Professional Perspective

Navigating Russia Sanctions Compliance in the Crypto Space

Paul Hinton, The Brattle Group, & Sid Kamaraju, Pryor Cashman LLP

Bloomberg Law

Navigating Russia Sanctions Compliance in the Crypto Space

Contributed by Paul Hinton, The Brattle Group, & Sid Kamaraju, Pryor Cashman LLP

June 2022

The US and European governments' sanctions, embargos, and export controls imposed on Russia in response to its invasion of Ukraine pose compliance challenges and heightened enforcement risks. These sanctions apply not only to traditional financial institutions, namely banks, but also to money services businesses (MSBs) such as crypto exchanges and custodial wallet providers using convertible virtual currencies (CVCs), more commonly known as cryptocurrency businesses.

This article identifies some known limitations of traditional surveillance strategies centered on list-based screening and details particular compliance challenges facing cryptocurrency businesses. It also examines how past regulatory investigations demonstrate the sophistication needed to implement a risk-based approach to compliance, as advised by the Office of Foreign Assets Control (OFAC), to ensure financial services businesses are not exploited to conduct prohibited or illicit activities. Finally, the article presents the considerable benefits of staying ahead of the constant adaptations of sanctioned actors to circumvent sanctions and anti-money laundering (AML) procedures.

DOJ Taps Crypto Task Force for Compliance

The Department of Justice (DOJ) assigned a dedicated interagency task force—called KleptoCapture—with the responsibility for the investigation, regulatory enforcement, and prosecution of violators of sanctions measures affecting businesses in the cryptocurrency space. The task force declared that combating the "use cryptocurrency to evade US sanctions, launder proceeds of foreign corruption, or evade US responses to Russian military aggression" is one of their "targeted efforts."

Institutions' surveillance systems and compliance personnel may find it difficult to scale-up operations to match the expanded number of sanctioned targets. Any existing weaknesses in sanctions compliance or the Bank Secrecy Act's (BSA) AML regulations—including "know your customer" (KYC) requirements and Travel Rule obligations—are also likely to be exacerbated.

According to DOJ, targets of the KleptoCapture task force can expect to be subjected to the "most cutting-edge investigative techniques—including data analytics, cryptocurrency tracing, foreign intelligence sources, and [the integration of] information from financial regulators and private sector partners" to enforce OFAC sanctions.

Compliance Challenges in Traditional Finance

The increase in sanction designations of Russian nationals and entities represents a challenge for banks to scale their list-based screening practices. While necessary, routine screening practices based on a list of sanctioned institutions or individuals—e.g., the OFAC's Specially Designated Nationals (SDN) list—or geolocations/IP addresses are unlikely to be sufficient on their own to detect and prevent money laundering, sanctions evasion, and other illicit financing activities.

List checking is not necessarily sufficient to satisfy the legal requirement to implement a program "commensurate with the risks posed by … the [MSB] services." This is particularly the case given that sanctions violations are typically strict liability offenses, and—in the event of a violation, even if an unwitting one—a company may very well find itself having to defend its sanctions compliance program to OFAC to avoid civil penalties.

The ability of targeted organizations to adapt to the imposition of sanctions by setting up new front companies means that list-based screening is always one step behind. Furthermore, OFAC's 50% rule extends sanctions to entities that are majority-owned by SDN individuals or companies or even a combination of such SDN list entities. KYC practices may not go far enough when what is needed is to identify whether a customer's customer or a licensee's sub-contractor has been sanctioned. For these reasons, understanding the relationships and networks surrounding sanctioned actors is key to managing risks of violations.

For example, the US's March 2022 ban on the exportation and re-exportation of luxury goods to Russia obligates companies in those industries not only to identify whether their direct counterparties are Russian but also whether they face any exposure from the resale of their goods to a Russian company downstream. Similarly, the broad spectrum of imposed sanctions requires compliance groups to understand and implement complicated risk detection and analysis procedures. Companies have to distinguish, for example, between entities that have been designated as SDNs—and thus are fully barred from US markets—and ones that are simply pursuant to menu-based sanctions that may only limit certain types of transactions.

A risk-based approach that goes beyond listed companies involves identifying the most active counterparties of known entities and, in turn, their largest counterparties. Some AML compliance systems provide real-time network analytics and use machine learning strategies to link customers, networks, and unknown counterparties to improve the ability to flag suspicious transactions that do not name a sanctioned entity. Banks whose systems fall short of standards expected by regulators face the risk of enforcement action.

For example, in March 2022, the Financial Crimes Enforcement Network (FinCEN) fined USAA Federal Savings Bank $140 million for failing to implement and maintain an AML program that met the minimum requirements of the BSA over a five-year period ending in April 2021. In that case, the bank also admitted that it willfully failed to accurately and punctually report thousands of suspicious transactions to FinCEN, including those in which customers were found to have used personal accounts for apparent criminal activity.

Compliance Challenges for the Crypto Industry

The ban on certain Russian banks from the SWIFT network, the freezing of US dollar and Euro-denominated assets,and the effective prohibition of Western banks from serving Russian clients raise questions about whether sanctioned Russian entities—including the state—will increase their use of Bitcoin or other cryptocurrencies. This, in turn, will likely result in a greater regulatory focus on the sanctions compliance of cryptocurrency businesses, many of which have only recently implemented AML systems.

However, there is skepticism among cryptocurrency and blockchain experts that there is sufficient liquidity outside of crypto exchanges and other centralized CVC MSBs that have adopted AML and sanctions controls to make this feasible to any material extent.

In Venezuela, President Nicolás Maduro launched a national cryptocurrency—the petro—in 2018 to help the country evade US sanctions, but it is unclear whether the petro was successful in doing so. While domestic use of cryptocurrencies in Latin America may provide protection against local currency depreciation, use for sanctions evasion is more challenging. To circumvent banks—needed to convert to fiat currencies—or crypto exchanges that adhere to sanctions, successful sanctions evasion would depend on convincing counterparties to accept digital payment directly.

Even if it may prove infeasible for sizeable Russian companies—particularly oil companies, which typically trade internationally in US dollars—to switch to crypto to evade sanctions, the prohibition of US dollar and Euro transactions will likely still make crypto transactions a more attractive channel, not least for sanctioned individuals. However, OFAC's September 2021 designation of virtual cryptocurrency exchange SUEX OTC as an SDN for facilitating ransomware payments and sanctions evasion shows that US regulators are eager to scrutinize cryptocurrency companies with weak AML practices. FinCEN too has signaled a stout enforcement posture on cryptocurrency companies by imposing a $100 million fine against BitMEX in August 2021 for willful failures to implement and maintain a compliant AML program and report suspicious activity.

The evolving regulatory environment in which crypto exchanges and other CVC MSBs operate makes it unclear how comprehensive and effective their current implementations of the Travel Rule and OFAC sanctions obligations are. Blockchain transactions are not inherently compliant with the Travel Rule but generally require separate messaging protocols to exchange the required originator and beneficiary information with counterparties.

The industry is still working out the interoperability of alternative competing messaging protocols to implement the Travel Rule, suggesting the current state of implementation is incomplete. Sanctions compliance steps based on customer identify, transaction activity, including IP address blocking, do not depend on Travel Rule implementation, but the availability of counterparty information via Travel Rule implementation may raise expectations of the extent of necessary counterparty due diligence.

The scale, timing, and coordination of US and European measures will test the effectiveness of sanctions in achieving foreign policy objectives. They will also test the crypto industry to meet AML obligations and effectively mitigate any illicit finance and national security risks posed by the misuse of digital assets. The course of international events will eventually reveal the impact of sanctions. Sanctions enforcement will adjudicate between the rhetoric of crypto-skeptics and converts on the question of whether crypto and blockchains are more or less vulnerable to illicit finance activity than traditional finance.

Ramped-up enforcement may accelerate innovation in crypto AML and sanctions compliance. Ultimately, this could produce real-time capabilities superior to those of traditional finance and accelerate competition for blockchain-based money transfer services as alternatives to SWIFT.

The transparency of the entire history of precedent transactions on public blockchains makes it possible to trace transactions across counterparties more easily and re-test entire histories when sanctioned entity lists are updated. In traditional finance, such tracing would only be possible by stitching together internal bank records from each counterparty, and the more labor-intensive costs of testing and re-testing are undoubtedly higher.

Blockchain analytics tools are also being used increasingly successfully in tracking illicit financial flows, exemplified by the FBI's recovery of more than half of the 75 Bitcoins paid in the 2021 Colonial Pipeline ransomware attack–$2.3 million of the $4.3 million paid. Such analytics, combined with the transparency features of blockchain technology and the centralized reality of pools of liquidity in the crypto ecosystem, could advance rather than exacerbate efforts to control illicit finance.

Investigative & Enforcement Methods

Investigations into potential sanctions violations across traditional banks and cryptocurrency businesses necessarily involve more extensive and intensive analysis. The methods employed in investigations can provide pointers for improvements in routine surveillance and identify a focal point of risk-based compliance activities recommended by regulators.

Such methods may include network analysis and tracing methods to map connections between all entities and follow fund flows rather than looking for known sanction targets in isolation. When screening processes flag outlier activity, internal investigations also benefit from employing these more advanced methods.

Network analytics techniques can prove useful in identifying activity patterns between entities based on timing and volumes rather than filtering transactions based on entity names. These methods can reveal which entities to look at and are not limited by the known entity names, which may have been superseded by successor entities launched to evade detection.

Tracing procedures that link transactions of a similar size and approximate timing allow for transaction fees and settlement timing mismatches and do not depend on exact matches between stated names of beneficiaries and recipients–which are often abbreviated or misspelled. Textural analysis algorithms or fuzzy match procedures can help overcome these challenges, and machine learning techniques can be helpful to find likely matches without the need for manual review.

When looking for overall patterns, exact matching accuracy is less important than picking up enough of the actual connected activity to advance an investigation. These network analysis methods make it possible to reveal meaningful patterns across large volumes of data that would be impractical to review manually.

Methods of graph analysis provide new ways of identifying relations between entities in large, complex networks of transactions with different measures of connectedness. Data visualization tools–such as Sankey diagrams to depict aggregate flows between entities and directed acyclic graphs (DAGs) to map flows across networks–are then essential to represent and navigate these patterns.

Internal investigations may involve integrating data from different operational systems, while external investigations by regulators go further to connect data obtained from other related entities. Hosting and linking disparate data sources, including transaction data and associated communications or documentation, can be critical in creating further opportunities to leverage data analytics and machine learning to connect textural sources with transaction activity without the need for manual review.

FinCEN's guidance for MSBs emphasizes that sanctions and BSA AML and counterterrorism financing (CTF) regulations do not end at the boundary between traditional finance and the CVC business. This makes it important to have the ability to integrate data sources on financial flows between fiat and crypto, encompassing SWIFT messaging and blockchain transactions in cryptocurrencies.

Some have described the scale of the sanctions against Russia as unprecedented, but it is the level of coordination and speed—rather than scale—that distinguishes the posture with Russia from how the US has approached sanctions against Iran. Consequently, we may draw relevant insights on what evasion strategies to expect from the results of sanctions enforcement against MSBs that facilitated the Iran oil trade in breach of US sanctions over the last decade.

The most high-profile enforcement action was the criminal prosecution of Reza Zarrab, who served Iranian clients through his MSBs in Turkey between 2010 and 2015, and of Mehmet Hakan Atilla, one of the Turkish bankers who provided Zarrab's businesses access to the international banking system. This case revealed how a network of related front companies could process $20 billion in Iranian oil proceeds and make the laundered funds available in the United Arab Emirates for use by Iranian clients under the cover of a trail of falsified trade documentation.

The Zarrab case also revealed how the channels of illicit activity adapted as the sanctions regime tightened, which in turn created opportunities for detection. Just as KYC is intended to provide a means of testing whether activity associated with particular accounts is unusual, systematic changes in activity that are correlated with the timing of the imposition of sanctions can flag entities that have something to hide. These changes include the appearance of new front companies that have no logical connection to the trade or are located in a different jurisdiction, unusual contractual provisions, switches in payment currencies, and changes in falsified documentation to mirror the change in sanctions.

Proactive Management of Enforcement Risk

DOJ's focus on enforcing sanctions against Russia, its institutions, and its persons creates strong incentives for financial institutions to be proactive in responding to compliance risk events to avoid enforcement action and protect their businesses. Investments in enhanced surveillance and internal investigation capabilities may also create business opportunities to operate in high-risk markets with more confidence.

Moreover, by proactively searching out and analyzing sanctions risks, companies can work to minimize the disruption to their businesses that can occur when new sanctions are imposed, at times seemingly out of the blue. For example, US companies are likely to find that their Russian customers can no longer pay them for goods already purchased—recognizing this risk early on can help companies mitigate it.

OFAC has a stated policy of crediting the efficacy of risk-based sanctions compliance programs as a mitigating factor in any enforcement action. In light of this policy, the increased focus on sanctions enforcement in response to the Ukraine invasion may increase the value of revisiting existing controls and reporting to ensure practices remain effective in this higher-risk environment.

The diversity of sanctions imposed means that companies need to understand and apply the nuances of the restrictions. For example, even though a customer may not be an SDN, they may still be designated under sectoral sanctions that would limit the kinds of payment terms the customer can receive.

OFAC also credits internal investigations that result in voluntary self-disclosure. Pursuant to the OFAC Enforcement Guidelines, self-disclosure may result in a 50% reduction in the base amount of any proposed civil penalty. Investigations may also help identify enforcement risks that can be mitigated through obtaining OFAC interpretive guidance, which may be requested to clarify regulatory requirements, or even exemptions. Institutions may create a safe harbor for specific activities by applying for OFAC licenses to authorize transactions or activities that would otherwise be prohibited.

The international sanctions on Russia for its invasion of Ukraine depend on the collective action of the private sector to implement prohibitions and controls. The months ahead will reveal whether the private sector can meet this challenge—and if it can do so ahead of rising risks of enforcement.