ACAMS

RAPID RESPONSE BRIEF

CRYPTO AND THE UKRAINE-RUSSIA WAR

Russia's expanded invasion of Ukraine, beginning in February 2022, amplified popular attention on the cryptoassets industry. Financial crime compliance and sanctions evasion risks, as well as positive use cases for humanitarian and military assistance to Ukraine (especially at the outset of the crisis), have been a continuing area of focus. US law enforcement and regulators took steps to educate key stakeholders about risks, as well as targeted actions against Russian-linked malign actors. Large cryptoasset firms took public positions about their continued operations in Russia, as many other companies voluntarily excited the jurisdiction but also acted on calls to block certain wallet holders.

This rapid response brief unpacks the crypto-related financial crime compliance developments in Ukraine and Russia this year to date.

How does this relate to AML/CFT compliance?

- The risk of widespread substitution of Russian economic activity through cryptoasset markets remains low. However, the US government has identified sanctions evasion risks, publicly provided guidance, and informed financial institutions of red flag indicators as Russia continues to engage in sanctions evasion.
- The US government continues to take coordinated interagency and international action against Russian-associated individuals and entities. This action includes sanctions designations and criminal prosecutions, such as the first designations against a cryptoasset exchange and a cryptocurrency mining company, both associated with Russia.
- Financial crime compliance requirements will continue to reflect cryptoasset related risks. Over the next few months, cryptoasset firms will need to navigate not just the uncertainty created by the bear market dynamics, but also heightened legislative, regulatory, and law enforcement attention on sanctions evasion risks from designated Russian entities, individuals, and third-party facilitators. Such governmental action could include additional sanctions designations, exchange takedowns, and law enforcement seizures.

Context

Russia cryptoasset financial crimes risks

1. Going into the conflict, Russia was deemed to pose a high risk for abuse of cryptoassets. One of the key vectors for this risk is in relation to ransomware attacks, payment for which is almost exclusively demanded in cryptocurrency. Ransomware attacks by Russian-based individuals and groups have been an area of enhanced concern for US and international businesses for some time, and this has been catalyzed considerably by the outbreak of conflict.[1] Indeed, a joint Cybersecurity Advisory issued in April stated that evolving intelligence indicated that the Russian government is exploring options for potential cyberattacks, and that some Russian-aligned cybergroups have recently publicly pledged support for the government, threatening to conduct cyber operations in retaliation for actions perceived to be against Russia.[2] All the while, Russia maintained variable policies towards the regulation of its own evolving cryptoasset market before this crisis.
2. In late 2021, the US government took sustained and coordinated interagency and international action against Russian-associated cryptocurrency exchanges. On September 21, the Treasury Department's Office of Foreign Assets Control (OFAC) designated Suex OTC, aka Successful Exchange, the first virtual currency exchange for laundering cyber ransoms.[3] The Treasury Department found that Suex OTC operated out of locations including Federation East Tower in Moscow, Russia.[4] OFAC concurrently updated its ransomware sanctions advisory.[5] In October 2021, OFAC released new guidance specifically for cryptoassets, "Sanctions Compliance Guidance for the Virtual Currency Industry".[6] On November 8, 2021, OFAC sanctioned two ransomware operators operating from Russia as well as Chatex, a cryptoasset exchange related to Suex OTC; interagency and international partners took coordinated civil and criminal actions.[7] The Treasury Department's Financial Crimes Enforcement Network (FinCEN) also published an updated advisory for financial institutions on ransomware and the use of the financial system to facilitate ransom payments.[8]

US government outreach to industry on sanctions evasion risks

3. From the outset of the crisis, media reports focused attention on the potential for Russian sanctions evasion efforts through the use of cryptoassets. Consensus exists that Russia could not use cryptoassets to entirely, or evenly substantially, substitute for losses caused by robust, multilateral, and coordinated sanctions, because of the limited overall market capitalization of cryptoassets, and predominant use of centralized, regulated exchanges, as well as liquidity constraints.[9]

---

1. Morgan Chalfant and Maggie Miller, The Hill, October 13, 2021, "Russia Excluded from Virtual White House Meeting on Ransomware", https://thehill.com/policy/cybersecurity/576417-white-house-convenes-virtual-meeting-of-countries-to-counter-ransomware/
2. Cybersecurity & Infrastructure Security Agency, Joint Cybersecurity Advisory, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure", https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
3. U.S. Department of Treasury, Office of Foreign Assets Control, September 21, 2021, "Treasury Takes Robust Actions to Counter Ransomware", https://home.treasury.gov/news/press-releases/jy0364
4. U.S. Department of Treasury, Office of Foreign Assets Control, September 21, 2021, "Publication of Updated Ransomware Advisory; Cyber-related Designation", https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921
5. U.S. Department of Treasury, Office of Foreign Assets Control, September 21, 2021, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments", https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
6. U.S. Department of Treasury, Office of Foreign Assets Control, October 2021, "Sanctions Compliance Guidance for the Virtual Currency Industry", https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf
7. U.S. Department of Treasury, November 8, 2021, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange", https://home.treasury.gov/news/press-releases/jy0471; U.S. Department of Treasury, November 8, 2021, "Cyber-related Designations and Designations Updates", https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211108.
8. U.S. Department of Treasury, Financial Crimes Enforcement Network, November 8, 2021, "FinCEN Advisory FIN-2021-A004 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments", https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN Ransomware Advisory_FINAL_508_.pdf
9. See, e.g., Aidan Arasingham and Gerard DiPippo, Center for Strategic and International Studies, March 15, 2022, "Cryptocurrency's Role in the Russia-Ukraine Crisis", https://www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis

4. However, the US government took steps to engage industry and the public on the sanctions evasion risks posed by Russia. As the invasion began, Treasury Department and White House officials directly appealed to large cryptoasset currencies, including centralized exchanges, to ensure that their platforms were not being used for sanctions evasion.[10]
5. Publicly, Treasury Department officials downplayed the sanctions evasion risks posed by cryptoassets. Todd Conklin, Counselor to the Treasury Department Deputy Secretary, pointedly stated "you can't flip a switch overnight and run a G20 economy on cryptocurrency".[11]
6. However, the US government simultaneously recognized the potential risks from cryptoassets to facilitate sanctions evasion. FinCEN published a March 7, 2022, alert on Russian sanctions evasion attempts; the alert dedicated an entire section to sanctions evasion using what the Treasury Department often calls convertible virtual currencies (CVCs), including three red flag indicators of potential sanctions evasion using CVCs as well as a section on ransomware and associated red flag indicators.[12]
7. The possibility of sanctions evasion also raised concerns from Congress, in particular Democratic Members of the US Senate, although the prospect of crisis-related legislation remains low. Several Democratic Senators sent a letter to the Treasury Department that stated "Strong enforcement of sanctions compliance in the cryptocurrency industry is critical…"[13] Two weeks later, some of those senators introduced legislation to increase regulatory and tax reporting requirements for certain crypto-related transactions and require the Department of Treasury to report to Congress and public.[14] On the same day, the Senate Committee on Banking, Housing, and Urban Affairs held a public hearing with crypto industry and academic experts, including a former acting director of FinCEN, a blockchain analytics firm, and a Ukrainian-based cryptoasset exchange.[15]

Post-invasion US enforcement actions taken

8. The US government has taken several public measures against Russian malign actors in the cryptoassets space since February 2022. As the crisis unfolded, the US Justice Department seized Hydra Market, a darknet marketplace used in Russian-speaking countries that transacted over US$2.5 billion in cryptocurrencies, coordinated with German law enforcement to seize servers and cryptocurrency wallets, and indicted a Russian national for operating and administering the servers.[16] Concurrently, OFAC sanctioned Hydra Market and Garantex, a virtual currency exchange operating in the same Federation Tower as sanctioned Suex OTC.[17] These actions also incorporated interagency and international cooperation, including with authorities in Estonia.
9. On April 9, 2022, OFAC took its first ever sanctions designation action against a virtual currency mining company, Bitriver AG, as part of a wider sanctions designation announcement. According to OFAC, Bitriver AG was "founded in Russia in 2017 and currently operates out of three offices across Russia."[18] OFAC designated Bitriver AG under Executive Order 14024 "for operating or having operated in the technology sector of the Russian Federation economy."[19]

---

10. Ben Bartenstein and Allyson Versprille, Bloomberg, February 28, 2022, "U.S. Prods Exchanges to Thwart Crypto Use by Sanctioned Russians", https://www.bloomberg.com/news/articles/2022-02-28/u-s-prods-crypto-exchanges-to-thwart-russia-sanctions-dodgers
11. TRM Labs, March 7, 2022, "5 Key Takeaways on Russia Sanctions: Unpacking TRM's Exclusive Interview with Senior U.S. Government Officials", https://www.trmlabs.com/post/trm-talks-russia-sanctions-what-did-they-say
12. U.S. Department of Treasury, Financial Crimes Enforcement Network, March 7, 2022, "FinCEN Alert FIN-2022-Alert001 FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts", https://www.fincen.gov/sites/default/files/2022-03/FinCEN Alert Russian Sanctions Evasion FINAL 508.pdf
13. Sens. Elizabeth Warren, Mark Warner, Sherrod Brown, and Jack Reed, March 2, 2022, Letter to Department of Treasury Secretary Janet Yellen, https://www.warren.senate.gov/imo/media/doc/2022.03.01 Letter to Treasury re OFAC crypto sanctions enforcement.pdf
14. Senator Elizabeth Warren, March 17, 2022, "Warren, Reed, Warner, Tester, Colleagues Introduce the Digital Assets Sanctions Compliance Enhancement Act of 2022", https://www.warren.senate.gov/newsroom/press-releases/warren-reed-warner-tester-colleagues-introduce-the-digital-asset-sanctions-compliance-enhancement-act-of-2022
15. U.S. Senate Committee on Banking, Housing, and Urban Affairs, March 17, 2022, "Hearing on Understanding the Role of Digital Assets in Illicit Finance", https://www.banking.senate.gov/hearings/understanding-the-role-of-digital-assets-in-illicit-finance
16. U.S. Department of Justice, April 5, 2022, "Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace", https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace
17. U.S. Department of Treasury, April 5, 2022, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex", https://home.treasury.gov/news/press-releases/jy0701
18. U.S. Department of Treasury, April 20, 2022, "U.S. Treasury Designates Facilitators of Russian Sanctions Evasion", https://home.treasury.gov/news/press-releases/jy0731
19. Ibid.

Humanitarian response and capital flight

10. The crisis has also demonstrated other use cases for cryptocurrencies as a store of value and a medium of exchange. At the outset of the conflict, Ukrainian government agencies, including its defense ministry, began requesting and accepting donations of cryptoassets to support its war effort. Estimates vary but these donations likely totaled over US$100 million equivalent.[20] While this amount pales in comparison to the tens of billions of dollars in assistance by partner governments, including the United States, this assistance use case, benefiting from anti-money laundering (AML) controls through blockchain analytics firms, shows how value can be sent responsibly to a conflict zone in a timely manner.[21]
11. Alternately, reports exist that Russians are using cryptoassets to facilitate capital flight from Russia, including to high-risk jurisdictions like the United Arab Emirates.[22] While this does not necessarily indicate sanctions evasion, such use of alternative asset classes in times of crisis may create additional financial crime compliance risks. Russians, particularly those abroad, may also seek to use cryptoassets given the sanctions imposed against Russian financial institutions which makes opening or maintaining bank accounts more difficult.[23]

Practical Steps for Compliance

- Review the March 7, 2022 FinCEN Alert on potential Russian sanctions evasion attempts, including the red flag indicators on convertible virtual currencies (CVCs) to integrate into existing compliance programs.
- Review the 2019 OFAC guidance "A Framework for OFAC Compliance Commitments", and OFAC's October 2021 Sanctions Compliance Guidance for the Virtual Currency Industry, to update compliance controls to reflect current bureau guidance.
- Continue to monitor for new or irregular account activity that serves as an on or off-ramp for cryptoassets. The US government has identified risks posed by transactions through nested exchanges and high-risk exchanges.
- Participate in public-private and private-private information sharing programs, including on ransomware, where applicable and appropriate. Cryptoasset service providers can share relevant intelligence through the voluntary disclosure of information made possible under Section 314(b) of the USA Patriot Act.
- Update compliance policies, procedures, and systems to account for new types of OFAC sanctions, such as against virtual currency exchanges and virtual currency mining companies.
- Ensure consideration of ransomware sanctions and wider financial crime risks, and take appropriate steps to mitigate them – for example through policies and procedures, training, and an effective cyber incident response plan. Review the OFAC Ransomware Advisory and FinCEN Ransomware Advisory for further information on ransomware sanctions risks, as well as viewing the recent ACAMS Masterclass on the nexus of ransomware, sanctions, and cryptocurrency.

20. See, e.g., PYMNTS.com, March 31, 2022, "Ukrainian Aid in Crypto Donations Reaches $136M", https://www.pymnts.com/cryptocurrency/2022/ukrainian-aid-crypto-donations-reaches-136-million-dollars/
21. Michael Chobanian, Blockchain Association of Ukraine, March 17, 2022, Written Statement Before the United States Committee on Banking, Housing, and Urban Affairs, https://www.banking.senate.gov/imo/media/doc/Chobanian Testimony 3-17-22.pdf
22. Simeon Kerr, The Financial Times, March 10, 2022, "Wealthy Russians Flock to Dubai as West Tightens Sanctions", https://www.ft.com/content/d6d3b45a-35cc-4e32-b864-b9c0b1649a79
23. Ibid.

ACAMS Contacts

Justine Walker, Global Head of Sanctions, Compliance and Risk
Joby Carpenter, Global SME – Cryptoassets and Illicit Finance

Developed in partnership with **Alex Zerden,** ACAMS co-opted expert/CNAS Adjunct Senior Fellow

July 7, 2022

Disclaimer

The content contained herein is for general information purposes only and is neither legal nor business advice. You should consult your own legal and business advisors for advice that applies to your particular situation.

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counter-terrorism financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives.

Visit www.acams.org/sanctions for more information.