protiviti®
Global Business Consulting

SANCTIONS SERIES

Mitigating crypto sanctions evasion risk in financial institutions

By Jackie Sanz and Bernadine Reese

The Financial Action Task Force (FATF) has long warned that criminals leverage virtual assets not only for predicate or money-laundering offenses but also to evade financial sanctions and raise funds to support terrorism.[1] Even so, the number of recent headlines about criminal activity and sanctions evasion in the crypto industry is alarming. Cryptocurrency-based crime hit an all-time high of $20.6 billion in 2022, up from $14 billion in 2021, the prior all-time high,[2,3] with no less than 43% of the illicit transaction volume in 2022 associated with sanctioned entities.[4]

For financial institutions that engage in crypto asset transactions, sanctions enforcement actions loom large. In November 2022, the U.S. Treasury's Office of Foreign Assets Control (OFAC) announced a $362,159 settlement with virtual currency exchange Kraken over the failure to block internet protocol (IP) addresses of users in Iran.[5] The New York State Department of Financial Services (NYDFS) in January 2023 reached a $100 million settlement with cryptocurrency exchange Coinbase for failing

1 *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, Financial Action Task Force, September 2020, www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.

2 *The 2022 Crypto Crime Report*, by Kim Grauer, Will Kueshner and Henry Updegrave, Chainalysis, February 2022, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

3 *The 2023 Crypto Crime Report*, by Kim Grauer, Eric Jardine, Erin Leosz and Henry Updegrave, Chainalysis, February 2023, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

4 Ibid.

5 Settlement Agreement Between the U.S. Department of the Treasury's Office of Foreign Assets Control and Payward, Inc. ("Kraken"), U.S. Department of the Treasury, November 28, 2022, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20221128#:~:text=11%2F28%2F2022%20The%20U.S.%20Department%20of%20the%20Treasury%E2%80%99s%20Office,with%20operations%20in%20the%20United%20States%20and%20elsewhere.

to onboard customers thoroughly.[6] The U.S. Department of Justice (DOJ) continues to investigate Binance, the largest cryptocurrency exchange, for an estimated $7.8 billion in money-laundering transactions since 2018 that potentially violate sanctions against Iran.[7] These examples are shots across the bow for financial institutions to focus on crypto sanctions evasion and the controls needed to ensure compliance.

Cryptocurrency-based crime hit an all-time high of $20.6 billion in 2022, up from $14 billion in 2021, the prior all-time high, with no less than 43% of the illicit transaction volume in 2022 associated with sanctioned entities.

Crypto transactions sanctions evasion risks

Despite a difference in the mechanics of cryptocurrency and fiat currency transactions, many of the risks arising from cryptocurrency transactions will be familiar to financial institutions. Still, some aspects of crypto transactions create unique risks that should be considered carefully.

The ability to move funds across borders at speed, at any time and without a face-to-face touchpoint historically required by traditional banks remains an enticing feature of cryptocurrency for criminals. Owing to these characteristics, cryptocurrencies are prone to layering (i.e., multiple, consecutive transfers of illegal funds over crypto infrastructure to obscure their origin and create the optics of legitimacy). Though blockchain is transparent to users, layering complicates and delays the process of tracing the source of funds, especially as funds are converted to cash as quickly as possible as part of the technique.

Furthermore, the use of privacy coins combined with mixers and tumblers (e.g., services that blend cryptocurrency funds) to obscure the identity of wallets and IP addresses poses a clear challenge, particularly for customer due diligence and potential money laundering activity. The anonymity that decentralised applications provide has enabled sanctioned individuals to transfer value across the world, circumventing traditional exchanges or capitalising on jurisdictional arbitrage to avoid know-your-customer (KYC) regulation or benefit from exchanges that do not have stringent sanctions controls.

While the lack of regulatory clarity and the ability to arbitrage crypto assets definitions internationally create additional compliance risks, international industry standard-setting bodies including the FATF and the Joint Money Laundering Steering Group (JMLSG) and regulators such as OFAC have made it clear that all countries need to implement measures

[6] Superintendent Adrienne A. Harris Announces $100 Million Settlement With Coinbase, Inc. After DFS Investigation Finds Significant Failings in the Company's Compliance Program, New York State Department of Financial Services, January 4, 2023, www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.

[7] "Crypto Exchange Binance Helped Iranian Firms Trade $8 Billion Despite Sanctions," by Angus Berwick and Tom Wilson, Reuters, November 7, 2022, www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/.

to ensure sanctions compliance for crypto assets.[8,9,10] Additionally, in March 2022, the U.K.'s Office of Financial Sanctions Implementation (OFSI), the Financial Conduct Authority (FCA) and the Bank of England (BoE), echoing a position already made clear by regulators in other countries, issued a joint statement asserting that "financial sanctions regulations do not differentiate between crypto assets and other forms of assets," and that "the use of crypto assets to circumvent economic sanctions is a criminal offence under the Money Laundering Regulations 2017 and regulations made under the Sanctions and Anti-Money Laundering Act 2018."[11]

The anonymity that decentralised applications provide has enabled sanctioned individuals to transfer value across the world, circumventing traditional exchanges or capitalising on jurisdictional arbitrage to avoid KYC regulation or benefit from exchanges that do not have stringent sanctions controls.

Even though financial institutions may accept virtual currency from a fully transparent intermediary (e.g., a cryptocurrency exchange) that provides the name of the account holder, and the necessary KYC data, they can't rely on others on-chain to remain compliant. Instead, they must conduct their own risk assessments and develop controls that show regulators and auditors they have integrated crypto into their sanctions compliance programs.

Risk-based approach to controls

As with sanctions compliance for fiat currency, effective cryptocurrency sanctions compliance controls should be approached on a risk basis. Institutions should consider the following preventive and detective controls as they expand their crypto asset footprint:

- Update business-wide and customer risk assessments to reflect changes in the nature and type of sanctions measures related to crypto assets. A significant variety of crypto assets has varying privacy features and different means of transacting and, as a result, different financial crime risk characteristics and vulnerabilities. The sanctions risk assessment should consider each coin, token and crypto asset offered by the institution to identify money laundering and sanctions risk

[8] "The FATF's New Sanctions Compliance Guidance for the Virtual Currency Industry," by Thorsten J. Gorny, Sanctions.io, November 14, 2021, www.sanctions.io/blog/the-fatfs-new-sanctions-compliance-guidance-for-the-virtual-currency-industry#:~:text=The%20new%20FATF%20sanctions%20rules%20require%20any%20person,to%20sanctions%20and%20ensuring%20that%20businesses%20respond%20accordingly.

[9] *Part II Sector 22 Cryptoasset Exchange and Custodian Wallet Providers*, The Joint Money Laundering Steering Group, March 2023, www.jmlsg.org.uk/wp-content/uploads/2023/03/JMLSG-Part-II_Sector-22_March-2023.pdf.

[10] Publication of Sanctions Compliance Guidance for the Virtual Currency Industry and Updated Frequently Asked Questions, U.S. Department of the Treasury, October 15, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015.

[11] Joint Statement from U.K. Financial Regulation Authorities on Sanctions and the Cryptoasset Sector, Bank of England, March 11, 2022, www.bankofengland.co.uk/news/2022/march/joint-statement-from-uk-financial-regulation-authorities-on-sanctions-and-the-cryptoasset-sector.

exposure, as well as to ensure that transfers from cryptocurrency into fiat currency are subject to appropriate scrutiny and financial crime controls. The additional measures will also help to determine the inherent versus residual risk after applying controls and whether the residual risk falls within the institution's risk appetite.

- Ensure that all customers and transactions are screened against relevant updated sanctions lists and that re-screening is in place to identify sanctions breaches. When screening, consider available technologies that permit screening down the chain (rather than limiting the screening to the immediate transaction) to allow visibility of potential sanctions breaches related to previous transactions in that coin. This action will allow institutions to understand the history of wallets and/or coins to identify likely sanctioned parties and IP addresses linked to sanctioned wallets and jurisdictions and effectively manage risk tolerance.
- Train compliance teams in blockchain analytics for use in identifying transactions linked to higher-risk wallet addresses.
- Through discussions with financial intelligence units, gather insights on the latest crypto typologies (e.g., those relating to the abuse of unlicensed or noncompliant exchanges) and additional controls, and share best-practice examples.
- Screen transactions, wallets, clients, counterparties and partners with significant exposure to sanctioned addresses. Even if an IP address hasn't been previously associated with a specially designated national (SDN) and blocked persons list at the time of a transaction, those later linked to a SDN could be a violation. IP addresses therefore need to be regularly reconciled against SDN lists. Block sanctioned individuals or businesses from signing up for or using services when IP address data is associated with sanctions. IP addresses can be used not only for security purposes but also to screen for and prevent potential sanctions violations.
- Monitor blockchain transactions to detect any sanction risks, typologies and red flags associated with beneficiaries, originators and intermediaries associated with crypto. Analysing customer transaction history for connections to sanctioned jurisdictions or transactions with virtual currency addresses that have been linked to sanctioned actors is key. Blockchain transaction monitoring will enable firms to identify instances of smurfing (e.g., the use of money mules to split funds to batches below cash-monitoring thresholds or provide false documents to surpass identification and verification).

- Implement effective blockchain monitoring solutions that allow for regular pre- and post-transaction screening and technology calibration.
- Apply event-driven reviews to detect changes in company structure, including ownership and directorship, company status, and transactions from a specific address that OFAC has identified on the SDN list.

As they develop controls, compliance teams should be aware of certain red flags that indicate increased risk, including the following:

- Customers who reside in, or are conducting transactions to and from, a country subject to sanctions
- Transactions with a wallet address associated with a sanctioned or high-risk business
- Transactions with crypto exchanges or custodian wallet providers with lax customer due diligence procedures;
- Volume and frequency of cash transactions that do not make economic sense
- Logins attempted from a nontrusted IP address or from a user's IP that was previously identified as being associated with suspicious activity
- The use of a virtual private network, mixers and tumblers.

Conclusion

Crypto asset transactions bring a unique set of challenges for financial institutions and their compliance teams. Global regulators have put institutions on alert that the cryptocurrency market is being leveraged to evade sanctions and that action must be taken. Institutions would be well advised to heed this call and adopt a risk-based approach to reassess the controls they have in place so they may mitigate evasion threats and avoid penalties.

About the authors

Jackie Sanz is a managing director in Protiviti's Risk & Compliance practice. Based in Toronto, Sanz has been the chief compliance officer, chief privacy officer, chief anti-money laundering officer and senior complaints officer of an international asset manager and fund company with locations in Australia, Canada, Hong Kong, Ireland, Peru, Singapore and the U.S. She has also played the same role for a Canadian trust company. Sanz spent three years in Luxembourg focused on société d'investissement à capital variable (SICAV)/fonds commun de placement (FCP) for offshore distribution as well as Cayman Islands and British Virgin Islands funds.

Bernadine Reese is a managing director in Protiviti's Risk & Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 25 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimising their risk and compliance arrangements. She is a Certified Climate Risk Professional.

Acknowledgments: Protiviti Senior Manager Sahaar Alouan contributed to this paper.

About Protiviti's Financial Crime practice

Protiviti's Financial Crime practice specialises in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of AML/combating the financing of terrorism (CFT) and sanctions risk assessment, control enhancements and change capability to deliver effective operational risk and compliance frameworks. Our team of specialists assists organisations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

© 2023 Protiviti Inc. PRO-0323-IZ-ENG
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®