations surrounding senior foreign political figures, private bank accounts, and correspondent accounts.

6. The same money laundering and sanctions obligations apply to cryptoasset providers (considered money service businesses (MSBs) under the BSA) as to conventional FIs. Jurisdictional risks relating to established FIs also apply to cryptoasset providers. Internet protocol (IP) addressees and high-risk jurisdictions provide transaction and trade opportunities unavailable to sanctioned entities in major financial centers or through regulated cryptoasset exchanges and wallet providers.

7. Transactions linked to sanctioned cryptoasset entities and wallet addresses present a high risk to CVC related activity. However, it is notable that sanctions lists are public; the downside to this is that those on the list will not transact using real identifiers. Those who continue to attempt to evade sanctions will also use VPNs to mask their IP address.

8. Customers using exchanges or MSBs in high-risk jurisdictions may seek to take advantage of anti-money laundering/terrorist financing deficiencies, including porous KYC and CDD controls often associated with high risk and non-cooperative jurisdictions.

9. The alert restates previous red flags linked to Russian cybercrime and ransomware activity. It is highly likely that the threat posed by hostile state activity or organized crime groups operating inside Russia with explicit impunity will increase significantly on the back of geopolitical events.

SAR filing considerations

Financial institutions wanting to expedite the reporting 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. If a financial institution has reason to suspect a potential sanctions nexus with regard to a ransomware payment or attack, they should file a SAR and make a report to OFAC by emailing OFAC_Feedback@treasury.gov.

FinCEN's notice provided several requests related to filing a SAR, listed below.

SAR form and narrative considerations:

- SAR Field #2: Reference **FIN-2022-RUSSIASANCTIONS**
- Correlate the connection between the suspicious activity being reported on and the activities addressed in the alert
- Provide as many relevant details around the activity identified during the investigation as possible

SAR form considerations specific to convertible virtual currency exchanges:

- Include relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields (42-44) on the SAR

- Suspicious indicators, can 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, and MAC addresses or port numbers

Practical Steps for Financial Institution Compliance

- Ensure SAR filing procedures and quality control steps are in place to include the appropriate reference (and corresponding nexus) in the SAR form and narrative, and indicate the connection between the suspicious activity being reported and the red flags or activities highlighted in the alert.
- Establish frequent briefings on the status of your sanctions compliance program, and the efforts to align your risk-based AFC program to detect and report possible sanctions evasion, to the board of directors, or a committee thereof and senior management.
- Ensure appropriate staff are frequently trained on the evolving sanctions compliance landscape, and that the training update includes any adjustments to sanctions regulatory requirements or sanctions compliance internal policies, procedures, or processes.
- Validate that appropriate team members are aware of the SAR form and SAR narrative considerations identified in FIN-2022-RUSSIASANCTIONS, to make sure the SAR form requests made by FinCEN are addressed.
- Quickly inform appropriate personnel of critical advisories or alerts, such as the Fin-2022-RUSSIASANCTIONS, to immediately address any updates to policies, procedures, or processes. This should be considered across all business, product, and service lines, as well as geographies.
- Train staff on red flag indicators of foreign political corruption and efforts by corrupt senior political figures.
- Include examples of red-flag indicators of sanctions evasions, ransomware attacks or payment, and other cybercrimes in training updates.
- Document and maintain your rapid response training programs, including material, dates of training sessions, and attendee records.
- Consider implementing a risk-based rapid response training plan, to ensure appropriate personnel are trained on the evolving sanctions-evasion threat landscape and the rapidly changing complex sanctions regime.
- Evaluate your transaction monitoring program to ensure the red flags identified in the alert would be identified within your systems.

Considerations for Crypto Asset Compliance

- This alert is a call to arms for the cryptoasset sector and its compliance community. FinCEN is reacting to a strong desire from the United States Government and regulatory agencies for cryptoassets to respond to the magnitude of the occasion.

- Several red flags in the alert show crossovers between cryptoasset providers and conventional financial sector activity. Compliance professionals focused on cryptoassets will be well served by considering which red flags overlap with their risk mitigation controls.

- As cryptoasset providers' AML/CTF frameworks mature, they can learn from the ever-increasing volume of thought leadership, threat analysis, typologies, red flag indicators and alerts issued by regulators and law enforcement. It is requisite on the sector to understand its broader exposure to predicate criminality, including money laundering, fraud, corruption, market abuse, and wider thematic issues.

- Despite cryptoassets' current total market cap sitting at US$1.74 trillion against Russia's GDP of US$1.483 trillion (2020), and blocked Central Bank holdings equating to US$630 billion, the prospect of cryptoassets being used to circumvent sanctions at scale remains low.

- Cryptoasset businesses and financial institutions must prepare for a tightening sanctions compliance environment. Preparedness is key, and compliance officers must take a proactive approach.

Looking ahead

As the Russian Federation continues to invade Ukraine, and the country of Belarus provides support to the invasion, sanctions and additional restrictions will continue to evolve. It is imperative that US financial institutions monitor OFAC sanctions lists and the US Treasury for evolving guidance on the unprecedented situation in Ukraine. ACAMS will continue to monitor the situation and will give guidance via its newly formed Ukraine Crisis Hub.

Authors

Lauren Kohr, Senior Director AML, Americas
Joby Carpenter, Global SME – Cryptoassets and Illicit Finance
Tiffany Polyak, Project Coordinator/Researcher

March 9, 2022

About ACAMS

ACAMS is the largest global membership organization dedicated to enhancing the knowledge and skills of anti-money laundering (AML) and financial crime prevention professionals from a wide range of industries, with over 85,000 members in over 180 countries/regions. Its CAMS certification is the most widely recognized AML certification among compliance professionals worldwide. ACAMS offers two exclusive programs for sanctions professionals – the internationally recognized Certified Global Sanctions Specialist (CGSS) accreditation, and the Sanctions Compliance Foundations online certificate. Visit www.acams.org/sanctions for more information.