GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation 2027

Ninth Edition

Contributing Editor:
Josias N. Dewey
Holland & Knight LLP

WSBA WALL STREET BLOCKCHAIN ALLIANCE

glg Global Legal Group

TABLE OF CONTENTS

Preface

Josias N. Dewey
Holland & Knight LLP

Glossary

The Contributing Editor shares key concepts and definitions of blockchain

Industry Viewpoint

1 **Crypto comes of age: the making of a digital financial system**
Ron Quaranta
Wall Street Blockchain Alliance

Expert Analysis Chapters

8 **Blockchain and intellectual property: a case study**
Ieuan G. Mahony, Brian J. Colandreo & Jacob Schneider
Holland & Knight LLP

24 **Cryptocurrency and other digital asset funds for U.S. investors**
Gregory S. Rowland & Trevor Kiviat
Davis Polk & Wardwell LLP

40 **Addressing the data proliferation problem by rebuilding digital and legal frameworks**
Tom Momberg & Angela Angelovska-Wilson
DLx Law PLLC

76 **The Future's So Bright, I Gotta Wear Shades: the GENIUS Act and the future of stablecoins in America**
Richard B. Levin, Bobby Wenner, Jorge Castiblanco & Cristofer Kelman
Taft Stettinius & Hollister LLP

96 **Trends in the derivatives market and how recent fintech developments are reshaping this space**
Jonathan Gilmour, Tom Purkiss & Jamie Errington
Travers Smith LLP

106 **Blockchain taxation in the United States**
David L. Forst, Sean P. McElroy & Matthew L. Dimon
Fenwick & West LLP

117 **OFAC sanctions and digital assets: regulation, compliance, and recent developments**
Evan T. Abrams, Andrew C. Adams & Scott R. Johnston
Steptoe LLP

135 **Beyond the perimeter: non-qualifying payment stablecoins under U.S. and EU law**
Gregory Strong, Sarah Weiyang Chen & Jonathan Galea
Cahill Gordon & Reindel LLP

Jurisdiction Chapters

147 **Australia**
Peter Reeves & Emily Shen
Gilbert + Tobin

162 **Austria**
Dr. Oliver Völkel & Jara Erhard
CERHA HEMPEL

168 **Bermuda**
Steven Rees Davies, Charissa Ball & Matthew Perriment
Carey Olsen

181 **Brazil**
Vanêssa Fialdini, Mariana de Azevedo Mendonça & Jorge Augusto de Holanda Souza
Fialdini Advogados

189 **British Virgin Islands**
Patrick Ormond & Katrina Lindsay
Carey Olsen

197 **Canada**
Alix d'Anglejan-Chatillon, Ramandeep K. Grewal, Éric Lévesque & Antonin Lapointe
Stikeman Elliott LLP

212 **Cayman Islands**
Chris Duncan & Richard Munden
Carey Olsen

221 **Germany**
Finn Niklas Nitz & André Schenk
SBS Legal Rechtsanwälte

231 **Greece**
Dr Anastasia Mallerou
Bernitsas

241 **India**
Reddy Pawan Kumar & Athif Ahmed
Hash Legal

253 **Japan**
Takeshi Nagase, Takato Fukui, Keisuke Hatano & Huan Lee (Henry) Tan
Anderson Mori & Tomotsune

263 **Kenya**
Keega Gakuua Gachutha, Alphonce Odido & Faith Njeri Njaggah
Keega & Company Advocates LLP

276 **Luxembourg**
Harry Lars Ghillemyn, Tristan Husson, Loïck Kabongo & John Sunday
Woud Law

288 **Netherlands**
Wouter Dammers & Joe Jay de Haas
LAWFOX Advocaten

298 **Norway**
Gjert Melsom, Andreas Bjørnebye & Axel Naustdal Cooper
Ernst & Young Advokatfirma AS

309 **Poland**
Robert Brodzik, Jarosław Fejdasz, Jan Janukowicz & Zuzanna Kielak
Kochański & Partners

321 **Romania**
Alexandru Stănescu, Simina Negulescu, Anca Popan & Miruna Rista
Lexters

332 **Singapore**
Kenneth Pereire & Lin YingXin
KGP Legal LLC

342 **Slovakia**
Peter Varga, Roman Baranec & Vladimir Gaduš
Highgate Law & Tax s. r. o.

351 **Spain**
Alfonso López-Ibor Aliño, Olivia López-Ibor Jaume & Victoria Moreno Motilva
López-Ibor Abogados, S.L.P.

362 **Switzerland**
Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock
Homburger

378 **Taiwan**
Robin Chang, Dennis Yu & Eddie Hsiung
Lee and Li, Attorneys-at-Law

385 **UAE**
Irina Heaver & Zainab Kamran
NeosLegal

396 **Ukraine**
Peter Bilyk
Juscutum

408 **United Kingdom**
Charles Kerrigan, Erica Stanford & Katherine Murray
CMS LLP

422 **USA**
Josias N. Dewey & Samir Patel
Holland & Knight LLP

OFAC sanctions and digital assets: regulation, compliance, and recent developments

Evan T. Abrams
Andrew C. Adams
Scott R. Johnston

Steptoe LLP

Introduction

In recent years, economic sanctions have become an increasingly important U.S. foreign policy tool and the digital asset industry has become a key focus of sanctions regulators and prosecutors. Regulators and courts have been clear that U.S. economic sanctions laws apply to digital assets, but a number of questions remain regarding the application of economic sanctions to certain digital asset contexts, and the nature of blockchain technology can create complex compliance challenges that are not present in the fiat context.

This chapter provides a high-level background on U.S. economic sanctions generally and then discusses how those sanctions have been applied to digital assets. It also provides a summary of key sanctions enforcement actions in the digital asset industry and discusses compliance expectations and challenges specific to the industry.

OFAC sanctions background

In the United States, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is the regulatory agency with primary responsibility for implementing U.S. economic sanctions programmes, which are predominantly founded on the powers granted to the President via the International Emergency Economic Powers Act (IEEPA).[1] "Person" is defined broadly by OFAC to mean "an individual or entity" and "U.S. person" is typically defined to mean "any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States".[2] OFAC is also responsible for civil enforcement of violations of the programmes' prohibitions while criminal enforcement is conducted by the U.S. Department of Justice (DOJ).

Sanctions can be applied to specific persons (i.e., "targeted"), specific industries or business sectors (i.e., "sectoral"), or to entire countries or regions (i.e., "comprehensive"). The United States currently maintains comprehensive sanctions regimes against Cuba, Iran, North Korea, the Crimea region of Ukraine, and the so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine. U.S. persons are broadly prohibited from dealing with those jurisdictions in any capacity, absent a specific exemption or a licence authorising the conduct in question. Other jurisdictions, such as Russia, Belarus,

and Venezuela, are subject to a broad array of sanctions, but are not subject to the same comprehensive measures applicable to the jurisdictions listed above.[3]

The impact of U.S. sanctions can be divided into two general categories: primary sanctions; and secondary sanctions.

Primary sanctions

Primary sanctions are the prohibitions applicable to transactions and activities with a U.S. nexus, including transactions and activities occurring in the United States or in which U.S. persons, including financial institutions, are involved. In other words, primary sanctions are the penalties and prohibitions that can be enforced with either civil (by OFAC) or criminal (by DOJ) penalties for violating U.S. sanctions laws. While primary sanctions predominantly affect U.S. persons, over whom OFAC and DOJ have legal jurisdiction, they can also extend to non-U.S. persons in certain situations, such as when a non-U.S. person is involved in a transaction "that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions".[4]

The relevant prohibitions can vary from programme to programme, with some sanctions prohibiting nearly all activity involving the sanctions target and the United States or U.S. persons, wherever located. Other sanctions prohibit a narrower range of conduct, such as certain dealings in debt or equity of the sanctions target.

Primary sanctions are a "strict liability" regime, meaning that no knowledge or intent is needed for a civil violation to arise. Criminal violations can arise only from wilful conduct.

Secondary sanctions

U.S. secondary sanctions typically apply to conduct undertaken by non-U.S. persons, even if there is no direct U.S. nexus, where the U.S. government has determined that the conduct is counter to a U.S. national security or foreign policy interest. Secondary sanctions authorise the imposition of sanctions against persons determined to engage in "sanctionable" conduct.

Non-U.S. persons can be targeted for sanctions under a variety of different programmes and can be identified on a number of lists published by OFAC. The most significant and common of these lists is the Specially Designated Nationals and Blocked Persons List (SDN List).[5] When a person appears on the SDN List, the property and interests in property of such person must be "blocked" (i.e., frozen) when within the United States or the possession or control of a U.S. person, and U.S. persons are generally prohibited from dealing with specially designated nationals (SDNs).[6] Entities owned 50% or more by one or more SDNs are also considered blocked.[7]

Persons can be added to the SDN List for a broad range of conduct, such as human rights abuses, corruption, nuclear proliferation, narcotics trafficking, cybercrimes, engaging in destabilising activity in certain regions, and undermining the democratic nature of certain regimes, among many other activities.

While the most common type of secondary sanction is inclusion on the SDN List, a range of other sanctions can be imposed. Sanctionable conduct can include a variety of activities beyond the broad nefarious activities listed above; for example, providing material support or goods or services to certain SDNs or "knowingly" engaging in a "significant transaction" for or on behalf of "any person subject to sanctions imposed with respect to the Russian Federation".[8]

OFAC has significant discretion in deciding when to impose secondary sanctions and, generally speaking, is most likely to impose such sanctions where the relevant conduct aligns with foreign policy priorities of the current administration and is "material" or "significant" (in certain cases, satisfaction of those latter elements is a legal requirement for the imposition of secondary sanctions).

OFAC sanctions and digital assets

OFAC guidance indicates that the agency interprets its regulations broadly with regard to digital assets and treats digital assets in largely the same manner as fiat currency. For example, OFAC FAQ 560 states that the OFAC compliance obligations for digital currency transactions and fiat currency transactions are the same, and goes on to explain, "U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions".[9]

Blocked wallet addresses

OFAC now routinely identifies digital asset wallet addresses as blocked property of SDNs and publishes those wallet addresses in the relevant SDN List entry.[10] Bitcoin wallet addresses form the majority of these wallets, but OFAC has begun identifying wallet addresses associated with a number of other digital assets as well.

Importantly, a wallet address may constitute or contain blocked property regardless of whether it is identified on the SDN List. OFAC's inclusion of an identified wallet in an SDN List entry is intended to assist industry by publicly identifying the wallet address, but any wallet in which an SDN has a property interest, like all property and property interests of an SDN, must be blocked and reported to OFAC by U.S. persons, regardless of whether the wallet has been identified by OFAC.

Procedures to block crypto assets

OFAC FAQ 646 provides guidance on how persons holding digital assets required to be blocked by OFAC regulations should handle those assets.[11] According to OFAC, an institution may choose, for example, to block each digital currency wallet in which a blocked person has an interest, or may use its own wallet to consolidate wallets that contain the blocked digital currency (similar to an omnibus account), titled, for example, Blocked SDN Digital Currency.[12]

The FAQ adds that each of these methods is satisfactory if there are compliance controls that will allow the digital currency to be unblocked only when the legal prohibition requiring the blocking of the digital currency ceases to apply. The FAQ also explains that holders of blocked digital currency are not obligated to convert the blocked digital currency into traditional fiat currency and, distinct from traditional fiat currency blocks, are not required to hold such blocked property in an interest-bearing account. Persons holding any blocked assets, including digital currency, are also required to submit certain reports to OFAC that include annual reports for as long as the block remains in place.[13]

OFAC sanctions compliance guidance

In October 2021, OFAC published *Sanctions Compliance Guidance for the Virtual Currency Industry* (VC Compliance Guidance).[14] The guidance reiterates that OFAC rules apply to activity conducted in digital assets, highlights the strict liability nature of OFAC regulations, and summarises the general scope and structure of OFAC sanctions regimes.

The guidance also lays out sanctions compliance best practices for the digital asset industry, which it breaks into five categories, consistent with the agency's general approach to compliance programmes, including: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

Among other measures, the guidance highlights the importance of using geolocation tools, such as IP address blocking controls, and conducting appropriate know-your-customer (KYC) due diligence during customer onboarding and throughout the lifecycle of the customer relationship. The guidance also

emphasises the value of blockchain transaction monitoring and investigation software and provides non-exhaustive lists of red flags and remedial measures taken by digital asset companies that have been subject to prior OFAC enforcement actions.

OFAC ransomware guidance

On September 21, 2021, OFAC published an *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*.[15] The advisory notes that OFAC has designated a number of ransomware[16] attackers as SDNs. Other ransomware attackers may not be included on the SDN List but could be located in a jurisdiction subject to comprehensive U.S. sanctions or may be affiliated with the governments of those jurisdictions.

The advisory emphasises that "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands" and highlights that OFAC's primary sanctions are a strict liability regime (as discussed above), which can present significant complications for victims of ransomware attacks and those assisting victims, who are often unable to definitively determine the identity of the attacker and thus might not know whether a payment is being made to a sanctioned party.

The advisory further notes that companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, encourage future ransomware payment demands and also may risk violating OFAC regulations.

The advisory encourages persons to self-report ransomware attacks to appropriate law enforcement agencies. According to OFAC, the agency considers a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, made as soon as possible after the discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response by OFAC in response to the company's actions.

Both OFAC and DOJ remain active in combatting ransomware. For example, on August 14, 2025, DOJ seized over $2.8 million in cryptocurrency as part of an indictment for crimes related to the use of Zeppelin ransomware.[17] On July 13, 2026, OFAC sanctioned First VPN Service and its administrator for enabling ransomware actors, and another individual for selling "cryptors" to disguise ransomware.[18]

Country-specific considerations

Iran shadow banking

OFAC is engaged in efforts to combat Iranian "shadow banking" (i.e., the elaborate financial infrastructure utilised by Iran to attempt to evade U.S. sanctions). Digital currency has recently become a key front in this fight, with OFAC taking three major actions against alleged Iran-backed digital currency actors since September 2025.

On September 16, 2025, OFAC designated a number of Iran, Hong Kong, and UAE-based persons for actions that included "evad[ing] sanctions by laundering money through overseas front companies and cryptocurrency". The action included sanctions against an alleged "money changer who provided Hizballah with access to digital wallets in order to receive funds related to IRGC-QF commodity sales".[19]

On June 2, 2026, OFAC took a major action targeting Iran's digital currency infrastructure. It sanctioned Nobitex, which it characterised as Iran's largest digital asset exchange, along with Nobitex's senior leadership. As part of the same action, OFAC also designated three additional Iranian digital asset exchanges named Wallex, Bitpin, and Ramzinex. By OFAC's estimate, the sanctioned exchanges accounted for more than 70% of all Iranian digital asset inflows in 2025.[20]

On August 7, 2026, OFAC designated another Iran-based digital asset exchange, Aban Tether, and an international network of companies based in Georgia, Poland, and the UAE allegedly involved in the Shelbit digital currency exchange. This action is significant, as it is the first time OFAC has sanctioned a non-Iran-based digital currency exchange for transmitting funds on behalf of Iran. OFAC stated that "[t]hey executed this scheme through sprawling corporate networks and an extensive online gambling enterprise that obscured the origin of the funds and ultimately laundered the illicit proceeds for the benefit of the IRGC and regime-connected individuals".[21]

Southeast Asia scam centres

In 2024, OFAC began taking action against highly lucrative so-called "pig butchering" scam centres. As OFAC's first cyber scam press release explains, these scams "involve[] convincing victims to invest in virtual currency, or in some cases, over-the-counter foreign exchange schemes, all with the intent of defrauding them of their funds. These scams are largely perpetrated by criminal organizations based in Southeast Asia".[22]

On September 8, 2025, OFAC sanctioned additional persons in Cambodia and Burma allegedly involved in cyber scams, again emphasising the vulnerability of digital assets and the ways in which organised crime syndicates are involved in the schemes.[23]

On October 14, 2025, in coordination with the United Kingdom, OFAC announced a significant action targeting 146 targets within Prince Group, which OFAC described as a "transnational criminal empire" involved in online investment scams. Concurrent with this action, the Financial Crimes Enforcement Network (FinCEN) finalised a rule under section 311 of the USA PATRIOT Act to sever Huione Group from the U.S. financial system for laundering proceeds of virtual currency scams and heists on behalf of malicious cyber actors.[24] Finally, DOJ also unsealed an indictment against the head of Prince Group and filed "a civil forfeiture complaint against approximately 127,271 bitcoin, currently worth approximately $15 billion, that are proceeds and instrumentalities of the defendant's fraud and money laundering schemes, and were previously stored in unhosted cryptocurrency wallets whose private keys the defendant had in his possession… The complaint is the largest forfeiture action in the history of the Department of Justice".

OFAC followed up this action by targeting more than 30 additional alleged affiliates of Prince Group on June 23, 2026.[25] This last designation cited and built on the new Executive Order (EO) 14390 Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens,[26] a strong indication that this line of effort will continue to intensify in the coming years.

Russia sanctions evasion

Following Russia's invasion of Ukraine in February 2022, the United States imposed significantly heightened sanctions and export controls measures targeting Russia. Combatting the potential use of digital assets by Russia or Russian persons to evade or circumvent those restrictions has been a priority of U.S. government officials.

For example, EO 14024, entitled *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation*, specifically authorises the SDN designation of persons determined to be responsible for or complicit in "deceptive or structured transactions or dealings to circumvent any United States sanctions, including through the use of digital currencies …" where such action is for or on behalf of, or for the benefit of, directly or indirectly, the Government of the Russian Federation.[27]

OFAC FAQ 1021 further reiterates that the prohibitions imposed on Russia via EO 14024 extend to transactions in virtual currency.[28] The FAQ explains, "[s]anctioned Russian persons are known to employ a wide variety of measures in their efforts to evade U.S. and international sanctions. As such, U.S. persons, wherever located, including firms that process virtual currency transactions, must be vigilant against attempts to circumvent OFAC regulations and must take risk-based steps to ensure they do not engage in prohibited transactions".

The FAQ then provides a number of examples of activity involving digital assets that would be prohibited under OFAC rules, such as "virtual currency transactions involving the Central Bank of the Russian Federation, National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation", among others.

The FAQ concludes by noting that "OFAC is closely monitoring any efforts to circumvent or violate Russia-related sanctions, including through the use of virtual currency, and is committed to using its broad enforcement authorities to act against violations and to promote compliance".

Venezuelan petro

On March 19, 2018, President Trump issued EO 13827, entitled *Taking Additional Steps to Address the Situation in Venezuela*.[29] The order prohibits "[a]ll transactions related to, provision of financing for, and other dealings in, by a United States person or within the United States, any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela".[30]

The action was specifically aimed at the petro, which is a Venezuelan government-issued digital asset that is purportedly backed by oil and mineral reserves in the country.

However, the order applies more broadly to any other digital assets issued by, for, or on behalf of the government of Venezuela. The action marks the first and only time that OFAC issued a blanket ban on dealings in a given digital asset. However, as more countries, including those subject to comprehensive U.S. sanctions, explore central bank digital currencies (CBDCs) or other types of government-backed digital assets, it is possible that OFAC will take additional, similar actions in the future.

OFAC enforcement actions against digital asset platforms

Beginning in December 2020, with an enforcement action against BitGo,[31] OFAC has brought a series of enforcement actions against digital asset platforms. In addition to BitGo, the targeted companies include BitPay, Bittrex,[32] Kraken, Poloniex, CoinList Markets, and Binance.[33] While each enforcement action was factually unique, all of them involved the use of the platform by users located in comprehensively sanctioned jurisdictions. In a number of cases, OFAC found that the platforms had reason to know of the location of the users based on either KYC documents or geolocation data associated with a user's IP address used to access the platform. One case also involved dealing with SDNs.

Among other takeaways, the actions demonstrate the importance of using all available risk-relevant data to assist in sanctions compliance and taking measures to prevent users located in comprehensively sanctioned jurisdictions from accessing the platforms.

SDN designation of non-U.S. exchanges, mixers, and tumblers

Starting in late 2021, OFAC began a string of SDN designations focused on non-U.S. digital asset exchanges, mixers, and tumblers. The targeted platforms include SUEX, Chatex, Garantex, Blender.io, Hydra Market, Tornado Cash, Sinbad.io, and Bitpapa, among many others.[34] Most recently, OFAC re-designated Garantex and designated Grinex, which it described as "Garantex's successor" on August 14, 2025.[35] OFAC has also designated many entities and individuals that purportedly used digital assets for nefarious purposes, including money laundering, ransomware, and sanctions evasion, among other conduct.[36]

These actions highlight the significant discretion of OFAC to target actors that it believes are acting contrary to U.S. foreign policy or national security objectives, regardless of the jurisdiction of those actors and regardless of whether there is any U.S. nexus.

The SDN designations have implications both for U.S. persons and persons acting within the United States, who are generally prohibited from dealing with SDNs, and for non-U.S. persons outside the United States. Most EOs authorising the issuance of SDN designations also authorise OFAC to designate any person

determined to have "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of … any person whose property and interests in property are blocked pursuant to this order".[37] In other words, persons who deal with SDNs also risk being designated as SDNs themselves. Therefore, any person dealing with an SDN digital asset platform may face sanctions risk from OFAC.

Tornado Cash and implications for DeFi platforms

Perhaps the most contentious and widely followed OFAC action in the digital asset space has been its designation, and subsequent delisting, of virtual currency mixer Tornado Cash as an SDN.[38]

OFAC designated Tornado Cash in 2022 under EO 13694, as amended,[39] which pertains to North Korea. OFAC cited the use of Tornado Cash by the Lazarus Group, a North Korean state-sponsored hacking group, to launder hundreds of millions of dollars for the benefit of North Korea as the primary reason for the designation.[40]

When designating Tornado Cash, OFAC determined that Tornado Cash was a "person" that was eligible for designation under the relevant authorities. OFAC also identified the smart contracts underpinning the Tornado Cash protocol as property in which Tornado Cash has a "property interest" (i.e., OFAC concluded that the smart contracts were blocked property). Those findings were challenged in *Joseph Van Loon, et al. v. Department of Treasury, et al.*[41] and *Coin Center, et al. v. Yellen, et al.*[42] The government successfully defended the sanctions at the district court level in *Van Loon*, but lost on appeal before the Fifth Circuit, as discussed in further detail below. The government also prevailed in district court in *Coin Center*; however, the lower court's ruling was vacated by the Eleventh Circuit through a joint motion in July 2025, resulting in dismissal of Coin Center's appeal.[43]

Van Loon appeal

On November 26, 2024, the U.S. Court of Appeals for the Fifth Circuit ruled that OFAC exceeded its statutory authority when it designated Tornado Cash, in a rare loss for OFAC and significant victory for the digital asset industry.[44]

Before the Fifth Circuit, the appellants, comprising a group of Tornado Cash users backed by industry, argued three theories: (1) Tornado Cash is not a foreign "national" or "person"; (2) the immutable smart contracts are not "property"; and (3) Tornado Cash cannot have a property "interest" in the immutable smart contracts. The Fifth Circuit ruled only on the second argument, finding that immutable smart contracts are not property, and did not reach a conclusion with respect to the other two arguments advanced by the appellants.

In the Fifth Circuit's view, the immutable smart contracts lacked the core characteristics of property, including the ability to be owned or controlled and the ability to exclude others from enjoyment of their benefit. The court concluded that no person, Tornado Cash or others, could own or exercise dominion over the immutable smart contracts. Further, no one could update, remove, or otherwise control those smart contracts in a way that would exclude anyone from using them. The court also highlighted that because the immutable smart contracts are unchangeable and unremovable, OFAC's designation does not actually prevent persons from using the protocol or withdrawing or accessing tokens held in the protocol.

The Fifth Circuit relied principally upon a common sense understanding of the word "property", which is not a defined term in IEEPA, the statute underpinning the sanctions. Interestingly, the court placed significantly less emphasis on OFAC's regulatory definition of "property", citing the recent Supreme Court ruling overturning the so-called "*Chevron* deference" doctrine, which reduced the deference federal courts give to administrative agencies in interpreting statutes. However, the Fifth Circuit concluded that, even if it were to defer to OFAC's definition of property under IEEPA, which includes, in part, all "contracts" and "services", the immutable smart contracts would still be outside the scope of that definition. The

Fifth Circuit held that immutable smart contracts are not contracts, concluding that immutable smart contracts lacked the essential requirements of a contract because there is only one party (the third-party user) involved in a transaction with an immutable smart contract. There is no counterparty, just the immutable software code. Tornado Cash, including its founders, its developers, and its decentralised autonomous organisation (DAO), cannot "revoke" the immutable contracts even if they wished to do so because no one controls the immutable smart contracts or their operation.

The Fifth Circuit also concluded that the immutable smart contracts are not a "service" within the scope of OFAC's definition of property. The court explained that a "service" must entail human effort, and that smart contracts are more akin to a tool that is used in providing a service than a service itself. In addition, the court concluded that Tornado Cash does not own the services provided by the immutable smart contracts. The court found that nothing suggests that Tornado Cash itself receives fees from transactions through either mutable or immutable smart contracts (as opposed to adjacent software such as relayers) and that none of the immutable smart contracts entitle the creators to a benefit.

Tornado Cash delisting

On March 21, 2025, OFAC announced the delisting of Tornado Cash "[b]ased on the Administration's review of the novel legal and policy issues raised by use of financial sanctions against financial and commercial activity occurring within evolving technology and legal environments…".[45]

Future implications

Even after the *Van Loon* decision, significant uncertainty remained about Tornado Cash's future. Although Treasury's announcement appeared to resolve some of those questions, the Trump administration's decision to delist Tornado Cash, rather than pursue further appeals, may leave the door open to similar sanctions designations in the future. Treasury stated that it "remains committed to using our authorities to expose and disrupt the ability of malicious cyber actors to profit from their criminal activities through the exploitation of digital assets and the digital assets ecosystem".[46] Treasury also noted that it is "committed to enforcing our sanctions against [North Korea] to constrain the regime's ability to fund its weapons of mass destruction and ballistic missile programs".[47] Therefore, the possibility of Treasury sanctioning decentralised protocols in the future remains, particularly if the technology and economics of those protocols differ from the smart contracts used for Tornado Cash. The ruling also represents the view of only one circuit, meaning appeals courts in other jurisdictions could, potentially, reach a different conclusion if presented with the same facts.

Designation and prosecution of Tornado Cash founder

In August 2023, OFAC announced the SDN designation of Roman Semenov, one of three alleged co-founders of Tornado Cash,[48] and DOJ charged Semenov and Roman Storm, another Tornado Cash founder, with multiple alleged criminal violations related to anti-money laundering (AML) and economic sanctions laws.[49] Semenov and Storm allegedly coded Tornado Cash, held a significant number of governance tokens, and developed a frontend user interface, over which both individuals retained control, that helped users access the protocol. Users were not required to access the protocol via this frontend user interface, but, according to the indictment, the significant majority of users did use the interface.

The indictment alleged that the defendants were aware that the Tornado Cash protocol was being used by a number of malign actors to launder the proceeds of hacks and other illegal conduct, and that the defendants profited from such activity through their holding of TORN tokens (the governance token of the Tornado Cash DAO) and the implementation of a "relayer register" that required Tornado Cash relayers to purchase TORN tokens in order to be chosen to process withdrawals from the Tornado Cash frontend user interface.

The indictment further alleged that the founders made changes to the frontend user interface to prevent transactions flowing directly from wallets that had been identified as blocked property of the Lazarus Group (and others), but privately acknowledged that the measures were inadequate because they could easily be bypassed by transferring tokens from the identified wallets into a new wallet and then using the Tornado Cash frontend.

Storm and Semenov were charged with three counts, including (1) conspiracy to commit money laundering, (2) conspiracy to operate an unlicensed money transmitting business, and (3) conspiracy to violate IEEPA.[50] Given the sanctions focus of this chapter, we focus on the third count related to IEEPA (although the first two counts raise a number of important considerations with respect to AML laws in the decentralised finance (DeFi) context).

Storm sought dismissal of the IEEPA-related charges, arguing that (1) the indictment seeks to penalise the defendants for making "informational materials" available on the Internet, which is activity exempted from the scope of IEEPA, and (2) the defendants did not engage in a "wilful" violation of IEEPA, which is required for criminal violations to arise.[51] The court denied the motion to dismiss without a written ruling.[52]

In August 2025, Storm was convicted on one count of conspiracy to operate an unlicensed money transmitting business, following a four-week jury trial before the Southern District of New York.[53] The jury could not reach a consensus regarding the charges of conspiracy to commit money laundering or conspiracy to violate sanctions (though federal prosecutors could retry Storm on these two charges).[54] Semenov still faces charges, but is currently at large.[55]

Digital assets and export controls

While this chapter is focused principally on economic sanctions, it makes sense to briefly address the closely related area of export controls. Particularly since the Russian invasion of Ukraine in February 2022, the U.S. government has become increasingly focused on the potential role of financial institutions and others involved in international payments in identifying and reporting potential export controls violations. For example, the Department of Commerce's Bureau of Industry and Security (BIS) and Treasury's FinCEN have issued joint alerts urging financial institutions to exercise "increased vigilance" with respect to potential Russia and Belarus export controls evasion attempts.[56]

In terms of enforcement, on October 19, 2022, DOJ charged five Russian nationals and two Venezuelan nationals with using a complex series of transactions involving digital assets and shell companies to unlawfully obtain U.S. military technology and sanctioned Venezuelan oil.[57]

As U.S. export controls continue to expand and increase in complexity, this trend is likely to continue and digital asset platforms should consider export controls compliance in addition to OFAC sanctions.

Compliance programme considerations

OFAC regulations do not technically require any entity to implement an OFAC compliance programme, but OFAC "strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program".[58] Given this guidance, the strict liability standard under U.S. primary sanctions, and OFAC's broad discretion with respect to secondary sanctions, many entities elect to implement a robust sanctions compliance programme.[59] Moreover, many digital currency projects operating in the United States are subject to the AML and KYC requirements of the Bank Secrecy Act (BSA), whether as money services businesses or as certain Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC) registrants. These BSA obligations, in turn, effectively impose sanctions screening as a part of an effective compliance programme.

OFAC and DOJ have made clear in a number of instances that maintaining a compliance programme is an important factor when they determine whether to bring an enforcement action and what penalty to impose. For example, OFAC's *Economic Sanctions Enforcement Guidelines*, which set out general parameters regarding how OFAC approaches enforcement in the event of a violation of OFAC regulations, include maintenance of a compliance programme as one of the general factors affecting OFAC's enforcement response to an apparent violation.[60] Specifically, the agency will consider – as either a mitigating factor or an aggravating factor – the existence, nature, and adequacy of a person's risk-based OFAC compliance programme at the time of the apparent violation.

OFAC has further issued guidance entitled *A Framework for Compliance Commitments*, which outlines the key elements OFAC expects to see when reviewing an entity's compliance programme.[61] It also cites the lack of a formal OFAC sanctions compliance programme as a primary root cause of OFAC sanctions violations and notes that OFAC frequently cites the absence of such a programme as an aggravating factor in its enforcement analysis.

With respect to criminal enforcement, DOJ publishes a reference guide for prosecutors known as the *Justice Manual*, which includes a section on Principles of Federal Prosecution of Business Organizations that outlines various factors that federal prosecutors consider when taking action against a business. One of those factors is the adequacy and effectiveness of the entity's compliance programme at the time of the offence. The manual explains, "the critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or permitting employees to engage in misconduct to achieve business objectives".[62] This policy has been reenforced under the recent policy updates implemented under the Trump administration's DOJ leadership, which released the first-ever Department-wide Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP) on March 10, 2026. This document emphasises the importance of effective compliance processes in assessing a corporation's efforts to remediate in light of the discovery of federal offences.[63] On March 30, 2026, the DOJ's National Security Division (NSD) confirmed that the CEP applies to criminal matters within NSD's jurisdiction. This makes clear that the CEP framework now applies to DOJ enforcement decisions in national security matters, including cases involving export controls, sanctions, and other national security-related regulatory regimes.[64]

OFAC's VC Compliance Guidance, discussed above, also notes that all companies in the digital asset industry are encouraged to develop, implement, and routinely update a tailored, risk-based sanctions compliance programme.

Digital asset-specific compliance programme considerations

In addition to the above general sanctions compliance considerations, there are several sanctions considerations that are unique to digital asset companies. The use of blockchain analytics is a particularly important tool for the industry, and the ability to trace many digital asset transactions on public blockchains can provide detailed insight into the transactions of a given wallet, including any links to known bad actors or sanctioned persons.

Many blockchain analytics service providers offer services that can help identify whether a given wallet is specifically included on the SDN List, is associated with an SDN, or has otherwise interacted with a wallet known to belong to a sanctioned person. For privacy-enhanced blockchains with more limited publicly available information, companies should consider whether alternative means exist to mitigate the potentially heightened sanctions compliance risk of these blockchains and whether using these blockchains falls within their risk tolerance.

Both OFAC's enforcement actions and its sanctions compliance guidance highlight the importance of geolocating a user's IP address to identify whether a user is accessing a digital asset platform from a

device located in a comprehensively sanctioned jurisdiction. While sophisticated users can obscure their IP address by using a VPN or through other means, many users do not take these measures, as evidenced by OFAC's enforcement actions.

As noted above, OFAC has issued specific guidance on blocking digital assets. Digital asset companies should familiarise themselves with this guidance and consider creating written procedures for how the company will handle blocked assets. Such procedures are recommended to include periodic testing to ensure that compliance controls deployed to block digital assets are functioning properly.

There are additional and significant challenges that come with implementing compliance measures in a decentralised context, including identifying who is responsible for determining and implementing the appropriate measures and how to achieve compliance objectives while maintaining the decentralised nature of the protocol. These challenges are heightened by the fact that the movement toward greater centralisation can have important implications under other legal regimes, such as securities law and even the AML rules of certain jurisdictions that do not extend to fully decentralised platforms.

Open questions and enforcement outlook

While OFAC has noted that compliance obligations for transactions involving digital assets are the same as for fiat currency transactions, there are still many open questions with respect to how OFAC views the application of its regulations to the digital asset space. For example, the agency has not issued any formal guidance on how it views the obligations of persons such as:

- crypto miners and other validators;
- coders and developers;
- governance token holders in DeFi projects; and
- persons serving in foundations associated with specific blockchains.

In many of these instances, participants may have limited or no visibility into persons with whom they are directly or indirectly dealing or have no ability to limit the group of users with whom they directly or indirectly interact. For example, a miner validating a block in a blockchain typically has no ability to limit the transactions in that block and only limited insight into the parties to the transactions in the block.

There are also significant questions regarding the obligations of developers and coders that create and release protocols. The indictment of Tornado Cash's founders, discussed above, provides some insight into how DOJ views the compliance obligations of such persons. However, given a number of the unique facts in that case, it is unclear how broadly the lessons from that indictment can be applied.

While the industry continues to wait for additional guidance and clarity on some of these questions, it seems likely that OFAC SDN designations and enforcement actions both from OFAC and DOJ will continue and, perhaps, increase.

Recently enacted legislation and proposed regulations

Congressional interest in sanctions compliance in the digital asset space continues. Most notably, the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) was signed into law by President Trump on July 18, 2025. The GENIUS Act provides the first comprehensive framework for stablecoins – and digital assets in general – in the United States. Congress built specific economic sanctions compliance obligations into the GENIUS Act. Permitted payment stablecoin issuers (PPSIs) must maintain an effective sanctions compliance programme, including procedures to screen for and block transactions involving sanctioned persons or countries.[65] The law expressly requires verification against relevant sanctions lists (such as the SDN List) to prevent stablecoins from being used in violation of U.S. sanctions.[66] While most stablecoin issuers are already expected to have in place robust economic

sanctions compliance measures, in many cases this expectation is not explicitly built into the law and is instead something that arises indirectly from the requirement to have a "risk-based" AML compliance programme or similar broad concepts.

One of the most significant mandates is that issuers must have "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations".[67] This means issuers will need to maintain some degree of control – such as an ability to blacklist certain wallet addresses or burn tokens – despite the decentralised nature of most blockchain transactions. A number of the largest stablecoin issuers already have such functionality built into their technology. However, the GENIUS Act now makes such capabilities a legal prerequisite for operation. An issuer that cannot halt illicit transactions on its network would be barred from issuing stablecoins under the Act's standards. As detailed below, the implementation of this requirement could have significant implications for PPSIs and others in the digital asset ecosystem.

The Act also establishes a protocol for government coordination with PPSIs in enforcing sanctions. When Treasury moves to block a person's property (for instance, by adding them to the SDN List), the Act instructs Treasury to coordinate, where appropriate, with relevant PPSIs to ensure the person's stablecoin assets can be effectively frozen at the time sanctions are imposed.[68] This prevents sanctioned persons from seeing their designation and quickly converting their stablecoins into another asset before an issuer is able to freeze the tokens. Notably, while the Act encourages such coordination, it does not require advance notice to the issuer before Treasury takes action, leaving Treasury with discretion.

On April 8, 2026, Treasury announced a proposed rule to implement the GENIUS Act's illicit finance requirements.[69] Among the obligations included in the proposal are the requirement for PPSIs to:

- establish and maintain an anti-money laundering and countering the financing of terrorism (AML/CFT) programme;
- report suspicious activity;
- have the technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate federal or state laws, rules, or regulations;
- have the technical capabilities to ensure compliance with the terms of any lawful order; and
- maintain an effective sanctions compliance programme.[70]

With respect to OFAC compliance, the most significant component of the proposed rule is its assertion that PPSIs are responsible for actively monitoring the entirety of the secondary market for sanctions violations and intervening to freeze tokens where necessary. According to the proposed rule, "a U.S. person stablecoin issuer would engage in a prohibited provision of services to a blocked person if it allowed the blocked person to engage with the stablecoin issuer's smart contract to facilitate trades of stablecoins on the secondary market. In this instance, the stablecoin issuer would also be required to block such stablecoins because the blocked person has an interest in the stablecoins, which the issuer controls via its smart contract".[71]

The implications of that approach are significant given the difficulty PPSIs would face in conducting fulsome secondary market monitoring and the potential follow-on effects that could arise from secondary market freezing, such as disruptions to various DeFi protocols. As written, the logic underpinning OFAC's jurisdictional assertion does not appear limited to PPSIs but rather applicable to any blockchain developer with control over smart contracts.

Because this is a proposed rule, it is possible, if not likely, that Treasury may alter its approach in the final rule. This will be a critical area to watch for PPSIs and others across the blockchain ecosystem.

Trump administration guidance and priorities

The Trump administration has implemented a dramatic shift in attitude toward regulation of digital

assets broadly, including focusing on combatting illicit activity by bad actors, rather than "regulation by prosecution", as exemplified in the memorandum issued by Deputy Attorney General Todd Blanche entitled "Ending Regulation by Prosecution" (Blanche Memo). The Blanche Memo instructs federal prosecutors to cease "litigation or enforcement actions that have the effect of superimposing regulatory frameworks on digital assets".[72] Instead, prosecutors should focus on "prosecuting individuals who victimize digital asset investors, or those who use digital assets in furtherance of criminal offenses such as terrorism, narcotics and human trafficking, organized crime, hacking, and cartel and gang financing".[73] Despite this shift in focus, DOJ is likely to pursue certain prosecutions of digital asset companies where violations of the law implicate one of the administration's priority areas. Even in light of the Blanche Memo, actions relying on money transmission theories of prosecutions – often considered to fall closer to "regulatory" rather than "criminal" offences – have continued, such as with the *Samourai Wallet* case.[74] Therefore, the Blanche Memo should be interpreted as a shift in enforcement priority rather than a retreat from enforcement in the digital asset space.

On July 30, 2025, the Trump administration's Working Group on Digital Asset Markets issued its report on digital assets titled "Strengthening American Leadership in Digital Financial Technology" (Digital Asset Report).[75] The Digital Asset Report reiterates longstanding policy that OFAC sanctions apply in the digital asset context and indicates the Trump administration will continue to use OFAC authorities to pursue bad actors and sanctions evaders. The report highlights prior OFAC guidance, but acknowledges there is an industry demand for further guidance, which it notes "is particularly relevant for developers who are creating software in the DeFi space".[76] The Digital Asset Report recommends Treasury undertake a request for information (RFI) to solicit industry input on gaps in existing guidance, among other issues. It also recommends that Treasury update OFAC's existing VC Compliance Guidance based on input obtained through the RFI process.[77]



Endnotes

1 *See* 50 U.S.C. Ch. 35: International Emergency Economic Powers, available at https://www.law.cornell.edu/uscode/text/50/chapter-35

2 *See, e.g.*, 31 C.F.R. § 584.309 and 314, available at https://www.ecfr.gov/current/title-31/section-584.314

3 *See* U.S. Dep't Treas. Off. Foreign Assets Control, Sanctions Programs and Country Information, available at https://ofac.treasury.gov/sanctions-programs-and-country-information

4 *See, e.g.*, 31 C.F.R. § 584.205, available at https://www.ecfr.gov/current/title-31/section-584.205

5 *See* U.S. Dep't Treas. Off. Foreign Assets Control, Specially Designated Nationals and Blocked Persons List (SDN List), available at https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

6 *See, e.g.*, 31 C.F.R. § 584.201(a), available at https://www.ecfr.gov/current/title-31/part-584/subpart-B#p-584.201(a)

7 U.S. Dep't Treas. Off. Foreign Assets Control, Entities Owned by Blocked Persons (50% Rule), available at https://ofac.treasury.gov/faqs/topic/1521

8 22 U.S.C. § 8909; *see* Countering America's Adversaries Through Sanctions Act (CAATSA), Pub. L. No. 115-44 (Aug. 2, 2017).

9 U.S. Dep't Treas. Off. Foreign Assets Control, Questions on Virtual Currency: FAQ 560, available at https://ofac.treasury.gov/faqs/560

10 *See, e.g.*, multiple "Digital Currency Addresses" included in OFAC's August 7, 2026 list update, available at https://ofac.treasury.gov/recent-actions/20260807

11 *See* U.S. Dep't Treas. Off. Foreign Assets Control, Questions on Virtual Currency: FAQ 646, available at https://ofac.treasury.gov/faqs/646

12 *See id*.

13 31 C.F.R. § 501.603.

14 U.S. Dep't Treas. Off. Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021), available at https://ofac.treasury.gov/media/913571/download?inline

15 U.S. Dep't Treas. Off. Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), available at https://ofac.treasury.gov/media/912981/download?inline

16 Ransomware typically involves a hacker breaching a company's IT infrastructure and encrypting a company's data or other systems. The attacker then typically demands that the victim pay a ransom in exchange for a decryption key that allows the victim to unlock the IT systems or data. The ransom is almost always demanded in cryptocurrency.

17 U.S. Department of Justice, Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets (Aug. 14, 2025), available at https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets

18 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Malware and Infrastructure Providers Supporting Ransomware Attacks Against Americans (Jul. 13, 2026), available at https://home.treasury.gov/news/press-releases/sb0559

19 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Targets Financial Network Supporting Iran's Military (Sept. 16, 2025), available at https://home.treasury.gov/news/press-releases/sb0248

20 U.S. Dep't Treas. Off. Foreign Assets Control, Economic Fury Targets Iran's Largest Digital Asset Exchange for Terror Finance and Sanctions Evasion (Jun. 2, 2026), available at https://home.treasury.gov/news/press-releases/sb0519

21 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Crypto Exchanges Funding Iran's IRGC and Enabling Illicit Finance (Aug. 7, 2026), available at https://home.treasury.gov/news/press-releases/sb0598

22 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Cambodian Tycoon and Businesses Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams (Sept. 12, 2024), available at https://home.treasury.gov/news/press-releases/jy2576

23 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams (Sept. 8, 2025), available at https://home.treasury.gov/news/press-releases/sb0237

24 U.S. Dep't Treas. Off. Foreign Assets Control, U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia (Oct. 14, 2025), available at https://home.treasury.gov/news/press-releases/sb0278

25 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Further Dismantles Overseas Scam Operations Targeting Americans (Jun. 23, 2026), available at https://home.treasury.gov/news/press-releases/sb0538

26 White House, Executive Order 14390 (Mar. 6, 2026), available at https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens

27 Exec. Order No. 14024, 86 Fed. Reg. 20249 (Apr. 19, 2021).

28 *See* U.S. Dep't Treas. Off. Foreign Assets Control, Russian Harmful Foreign Activities Sanctions: FAQ 1021, available at https://ofac.treasury.gov/faqs/1021

29 Exec. Order No. 13827, 83 Fed. Reg. 12469 (Mar. 19, 2018).

30 *Id*.

31 *See* Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Dec. 30, 2020), available at https://ofac.treasury.gov/media/50266/download?inline

32 The case against Bittrex involved a joint action between OFAC and FinCEN, which issued a consent decree regarding alleged violations of the Bank Secrecy Act (BSA) and its implementing regulations, in addition to the sanctions violations identified by OFAC.

33 *See* Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), available at https://ofac.treasury.gov/media/54341/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of

Multiple Sanctions Programs (Oct. 11, 2022), available at https://ofac.treasury.gov/media/928746/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations (Nov. 28, 2022), available at https://ofac.treasury.gov/media/929541/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Poloniex, LLC for $7,591,630 Related to Apparent Violations of Multiple Sanctions Programs (May 1, 2023), available at https://ofac.treasury.gov/media/931701/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs (Nov. 21, 2023), available at https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf [joint action with DOJ]; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with CoinList Markets LLC for $1,207,830 Related to Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations (Dec. 13, 2023), available at https://ofac.treasury.gov/media/932406/download?inline

34 *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0364; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, 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; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex (Apr. 5, 2022), available at https://home.treasury.gov/news/press-releases/jy0701; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, 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; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency (Nov. 29, 2023), available at https://home.treasury.gov/news/press-releases/jy1933; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement (Mar. 25, 2024), available at https://home.treasury.gov/news/press-releases/jy2204

35 U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals (Aug. 14, 2025), available at https://home.treasury.gov/news/press-releases/sb0225

36 *See*, *e.g.*, Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Designates Virtual Currency Money Launderer for Russian Elites and Cybercriminals (Nov. 3, 2023), available at https://home.treasury.gov/news/press-releases/jy1874; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group (Feb. 20, 2024), available at https://home.treasury.gov/news/press-releases/jy2114; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, United States Sanctions Senior Leader of the LockBit Ransomware Group (May 7, 2024), available at https://home.treasury.gov/news/press-releases/jy2326

37 Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 2, 2015).

38 *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916

39 Exec. Order No. 13722, 82 Fed. Reg. 17331 (Apr. 10, 2017).

40 *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916

41 *See* Order, *Van Loon v. Dep't Treas.*, No. 23-cv-312-RP (W.D. Tex. Aug. 17, 2023).

42 *See* Order, *Coin Center v. Yellen*, No. 3:22-cv-20375 (N.D. Fla. Oct. 30, 2023).

43 *See* Order, *Coin Center v. Secretary, U.S. Dep't Treas.*, No. 23-13698 (11th Cir. Jul. 2, 2025).

44 *See* Order, *Van Loon et al. v. Dep't Treas.*, No. 23-50669 (5th Cir. Nov. 26, 2024).

45 *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Tornado Cash Delisting (Mar. 21, 2025), available at https://home.treasury.gov/news/press-releases/sb0057

46 *Id*.

47 *Id*.

48 *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash (Aug. 23, 2023), available at https://home.treasury.gov/news/press-releases/jy1702

49 *See U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Aug. 23, 2023).

50 *See* 50 U.S.C. Ch. 35 § 1701 *et seq*. IEEPA is the federal statute underpinning the SDN designation of the Lazarus Group.

51 *See* Memorandum of Law in Support of Roman Storm's Motion to Dismiss, *U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Mar. 29, 2024).

52 *See* Order, *U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Sept. 27, 2024).

53 *See* Order, *U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Aug. 6, 2025).

54 *Id*.

55 U.S. Federal Bureau of Investigation, Most Wanted: Roman Semenov, available at https://www.fbi.gov/wanted/wcc/roman-semenov

56 *See* Joint Alert, Fin. Crimes Enf't Network & Bureau Indus., Fin-2022-Alert003, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts (Jun. 28, 2022), available at https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; Joint Alert, Fin. Crimes Enf't Network & Bureau Indus., FIN-2-23-Alert004, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (May 19, 2023), available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf

57 *See* Press Release, U.S. Dep't J., Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme (Oct. 19, 2022), available at https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money

58 *See* U.S. Dep't Treas. Off. Foreign Assets Control, A Framework for OFAC Compliance Commitments (2019), available at https://ofac.treasury.gov/media/16331/download?inline

59 Some entities, such as U.S. financial institutions, may also be required or expected to have an OFAC compliance programme under other applicable regulatory regimes.

60 31 C.F.R. pt. 501, App. A.

61 *See* U.S. Dep't Treas. Off. Foreign Assets Control, A Framework for OFAC Compliance Commitments (2019), available at https://ofac.treasury.gov/media/16331/download?inline

62 *Justice Manual*, 9-28.800, updated January 2026, available at https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.800. Judges also take into account an effective compliance and ethics programme when determining appropriate sentencing under the U.S. Sentencing Commission's Sentencing Guidelines (U.S.S.G. 8B2.1).

63 U.S. Department of Justice, Department of Justice Corporate Enforcement and Voluntary Self-Disclosure Policy (Mar. 2026), available at https://www.justice.gov/dag/media/1430731/dl?inline

64 Steptoe LLP, DOJ Confirms New Corporate Enforcement Policy Applies to Export Control and Sanctions Matters (Apr. 2, 2026), available at https://www.steptoe.com/en/news-publications/doj-confirms-new-corporate-enforcement-policy-applies-to-export-control-and-sanctions-matters.html#_edn2

65 Guiding and Establishing National Innovation for Stablecoins Act (GENIUS Act) § 5(A)(vi), S. 1582, 119th Cong. (2025), available at https://www.govinfo.gov/content/pkg/BILLS-119s1582es/pdf/BILLS-119s1582es.pdf

66 *Id*.

67 GENIUS Act § 5(A)(iv).

68 GENIUS Act § 6.

69 *See* U.S. Dep't Treas., Treasury Proposes Rule to Implement the GENIUS Act's Requirements to Counter Illicit Finance (Apr. 8, 2026), available at https://home.treasury.gov/news/press-releases/sb0435

70 *See* U.S. Dep't Treas. FinCEN, Fact Sheet: Proposed Rule to Implement the GENIUS Act's Anti-Money Laundering Obligations and Sanctions Compliance Program Requirements (Apr. 8, 2026), available at https://www.fincen.gov/system/files/2026-04/FactSheet-PPSI-program-NPRM.pdf

71 OFAC and FinCEN, Proposed Rule, Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements (Apr. 10, 2026), available at https://www.federalregister.gov/d/2026-06963/p-162

72 *See* Memorandum, U.S. Department of Justice Office of the Deputy Attorney General, Ending Regulation by Prosecution (Apr. 7, 2025), available at https://www.justice.gov/dag/media/1395781/dl?inline

73 *Id*.

74 U.S. Attorney's Office for the Southern District of New York, Founders Of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty (Aug. 6, 2025), available at https://www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty

75 *See* Strengthening American Leadership in Digital Financial Technology, Working Gorup on Digital Assets (Jul. 30, 2025), available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf

76 *Id*.

77 *Id*.



Evan T. Abrams

Tel: +1 202 429 3052 / Email: eabrams@steptoe.com

Evan Abrams counsels financial institutions, multinational corporations, and individuals on a variety of international regulatory and compliance matters. He regularly advises clients on issues related to anti-money laundering (AML), economic sanctions, export controls, foreign anti-corruption, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Counterintelligence and Security Agency (DCSA). Among other sectors, his practice focuses on emerging technology, including financial technology (FinTech), where he leverages his deep understanding of business trends and technological developments to help clients achieve their commercial objectives while complying with complex regulatory regimes.



Andrew C. Adams

Tel: +1 212 957 3081 / Email: acadams@steptoe.com

Andrew Adams advises in the areas of government and internal investigations, corporate governance, and white-collar and regulatory matters. His practice focuses on anti-money laundering compliance, U.S. economic countermeasures, and national security crisis response, drawing on his time as the inaugural Director of the Department of Justice's Task Force KleptoCapture, a multi-agency response group focused on the economic sanctions and export controls imposed in response to Russia's invasion of Ukraine, and on his service as acting Deputy Assistant Attorney General for the National Security Division of the Department of Justice, with oversight of the Division's sanctions, export control, and national security cyber investigations.

Andrew has investigated, charged, and tried cases with an emphasis on: the integrity of financial institutions; transnational organised crime; sophisticated money laundering operations through both traditional and "crypto" platforms; sport integrity; and cases involving looted antiquities and frauds involving the sale of cultural property.



Scott R. Johnston

Tel: +1 202 429 1379 / Email: scjohnston@steptoe.com

Scott Johnston advises clients on complex economic sanctions, human rights, and anti-corruption matters informed by extensive experience at the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Scott served in several leadership roles at OFAC, including as Acting Assistant Director, where he supervised the teams responsible for investigations related to counternarcotics, transnational criminal organisations, all Africa country programmes, all Western Hemisphere country programmes, human rights, and anti-corruption.

Steptoe LLP

1330 Connecticut Avenue, NW, Washington, D.C. 20036, USA

Tel: +1 202 429 3000 / URL: www.steptoe.com

Global Legal Insights – Blockchain & Cryptocurrency Regulation provides in-depth analysis, insight and intelligence across nine expert analysis chapters and 26 jurisdictions, covering:

- Government attitude and definition
- Cryptocurrency regulation
- Sales regulation
- Taxation
- Money transmission laws and anti-money laundering requirements
- Promotion and testing
- Ownership and licensing requirements
- Mining
- Border restrictions and declaration
- Reporting requirements
- Estate planning and testamentary succession

globallegalinsights.com