GLI GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation

2023

Fifth Edition

Contributing Editor: **Josias N. Dewey**

glg global legal group

ENTERPRISE ETHEREUM ALLIANCE

Value Technology Foundation

WSBA WALL STREET BLOCKCHAIN ALLIANCE

CONTENTS

U.S. sanctions and cryptocurrency: Recent developments and compliance considerations

Roberto J. Gonzalez & Jessica S. Carey
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Particularly in the last two years, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"), and the U.S. government more generally, have become increasingly active in applying U.S. sanctions laws to the cryptocurrency arena. OFAC has issued guidance emphasising that U.S. sanctions apply to digital asset transactions as they do to any other type of transactions and outlining its compliance expectations for participants in the crypto space. Additionally, OFAC has not only begun to bring enforcement actions against crypto companies that violate U.S. sanctions, but has also started to impose sanctions on crypto exchanges and other entities in the crypto ecosystem deemed to be threats to U.S. national security and foreign policy interests. More recently, the U.S. sanctions imposed as a result of Russia's invasion of Ukraine have triggered increased concern that crypto transactions could be used as a method of sanctions evasion, heightening the vigilance of Treasury, the Department of Justice ("DOJ"), and other U.S. agencies with regard to the crypto space.

U.S. sanctions compliance guidance for the cryptocurrency space

Broadly speaking, U.S. sanctions prohibit U.S.-nexus[1] transactions with comprehensively sanctioned jurisdictions (currently, Cuba, Iran, North Korea, Syria, and three regions of Ukraine) or sanctioned entities and individuals, which are listed on OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List.[2] Violation of these sanctions can result in civil penalties as well as criminal prosecution. In 2018, OFAC published an FAQ confirming that sanctions compliance obligations are the same regardless of whether a transaction is denominated in virtual currency or traditional fiat currency.[3]

On October 15, 2021, OFAC published guidance outlining its compliance expectations for the cryptocurrency space (the "Guidance").[4] The Guidance reflects OFAC's efforts to engage with and provide greater regulatory clarity to participants in this innovative area. The Guidance provides an overview of U.S. sanctions, examples of sanctions-related compliance best practices for companies active in the cryptocurrency space, as well as steps that companies can take to mitigate sanctions-related risks.[5] It also discusses how each of the five pillars of an effective compliance programme laid out in OFAC's 2019 Framework for OFAC Compliance Commitments applies to the virtual currency space. These pillars are: management commitment; risk assessment; internal controls; testing/auditing; and training. This guidance was intended for U.S. companies as well as non-U.S. companies that conduct business in, with, or through the United States, with U.S. persons, or involving U.S.-origin goods.

The Guidance recognises that the internal controls a company in the virtual currency space will implement will depend on its sanctions risk profile, including the company's product and service offerings, where it operates, and other sanctions-specific risks. Appropriate

internal controls will likely include: written policies and procedures; Know-Your-Customer ("KYC") procedures; sanctions screening of transactions and parties; training for employees; and geolocation controls. With respect to geolocation, the Guidance indicates that OFAC expects that companies will not only use geolocation controls, such as as Internet Protocol ("IP") blocking, to detect the involvement of parties from comprehensively sanctioned jurisdictions, but that companies will also employ methods to detect attempts to defeat IP blocking, such as the use of VPNs. The Guidance also provides examples of "risk indicators or red flags" that actors in the cryptocurrency space should consider when monitoring and screening transactions and customers.[6]

At the same time that it published the Guidance, OFAC issued two new FAQs, which define the terms "digital currency", "digital currency wallets", "digital currency addresses", and "virtual currency" (FAQ 559) and clarify how U.S. persons can meet their obligations to block virtual currency under OFAC's regulations (FAQ 646). Specifically, virtual currency companies that maintain multiple wallets in which a blocked person has an interest may choose to block each virtual currency wallet or opt to consolidate wallets that contain blocked virtual currency (similar to an omnibus account). Further, OFAC clarified that there is no obligation to convert blocked virtual currency into fiat currency (*e.g.*, U.S. dollars), and that blocked virtual currency is not required to be held in an interest-bearing account.

It bears noting that OFAC's compliance guidance is only a starting point for crypto companies that need to implement sanctions compliance in their day-to-day operations. These companies, often aided by crypto-focused compliance and analytics firms, have had to develop their own techniques for implementing sanctions screening and investigations tailored to their particular businesses. For example, if a crypto exchange is facilitating its customer's transmission of crypto to an off-exchange wallet address, the exchange may not only screen the wallet address against the over 150 wallet addresses now listed on the SDN List, but the exchange may also choose to screen against a list of wallet addresses that have previously transacted, directly or indirectly, with sanctioned wallet addresses. These lists can be compiled in-house or by compliance firms, but how broadly to cast this net – *i.e.*, how many "hops" between a sanctioned wallet address and another address should count – is a matter of evolving compliance judgment, with no clear regulatory guideposts.

Virtual currency companies should also be mindful of sanctions compliance expectations that may apply at the state level. For example, virtual currency companies regulated by the New York State Department of Financial Services ("DFS") must comply with the Part 504 regulation, which prescribes specific elements of sanctions and anti-money laundering compliance procedures and requires one or more senior officials to certify annually the company's compliance.[7] In August 2022, the DFS announced its first enforcement action against a virtual currency company, Robinhood Crypto, which included a $30 million penalty and cited a violation of Part 504, among other violations.[8] This action shows that the compliance deficiencies that the DFS will pursue in enforcement against crypto companies are broadly consistent with those it has pursued against traditional financial institutions.

U.S. sanctions enforcement related to cryptocurrency

In the last two years, OFAC brought its first enforcement actions against two crypto companies, showing that the crypto space is firmly on the agency's enforcement radar. While these actions are novel for involving crypto, they involve compliance deficiencies that appear in prior OFAC cases.

On December 30, 2020, OFAC entered into a $98,830 settlement with BitGo, Inc. ("BitGo"), a U.S.-based company that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services.[9] OFAC determined that BitGo had engaged in transactions in apparent violation of the Ukraine, Cuba, Iran, Sudan, and Syria sanctions programmes. OFAC determined that the company failed to prevent persons it knew or should have known (based on IP address data that BitGo collected during the normal course of its business for security purposes) were located in comprehensively sanctioned jurisdictions from using its wallet service. OFAC determined that BitGo had processed 183 digital currency transactions totalling approximately $9,127 on behalf of individuals located in such jurisdictions. OFAC stated that this action highlights that "companies involved in providing digital currency services—like all financial service providers—should understand the sanctions risks associated with providing digital currency services and should take steps necessary to mitigate those risks".

OFAC cited as a mitigating factor that BitGo had implemented significant remedial measures, including: the hiring of a Chief Compliance Officer and the implementation of a new OFAC policy; IP address blocking, as well as email-related restrictions, for sanctioned jurisdictions; periodic batch screening; ensuring that end-user agreements contain sanctions provisions; and the screening of all accounts against the SDN List, including cryptocurrency addresses reflected on that list. Although the statutory maximum penalty for the apparent violations was over $53 million, OFAC applied its enforcement guidelines to reach the settlement amount of $98,830.

On February 19, 2022, OFAC entered into a $507,375 settlement with U.S.-based BitPay, Inc. ("BitPay"), a digital currency payment service provider that allows merchants to accept digital currency as payment for certain goods and services, relating to apparent violations that arose due to persons located in comprehensively sanctioned jurisdictions accessing BitPay's platform.[10] According to OFAC, BitPay allowed persons located in Crimea, Cuba, Iran, North Korea, Sudan, and Syria to transact with merchants on the BitPay platform, despite having data in its possession (including IP address and other location data) showing their location. While BitPay screened its direct customers – the merchants – against the SDN List and to ensure they were not located in comprehensively sanctioned jurisdictions, "BitPay failed to screen location data that it obtained about its merchants' buyers". Specifically, BitPay at times would receive information about those merchants' buyers at the time of the transaction, including a buyer's name, address, email address, and phone number, as well as IP address. OFAC found that BitPay had processed 2,102 digital currency transactions totalling approximately $129,000 on behalf of individuals located in sanctioned jurisdictions. OFAC stated that this enforcement action "emphasizes the importance of screening all available information, including IP addresses and other location data of customers and counterparties, to mitigate sanctions risk in connection with digital currency services".

As a mitigating factor, OFAC noted several compliance improvements undertaken by BitPay, including: implementing IP blocking; checking buyer address and email address information for indicia of sanctioned jurisdictions; and implementing a new requirement for buyers who wish to pay invoices above $3,000, which requires that they provide an email address, photo ID, and a selfie photo.

The DOJ may also criminally prosecute sanctions violations when the conduct at issue is "wilful". For example, on September 27, 2021, Virgil Griffith pleaded guilty to conspiring to violate U.S. sanctions by providing certain cryptocurrency and blockchain-related services to persons in North Korea.[11] As a part of the plea, Griffith admitted to having travelled to North Korea to attend and present at the "Pyongyang Blockchain and

Cryptocurrency Conference". While at the conference, Griffith "provided instruction on how the DPRK could use blockchain and cryptocurrency technology to launder money and evade sanctions". The plea also stated that Griffith had provided specific blockchain and cryptocurrency technology guidance to individuals whom Griffith understood worked for the North Korean government.

The unprecedented sanctions imposed on Russia as a result of its invasion of Ukraine have increased the priority of sanctions enforcement at the DOJ. As Deputy Attorney General Lisa Monaco stated: "One way to think about this is sanctions being the new FCPA." On March 2, 2022, the DOJ launched the KleptoCapture Task Force to ensure the full effect of Russian sanctions. Notably, one of the four missions of the Task Force is to "targe[t] efforts to use cryptocurrency to evade U.S. sanctions, launder proceeds of foreign corruption, or evade U.S. responses to Russian military aggression". With respect to sanctions enforcement in the crypto space, the DOJ and OFAC, along with other law enforcement partners, have "strong working relationships" that allow the agencies to "coordinate investigations, share resources, develop leads, and leverage subject-matter expertise".[12]

U.S. sanctions designations in the crypto space

The U.S. government has also sanctioned companies and other elements within the crypto space. On March 21, 2018, in response to Venezuela's attempt to evade sanctions by launching a new cryptocurrency known as "petro", the President issued Executive Order 13827, which prohibits U.S.-nexus transactions in any Venezuelan "digital currency, digital coin, or digital token", including petro.[13] On November 28, 2018, OFAC sanctioned Ali Khorashadizadeh and Mohammad Ghorbaniyan, two Iran-based individuals who converted digital currency payments into Iranian rial as part of a widespread ransomware scheme. While OFAC normally includes identifying information, such as date of birth and addresses, for the very first time it also publicly attributed virtual currency addresses to Khorashadizadeh and Ghorbaniyan. This, OFAC noted, was meant to help those in compliance roles and the virtual currency community identify transactions and funds that need to be blocked.

On September 21, 2021, OFAC announced its first designation of a crypto company – virtual currency exchange SUEX OTC, S.R.R. ("SUEX") – onto the SDN List.[14] An individual or entity's inclusion on the SDN List broadly cuts off the designated person from the U.S. economy and prohibits any transactions or dealings with the SDN that have a U.S. nexus. OFAC designated SUEX pursuant to the malicious cyber activities sanctions programme for having facilitated financial transactions on behalf of ransomware actors. Shortly thereafter, on November 8, 2021, OFAC designated another virtual currency exchange, Chatex, and its associated support network.[15] As noted in the press releases accompanying these designations, these actions were taken in the wake of rising ransomware attacks against U.S. companies, in which illicit cyber actors demanded payment from legitimate businesses, often in the form of cryptocurrency. By designating SUEX and Chatex, OFAC stated that it was disrupting a "principal means of facilitating ransomware payments and associated money laundering activities".

According to OFAC, researchers at Chainalysis found that SUEX had received over $160 million in Bitcoin from illicit and high-risk sources, with nearly $13 million coming from known ransomware operators, $24 million from cryptocurrency scam operators, and $20 million from darknet markets.[16] OFAC also determined that over half of Chatex's known transactions were connected to "illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware". OFAC also noted that Chatex had close ties to SUEX, in that it used SUEX's function as a nested exchange to facilitate transactions.

Along with designating SUEX and Chatex, OFAC also updated its Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, addressing not only the exchanges that facilitate ransomware payments, but also companies that pay the ransom demand.[17] The advisory warns that facilitating a ransomware payment may enable bad actors, including those that are related to sanctioned persons, to advance their illicit aims, including funding activities adverse to the national security and foreign policy objectives of the United States. Therefore, the advisory strongly discourages the payment of ransomware demands. It also notes that facilitating ransomware payments could potentially violate OFAC regulations if the recipient is a sanctioned person or located in a comprehensively sanctioned jurisdiction. The advisory noted that, because sanctions violations are strict liability offences, an individual or company could be subject to significant fines or penalties even if they did not have reason to know that a payment involved a sanctioned person or comprehensively sanctioned jurisdiction.

In April 2022, OFAC sanctioned three entities associated with Russia as a part of its effort to target cybercrime originating in Russia. On April 5, 2022, OFAC designated Hydra Market, the world's largest and most prominent darknet market, and Garantex, a Russian virtual currency exchange associated with illicit actors and darknet markets. OFAC also designated over 100 associated virtual currency addresses. According to Treasury Secretary Yellen, these actions, which were coordinated with international partners, were taken to send a message to criminals that "you cannot hide on the darknet or their forums, and you cannot hide in Russia or anywhere else in the world".[18] On April 20, 2022, OFAC designated BitRiver AG and 10 of its subsidiaries that operate in Russia's virtual currency mining space with the purpose of ensuring that the Russian government cannot evade or offset the impact of sanctions via the use of cryptocurrency.[19]

On May 6, 2022, OFAC took another unprecedented step by designating Blender.io ("Blender"), a virtual currency mixer.[20] According to OFAC, virtual currency mixers like Blender mix deposited crypto before sending them to their ultimate destination, a process that OFAC alleges "indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties".[21] OFAC alleged that Blender supported the malicious cyber activities of North Korea by processing $20.5 million of the $620 million that Lazarus Group stole from a blockchain project linked to the online game Axie Infinity. In a press release, Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson warned that the U.S. government would continue to target virtual currency mixers for sanctions designations because "virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests".

On August 8, 2022, OFAC announced its designation of Tornado Cash, which OFAC described as another "virtual currency mixer". According to OFAC, Tornado Cash was used to "launder more than $7 billion worth of virtual currency since its creation in 2019", including $455 million stolen by Lazarus Group in the Axie Infinity scheme, $96 million from the Harmony Bridge scheme, and at least $7.8 million from the Nomad Heist. OFAC alleged that "Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors" and vowed to "aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them".

Notably, there has been pushback from several quarters to the Tornado Cash designation. For example, Congressman Tom Emmer wrote to Treasury Secretary Yellen, arguing that the Tornado Cash Ethereum addresses on OFAC's SDN List are not subject to the U.S. government's sanctions authority under Executive Order 13694, issued pursuant to the

International Emergency Economic Powers Act ("IEEPA"), because the addresses correspond to smart contracts that are "widely distributed technological tools . . . [that] are not under the control of any entity or natural person".[22] Rather than being controlled by a company or person, Congressman Emmer argued that "the software itself is self-sufficient, as it is decentralized and open-source and will operate as an anonymizing software powered by code as long as the Ethereum network continues to operate". Similar arguments have been raised in a recent federal lawsuit filed by six U.S. individuals who used Tornado Cash for privacy and security reasons.[23] The controversy surrounding the Tornado Cash designation shows the potential limitations of applying decades-old statutes to cutting-edge technology.

Conclusion

The U.S. government's application of sanctions to the crypto area is nascent and still evolving, and it is likely that we will see additional crypto-related sanctions guidance, enforcement actions, and designations in the near term. The shape these efforts take may be partly influenced by President Biden's "whole-of-government" crypto executive order, which was issued on March 9, 2022, and tasks various federal agencies with preparing reports and recommendations about different aspects of the opportunities and risks posed by virtual assets. At the time of writing, the first set of reports are being issued, including a report by Treasury on illicit finance and crypto.[24] However, the shape of future sanctions policy and enforcement in the crypto area will likely be more heavily influenced by events in Russia and Ukraine and other geopolitical hot spots, as well as by other evolving national security and foreign policy threats.

Against this dynamic backdrop, U.S. and non-U.S. companies in the crypto space would be well advised to take the opportunity to review and, where appropriate, strengthen their sanctions compliance policies, as well as their risk assessments, due diligence procedures, and sanctions screening processes. It is also important to monitor OFAC, DOJ, and other agencies' enforcement actions to stay abreast of the latest ways in which crypto and illicit activity may intersect.

* * *

Endnotes

1. For purposes of U.S. sanctions, a U.S. nexus can arise in a variety of ways, including the involvement of U.S. persons (U.S. citizens, lawful permanent residents, or persons of any nationality located in the United States), U.S.-origin products, software, or technology, or causing or involving activity within U.S. territory (such as transactions that transit the U.S. financial system including, *e.g.*, through U.S. correspondent banking).
2. Under OFAC's 50% rule, entities that are 50% or more owned by one or more sanctioned individuals or entities are treated as sanctioned.
3. OFAC, *Questions on Virtual Currency – FAQ 560* (Mar. 19, 2018), available at https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560.
4. OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 15, 2021), available at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
5. *Treasury Continues Campaign to Combat Ransomware As Part of Whole-of-Government Effort*, U.S. Dep't of Treasury (Oct. 15, 2021), available at https://home.treasury.gov/news/press-releases/jy0410.

6. OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry*, at 17 (Oct. 15, 2021), available at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
7. 23 NYCRR § 504.3.
8. N.Y. Dep't of Fin. Services, *In the Matter of Robinhood Crypto, LLC* (Aug. 2, 2022), availableathttps://www.dfs.ny.gov/system/files/documents/2022/08/ea20220801_robinhood.pdf; N.Y. Dep't of Fin. Services, *DFS Superintendent Harris Announces $300 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations* (Aug. 2, 2022), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021; Jessica Carey, Roberto Gonzalez, and Carly Lagrotteria, *4 Takeaways from NY DFS' First Crypto Enforcement Action*, *Law360* (Sept. 6, 2022), available at https://www.law360.com/articles/1525935/4-takeaways-from-ny-dfs-first-crypto-enforcement-action.
9. U.S. Dep't of Treasury, Enforcement Release, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Dec. 30, 2022), available at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
10. U.S. Dep't of Treasury, Enforcement Release, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Feb. 19, 2022), available at https://home.treasury.gov/system/files/126/20210218_bp.pdf.
11. U.S. Dep't of Justice, Press Release, *United States Citizen Pleads Guilty To Conspiring To Assist North Korea In Evading Sanctions* (Sept. 27, 2021), available at https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-two-european-citizens-conspiring-us-citizen.
12. U.S. Dep't of Justice, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* (Sept. 6, 2022), available at https://www.justice.gov/ag/page/file/1535236/download.
13. E.O. 13827 of March 19, 2018, *Taking Additional Steps to Address the Situation in Venezuela*, 83 Fed. Reg. 55 (Mar. 21, 2018), available at https://home.treasury.gov/system/files/126/13827.pdf.
14. U.S. Dep't of Treasury, Press Release, *Treasury Takes Robust Actions to Counter Ransomware* (Sept. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0364.
15. U.S. Dep't of Treasury, Press Release, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange* (Nov. 8, 2021), available at https://home.treasury.gov/news/press-releases/jy0471.
16. Chainalysis, *Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 million from Ransomware Attackers, Scammers, and Darknet Markets* (Sept. 22, 2021), available at https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021.
17. U.S. Dep't of Treasury, Advisory, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.
18. U.S. Dep't of Treasury, Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (April 5, 2022), available at https://home.treasury.gov/news/press-releases/

jy0701#:~:text=WASHINGTON%20%E2%80%93%20Today%2C%20the%20U.S.%20Department,dangerous%20drugs%2C%20and%20other%20illegal.
19. U.S. Dep't of Treasury, Press Release, *U.S. Treasury Designates Facilitators of Russian Sanctions Evasion* (April 20, 2022), available at https://home.treasury.gov/news/press-releases/jy0731.
20. U.S. Dep't of Treasury, Press Release, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916.
21. U.S. Dep't of Treasury, Press Release, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats* (May 6, 2022), available at https://home.treasury.gov/news/press-releases/jy0768.
22. Representative Tom Emmer, Letter (Aug. 23, 2022), available at https://buckleyfirm.com/sites/default/files/Buckley%20InfoBytes%20-%20Rep.%20Emmer%20Letter%20to%20Treasury%20re%20Tornado%20Cash%20Sanctions%202022.08.23.pdf.
23. *Van Loon et al. v. Department of the Treasury, et al*. Civ. No. 6:22-cv-920, 17 (Paul, Weiss represents the plaintiffs in this action).
24. U.S. Dep't of Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (Sept. 20, 2022), available at https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

* * *

Acknowledgments

The authors would like to thank Associates Joshua R. Thompson, Alicia S. Walker, Carly M. Lagrotteria, and Kevin P. Madden for their contribution to this chapter.

Roberto J. Gonzalez
Tel: +1 202 223 7316 / Email: rgonzalez@paulweiss.com

Roberto Gonzalez is a litigation partner based in Paul, Weiss's Washington, D.C. office, and the co-chair of the firm's Economic Sanctions and Anti-Money Laundering practice. A recognised leader in the financial crimes space, Roberto previously served as the Deputy General Counsel of the U.S. Department of the Treasury, where he had oversight of the legal offices of OFAC and FinCEN and advised on significant regulatory and enforcement matters. He also previously served as the Principal Deputy General Counsel of the Consumer Financial Protection Bureau (CFPB) and, prior to that, as Associate White House Counsel to President Obama. He clerked for Justice John Paul Stevens on the U.S. Supreme Court.

Roberto has represented the world's largest banks and technology companies in a variety of sanctions and anti-money laundering investigations by the Department of Justice, the Department of the Treasury (OFAC and FinCEN), the federal banking agencies, and the New York Department of Financial Services, as well as by congressional committees. He also provides regulatory advice, compliance counselling, and deal due diligence support.

Roberto has represented various prominent companies in the crypto space, including major U.S. and non-U.S. crypto exchanges, stablecoin providers, DeFi companies, and infrastructure providers.

Jessica S. Carey
Tel: +1 212 373 3566 / Email: jcarey@paulweiss.com

Jessica Carey is co-chair of the Paul, Weiss Litigation Department, co-head of the Economic Sanctions and Anti-Money Laundering practice and a member of the firm's Management Committee. She is lead or co-lead counsel to numerous global financial institutions in confidential BSA/AML and economic sanctions government and Congressional investigations. Jessica frequently represents companies in sensitive investigations by the U.S. Department of Justice, the SEC, the CFTC, and federal and state banking regulators, including the New York State Department of Financial Services (DFS), as well as investigations by the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC), among other agencies. She has litigated numerous securities and complex commercial matters in federal and state courts across the country, including matters where billions of dollars are at stake. Jessica also represents algorithmic trading businesses, virtual currency exchanges, blockchain infrastructure platforms, and other financial technology companies in government and regulatory inquiries, including relating to AML and sanctions compliance controls.

A sampling of Jessica's recent AML and sanctions representations include a major financial institution in reviewing the bank's sanctions exposure following Russia's invasion of Ukraine, and the New York-based subsidiary of a non-U.S. bank in investigations by the DFS, FDIC, and FinCEN, involving allegations of AML deficiencies and inadequate remediation.

Paul, Weiss, Rifkind, Wharton & Garrison LLP

2001 K Street, NW, Washington, D.C. 20006-1047, USA
Tel: +1 202 223 7300 / URL: www.paulweiss.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data
Banking Regulation
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS