CAPCO

REGULATORY UPDATE:
HOUSE FINANCIAL SERVICES SUBCOMMITTEE PROVIDES UPDATES ON SCHEMES TO EVADE US SANCTIONS

All "U.S. Persons" are required to comply with prohibitions on transactions with designated sanctions targets as determined by the Department of Treasury's Office of Foreign Asset Control ("OFAC")[1]. As discussed below, opportunities to evade sanctions are abundant, despite the extensive nature of their coverage. Therefore, it is imperative that a financial institution's sanctions compliance program continues developing to meet ever-evolving efforts toward evasion. This paper summarizes a recent U.S. government hearing regarding sanctions, discusses methods of evasion – both "traditional" and "non-traditional" – and suggests steps financial institutions can take to avoid violations and financial penalties.

On June 16, 2021, the House Financial Services Subcommittee on National Security, International Development, and Monetary Policy held a virtual hearing titled "Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes." The hearing was focused on the United States' current economic sanctions program, the role of the OFAC, and the Financial Crimes Enforcement Network ("FinCEN"). The key discussion points during the hearing were the current methods of sanctions evasion being used, the role of cryptocurrency in financing sanctioned groups, and the responsibilities of financial institutions in sanction enforcement.

The hearing began with the chairman of the subcommittee, Rep. Jim Himes (D-CT), emphasizing the role of sanctions in the U.S.' foreign policy agenda, stating, "Sanctions have succeeded in isolating human rights violators or enemies of the United States. … Without sanctions, military action is more necessary to maintain order." Himes also mentioned two relevant pieces of legislation– the Corporate Transparency Act and the Anti-Money Laundering Act – about which he commented, "These bills give law enforcement the resources and authority to better track money launderers, including sanction evaders, and their success will depend in large part on this body adequately funding their implementation." The ranking member of the subcommittee, Rep. Andy Barr (R-KY), appeared in agreement, adding, "as technology develops and adapts to changing threat frameworks, our adversaries change their playbook." The hearing witnesses included experts in the cryptocurrency, financial, and foreign affairs fields and consisted of:

- Ivan A. Garces, Principal and Chair, Risk Advisory Services, Kaufman Rossin
- Eric B. Lorber, Senior Director, Center on Economic and Financial Power, Foundation for Defense of Democracies
- Lakshmi Kumar, Policy Director, Global Financial Integrity
- Jesse Spiro, Global Head of Policy & Regulatory Affairs, Chainalysis
- Dr. Jeffrey W. Taliaferro, Professor, Department of Political Science, Tufts University

The United States maintains a comprehensive sanctions program that targets nations, specific individuals, companies, and institutions that are enemies of the state or antithetical to foreign policy objectives. As stated by Congressman Himes, sanctions are intended as a step before military action, and are intended to prevent illicit behavior or to compel bad actors to change their policies. Currently, the U.S. maintains sanctions programs against Iran, North Korea, Venezuela, and Russia, along with a variety of associated individuals and groups that assist in financing these nations. These bad actors use a variety of methods to circumvent economic sanctions to not only finance their operations but gain access to U.S financial markets. Often used to make large purchases or launder money from sanctioned states, front or "shell" companies have no employees or office, but exist on paper in order to maintain anonymity in transactions. Trade-based money laundering ("TBML") consists of trade arrangements that move goods or currency to mask illegal origin or destination. As stated by Kumar in her testimony, "common techniques to

[1] This includes: United States citizens and resident aliens (regardless of their location); United States businesses and any applicable foreign branches; and any person or entity in the United States.

disguise the proceeds of crime and move value through trade include misrepresenting the price, quantity, quality, type, volume, and origins of goods. This can be done through over or under invoicing, double invoicing, phantom shipments (where no good is actually moved) etc." The last main method of sanctions evasion is maritime obfuscation, which consists of maritime vessels deliberately concealing their origin, ownership, or destination. These three categories of sanctions evasion techniques are used by sanctioned nations, companies, institutions, and individuals to finance illicit operations.

Currently, OFAC maintains the Specially Designated Nationals and Blocked Person List ("SDN List"), which compiles all current targets of U.S economic sanctions, in order to assist stakeholders in preventing illicit payments or movement of currency. Financial institutions have OFAC compliance programs to screen transactions, ensuring that all payments to prohibited individuals are blocked and reported to the Department of the Treasury. As discussed by Ivan Garces, these compliance programs are costly and time-intensive as many operational components cannot be fully automated. The large volume of transactions and complexity of sanctions frameworks often leads to false positives and a need for further human screening. Garces described in his written testimony that "most importantly, in the times in which we live with an increasing number of sophisticated bad actors, financial institutions can't be expected to connect all of the dots. Efforts to enhance corporate transparency and implement a national beneficial ownership registry, such as is provided for in the Corporate Transparency Act, is a step in the right direction, but further clarification and guidance will be needed to help ensure that additional compliance risk and regulatory expectations, that won't add value to the program, are not unintentionally created for financial institutions." Additionally, Garces stressed that with further resources, financial institutions could further automate the processes, rendering a more efficient and thorough sanctions compliance program.

With the emerging role of cryptocurrency in the financial ecosystem, it is easy to assume criminals and sanctions evaders would make use of the seemingly untraceable form of payment. However, in Lorber's answer to a question from Rep. Himes regarding cryptocurrency, he characterized the present

amount of crypto use in illicit transactions as "relatively low." Lorber made clear that this level of use could change over time, but at the moment, compared to the many legitimate uses of cryptocurrency, illicit payments and transfers account for a small portion of transactions. In his recommendations for the future, however, Lorber stressed the need for more sanctions compliance programs within cryptocurrency exchanges in order to prevent misuse. Spiro concurred with this position and suggested that cryptocurrencies are not as anonymous as they may seem: "It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than other traditional forms of value transfer.… because of its inherent transparency and traceability, there are many advantages to cryptocurrency when it comes to investigating sanctions evasion."

Spiro described centralized exchanges, such as cryptocurrencies, as "choke points" in efforts to prevent sanctions evasion. He explained to the subcommittee that, when used correctly, the currently collected data "can be used to see the point of transaction between sanctioned individuals and an exchange." Specifically pertaining to the increase in ransomware attacks on U.S businesses, Spiro looked at this unfortunate development with optimism, suggesting that with the data left behind by these attacks and additional resources, investigators will be able to pull additional intelligence and uncover money laundering networks. Both witnesses in the cryptocurrency space corroborated that cryptocurrency could be a tool for bad actors, but stressed that with technological advancements, investigators will be able to examine public ledgers and better understand sanctions evasion and money laundering.

All witnesses spoke about the responsibility of financial institutions in preventing sanctions evasion and money laundering and reached a similar conclusion: financial institutions have a responsibility to prevent sanctions evasion, but the federal government has a responsibility to educate financial institutions about their obligations. Many large financial institutions have some version of an OFAC compliance program, but Lorber stressed that more U.S stakeholders need to be involved in the sanctions enforcement process. Broadly, Lorber suggested that OFAC needs to make clear to financial institutions that they have specific responsibilities in upholding economic sanctions if they operate within the U.S, and if they neglect these responsibilities, the firm may be involved in a drawn-out auditing process. However, Lorber also acknowledged that while OFAC publicizes the SDN List, financial institutions should have more access to information so they can better understand the importance of their compliance. Lorber suggested an "OFAC Exchange," where a group of financial institutions would be gathered together and given unclassified information about sanctions evasion, money laundering, and the financing of terrorism in order to "get them to harden their systems." If banks were given more comprehensive information about international financial criminals, Lorber suggested it would spur stakeholders to take a more active role in sanctions enforcement.

The witnesses at this hearing made clear that while there are massive efforts by bad actors to evade sanctions, obtain financing, and launder money, there are also a variety of tools that the United States has to enforce sanctions and prevent criminal or unfriendly regimes from conducting illicit business. Witnesses suggested that with further investment in cryptocurrency tracking technology and stronger efforts in involving financial institutions, the United States will have greater success in carrying out sanctions packages and furthering foreign policy objectives.

Financial institutions must be mindful of their OFAC compliance obligations to prevent sanctions evasions, including those presented by crypto and other virtual currencies. Given that a strict liability standard applies to unauthorized dealing with sanctions parties and/or jurisdictions, financial institutions should make use of all available resources in order to prevent illicit activity, including an "OFAC Exchange," if one is established. Risk-based compliance programs should be constantly evaluated to ensure emerging risks, including those presented by crypto-currency and similar digital transactions, are adequately addressed, especially since FinCEN emphasized that compliance obligations remain the same regardless of a transaction's denomination.

AUTHORS

Peter Dugas, Executive Director

Spencer Schulten, Executive Director

Geoffrey Lash, Principal Consultant

Ethan Parker, Center of Regulatory Intelligence

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO

JN_3321