

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Skadden

09 / 07 / 22

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

Editor's note: This client alert has been updated to reflect new developments.

Regulatory scrutiny of the use and management of cryptocurrency and other digital assets such as utility tokens and non-fungible tokens (NFTs) (collectively, cryptoassets) is rapidly growing on both sides of the Atlantic. With increasing governmental enforcement and private litigation involving cryptoassets, it is vital for individuals and businesses whose activities involve these assets to understand the broad legal framework for enforcement and the types of disputes and legal actions into which they could be drawn. Even if they are not the targets of enforcement actions or parties to legal proceedings, they may have to respond to subpoenas or other court orders. While most of the enforcement actions and litigation to date has involved cryptocurrencies, some have involved NFTs and other types of digital assets.

This article analyzes tools and procedures that enforcement authorities in the U.S. and U.K. may use to seize and forfeit cryptoassets and provides an overview of related regulatory developments in these jurisdictions.

Factual Background

Cryptocurrencies and other digital assets constitute a growing share of global financial assets. As of April 2022, cryptocurrencies were purportedly worth almost \$2 trillion, the [U.S. Securities and Exchange Commission \(SEC\)](#) estimated. Despite the recent volatility in cryptocurrency markets and the decline in the value of some cryptocurrencies in May and June of 2022, cryptoassets remain widely held and retain significant value. As of June 2022, cryptocurrencies were still valued at just under \$1 trillion, with cryptocurrency prices showing signs of recovery according to reports by Reuters in [June 2022](#) and [August 2022](#). In February 2022, [Her Majesty's Revenue and Customs \(HMRC\)](#) estimated that approximately 10% of U.K. adults own or have owned cryptoassets, and 68% of those are “likely” or “very likely” to acquire more.

The meteoric rise in the use and management of cryptocurrency in recent years has led to an increase in related crime. [According to data provider Chainalysis](#), \$1.9 billion worth of cryptocurrency was stolen from January 2022 through July 2022, compared to just under \$1.2 billion at the same point in 2021. Per the Chainalysis 2022 midyear report, much of this illicit activity can be attributed to the rise in funds stolen from decentralized finance (DeFi) protocols, with North Korea-affiliated groups alone having stolen an estimated \$1 billion of cryptocurrency from DeFi protocols as of July 2022. Fraudsters may deploy a range of strategies, including ransomware attacks, hacks or deception to steal from unsuspecting victims, or use cryptoassets to launder criminal proceeds.

Against this backdrop, both U.S. and U.K. law enforcement agencies have increasingly used the tools at their disposal to combat cryptocurrency-related crime. For example, in February 2022 the U.S. Department of Justice (DOJ) [announced the seizure of \\$3.6 billion worth of bitcoin](#) in connection with the 2016 hack of Bitfinex — the largest financial seizure ever.

Similarly, in July 2021, London's Metropolitan Police seized £180 million of cryptocurrency in connection with suspected money laundering and, more recently, the U.K.'s [National Crime Agency \(NCA\)](#) reported that it confiscated around £26.9 million in cryptocurrency assets between April 1, 2021, and March 31, 2022.

US Enforcement Procedures Applicable to Cryptoassets

In the U.S., cryptoassets have been the focus of much attention by enforcement authorities in recent years. At the federal level, this is mainly the purview of the SEC, DOJ, the

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Commodity Futures Trading Commission (CFTC) and the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of Treasury.

UPDATE: On September 16, 2022, the DOJ released a report on The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets, which details the many ways in which illicit actors have exploited digital assets. The DOJ's report discusses the challenges created by novel technology for law enforcement and proposes new regulatory and legislative actions to allocate adequate resources to various agencies, assist law enforcement with gathering evidence and initiating prosecutions, and strengthen laws and penalties. For example, the DOJ report proposes lifting the \$500,000 cap on administrative forfeiture actions discussed in further detail below.

The DOJ simultaneously announced its establishment of the nationwide Digital Asset Coordinator (DAC) Network, composed of designated federal prosecutors from U.S. Attorneys' Offices nationwide and the Justice Department's litigating components. As members of the DAC Network, prosecutors will learn about the application of existing authorities and laws to digital assets and share best practices for investigating digital assets-related crimes, including drafting search and seizure warrants, restraining orders, criminal and civil forfeiture actions, indictments and other pleadings.

In February 2022, the DOJ formed the Virtual Asset Exploitation Unit (VAXU) within the Federal Bureau of Investigations (FBI), which is dedicated to blockchain analysis and virtual asset seizure. VAXU is expected to work closely with the DOJ's National Cryptocurrency Enforcement Team (NCET), which was launched in October 2021.

In addition, in March 2022, Attorney General Merrick Garland launched a new interagency taskforce dubbed KleptoCapture to "hold accountable corrupt Russian oligarchs." The task force's mission explicitly includes targeting the use of cryptocurrency to evade sanctions or launder money, with a focus on asset seizure.

In May 2022, the U.S. District Court for the District of Columbia upheld the DOJ's criminal complaint against an unnamed U.S. citizen who allegedly helped customers evade U.S. sanctions by funnelling more than \$10 million of bitcoin through a virtual currency exchange from the U.S. to a country that is subject to U.S. comprehensive sanctions. In so doing, the court adopted for the first time the Office of Foreign Assets Control's (OFAC's) recent guidance on sanctions compliance obligations, saying that virtual currency is subject to OFAC's regulations, and "financial services

providers" to whom U.S. sanctions regulations apply include virtual currency exchanges.¹

Overview of Cryptoasset Forfeiture by US Authorities

U.S. authorities have increasingly used asset forfeiture as a tool in crypto-related enforcement proceedings, seizing several billions of dollars of cryptoassets in recent years. For instance, since 2015, the U.S. Internal Revenue Service Criminal Investigation (IRS-CI) has seized over \$3.5 billion in cryptocurrency, and, as of December 2021, the U.S. Marshals Service held \$919 million in cryptocurrency.

In April 2022, federal prosecutors working with local Florida law enforcement obtained forfeiture of \$34 million worth of cryptocurrency tied to illegal dark web marketplace activities. The IRS-CI, Department of Homeland Security (DHS), FBI, U.S. Postal Inspection Service (USPIS) and U.S. Drug Enforcement Agency (DEA) jointly investigated this case.

U.S. prosecutors are expected to pursue increasingly aggressive civil forfeiture actions targeting cryptoassets. In these cases, the government can transfer the funds in question instantaneously,

whereas transfers involving fiat currency or personal property can take much longer, making crypto-related forfeiture an appealing mechanism for authorities.

In order to forfeit cryptoassets, U.S. authorities generally first trace the cryptoassets and transactions using publicly available blockchain information and analytics tools to identify relevant information, such as the dates and amounts of transactions and the origination and destination public address(es). If needed, agents can then issue subpoenas to financial institutions, virtual-currency exchanges or other third-party intermediaries to obtain relevant records.

This approach got a boost in 2020, when the U.S. Court of Appeals for the Fifth Circuit held in *United States v. Gratkowski* that federal agents did not need to first obtain a warrant based on probable cause to subpoena bitcoin records.² In *Gratkowski*, the federal agents used forensic software to extract suspicious addresses from the bitcoin blockchain and then subpoenaed a virtual currency exchange to trace the customers who had made bitcoin payments to those suspicious addresses.

¹ In re: Criminal Complaint, No. 1:22-mj-00067, 2022 WL 1573361, at *3 (D.D.C., 2022) (citing U.S. Dep't of the Treasury Sanctions Programs Related to Digital Currency Transactions); *see also* "OFAC Enters Into \$98.830 Settlement With BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," U.S. Department of Treasury (Dec. 30, 2020).

² *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020).

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

The court held that “a person generally has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” treating bitcoin records kept by the exchange in the same way as customer financial records kept by banks in that bank records are not subject to Fourth Amendment protections.³ The court further held that Gratoski did not have a privacy interest in his information on the bitcoin blockchain since that information is available to every bitcoin user, making it possible to determine the identities of the bitcoin address owner by analyzing the blockchain.⁴

Armed with this data, authorities can establish the asset’s nexus to criminal activity and its location — information that is required to obtain a search warrant authorizing seizure of the asset. Subsequently, authorities may seize the cryptoasset using such a warrant, or through another method that otherwise fulfils the government’s obligations under the Fourth Amendment (searches and seizures), such as with the owner’s consent. Forfeiture proceedings are then required so that the title to the seized assets can be permanently transferred to the government. Cryptoassets can be forfeited via administrative, civil judicial or criminal judicial forfeiture, as discussed below.

U.S. authorities are increasingly working with cryptoasset and blockchain analytics firms to use advanced technologies to uncover illicit activity and identify linked actors, in addition to crime proceeds and other forfeitable assets. Since 2017, federal agencies including the DEA, DHS, IRS, FBI and CFTC have spent millions of dollars on third-party cryptoasset tracing and blockchain analytic tools.⁵

These technologies have already been put to use at a large scale. For example, in November 2020, using blockchain forensics, [the DOJ and IRS identified and retrieved, through a civil forfeiture action](#), \$1 billion worth of illicit bitcoin stolen from Silk Road more than seven years earlier.

More recently, in February 2022, the U.S. District Court for the District of Columbia held that the government’s use of reliable blockchain analysis software that traced the flow of stolen digital currency to the investigation’s targets supported probable cause for

a search warrant.⁶ The court further highlighted that such software was becoming commonplace for law enforcement to track financial crimes, noting that this sort of analysis had demonstrated an “unprecedented rate of success” when compared to human informants, bolstered by the software’s “lack of incentive or capacity to lie.”⁷

This ruling was in accord with [the New York State Department of Financial Services’ April 2022 guidance](#) stating that cryptocurrency firms should use blockchain analytics tools to help mitigate and manage financial risk, and to meet AML and sanctions-related compliance requirements.

U.S. authorities are also working to increase cooperation with foreign authorities to identify and trace cryptoassets that may be subject to forfeiture. For example, on 5 April 2022, [the DOJ announced the seizure of Hydra Market](#), the world’s largest and longest-running darknet market. The Hydra servers and cryptocurrency wallets containing \$25 million worth of bitcoin were seized in Germany by the German Federal Criminal Police (the Bundeskriminalamt), in coordination with multiple U.S. agencies, including the DEA, DHS, USFIS, FBI, IRS, DOJ’s Office of International Affairs, the U.S. Attorney’s Office for the District of Columbia and the NCET.

Administrative Forfeiture

Many federal law enforcement agencies are authorized to seize cryptoassets valued at less than or equal to \$500,000 at the time of seizure via an administrative forfeiture procedure without judicial approval. The agency involved seizes the asset, provides notice to potential claimants, and processes any claims to the assets. Any timely and legally valid claims are referred to the U.S. Attorney’s Office, which must then commence a civil forfeiture action in federal court. In the absence of any such claims, the agency can complete the forfeiture without judicial involvement. Assets with a timely and legally valid claim to them, or those valued at more than \$500,000, must be forfeited via a civil or criminal forfeiture action.

The DEA, DHS and USFIS have all successfully seized and obtained legal title to cryptocurrency via administrative forfeiture in the past.⁸

³ *Id.* at 310-11 (citing to *United States v. Miller* 45 U.S. 435, 439-40 (1976)).

⁴ *Id.* at 312.

⁵ Felix Mollen, “[Coinbase Secures Another Millionaire Deal With the US Government To Let Them Use Its Blockchain Analytics Software](#),” CryptoPotato (June 8, 2020); Danny Nelson, “[Coinbase Offers US Feds New Crypto Surveillance Tools](#),” CoinDesk (June 5, 2020); Danny Nelson, “[Inside Chainalysis’ Multimillion-Dollar Relationship With the US Government](#),” CoinDesk (Feb. 10, 2020).

⁶ *Matter of Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, No. 20-SC-3310 (ZMF), 2022 WL 406410 (D.D.C. Feb. 8, 2022).

⁷ *Id.* at *13.

⁸ See, e.g., “[FOR SALE – Approximately 4,041,584,249,32 bitcoin](#),” U.S. Marshals Service (February 2020 auction); Roger Aitken, “[U.S. Marshals to Hold Bitcoin Auction for \\$50 Million Worth of Cryptocurrency](#),” *Forbes* (January 12, 2018).

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Criminal Forfeiture

Criminal judicial forfeiture actions are *in personam* (against the person) actions against a defendant where only property in which the defendant has a true interest may be forfeited. A criminal forfeiture proceeding starts by adding a forfeiture allegation to a charging document and requires that the defendant be convicted of an offense that allows the forfeiture of property. The government must establish by a preponderance of the evidence the requisite connection between the crime of conviction and the asset. Crimes such as those involving money laundering and various types of fraud and counterfeiting allow criminal forfeiture. A separate ancillary proceeding follows to determine any third-party ownership interests in the property that the government seeks to forfeit.

In what is believed to be the largest cryptocurrency fraud ever charged criminally, in November 2021, a district court granted the DOJ's request to liquidate \$57 million in cryptocurrency seized from Glenn Acaro, the top North American promoter of the cryptocurrency bitconnect. Acaro pled guilty to participating in a conspiracy that defrauded investors of over \$2 billion. In the charging document, the DOJ sought criminal forfeiture pursuant to 18 U.S.C. §982(a)(2)(A) and 28 U.S.C. §2461(c) of the fraudulently obtained proceeds in Acaro's possession, the majority of which were held in cryptocurrencies, including bitcoin, ethereum, litecoin, dash and several others.⁹

Civil Judicial Forfeiture

Civil judicial forfeiture actions are *in rem* court proceedings brought against property that was derived from or used to commit an offense, rather than against a person who committed an offense. Unlike criminal forfeiture, no criminal conviction is required. The government must still prove that the property was linked to criminal activity by a preponderance of the evidence.

This proceeding allows the court to gather everyone with an interest in the property and resolve all the claims to it in one proceeding.

Not only does this procedure require a lower burden of proof; it allows the government to reach more property than criminal forfeiture. This includes property of criminals located outside the U.S., such as terrorists and fugitives. It also permits recovery of assets held by deceased defendants, or where no defendant can be identified since the action is against the asset itself.

The government's notice requirement for *in rem* forfeiture proceedings can be met if the government attempts to provide actual notice. In *United States v. Twenty-Four Cryptocurrency Accounts*, for example, it was held that the government provided sufficient notice

to the public and to potential claimants of its forfeiture action *in rem* against cryptocurrency accounts allegedly used in connection with a child pornography website where the government had sent direct notice via certified mail or email to potential claimants who could be identified by currency exchange information; sent notice an additional time when emails or certified letters were returned as undeliverable; and posted a public notice on an official government forfeiture website for 30 consecutive days.¹⁰

The IRS and DHS enlisted the help of South Korean law enforcement to seize the servers and related materials, which were located in South Korea. A review of the seized materials revealed bitcoin transactions, which allowed law enforcement to obtain a warrant and seize all 24 related cryptocurrency accounts.¹¹ The court granted the government's motion for default judgment for the forfeiture of all 24 accounts.

UK Enforcement Procedures Applicable to Cryptoassets

In the U.K., regulation of cryptoassets has likewise become a focus for regulators and law enforcement agencies. Under the FCA's scrutiny, crypto-related firms now face a new requirement to register in the U.K., and cryptoasset firms must comply with anti-money laundering (AML) regulations, and are subject to the FCA's enforcement powers. Between January 10, 2020, and October 20, 2020, alone, the FCA opened 39 inquiries into cryptoasset businesses. In March 2022, the FCA announced that, between September 2021 and March 2022, it had opened 300 investigations into unauthorized cryptoasset operators. Echoing the FCA's commitment, the U.K. Serious Fraud Office (SFO) announced in its 2021/22 Business Plan that the "growth of cryptocurrency" would be one of its key focus areas.

In March 2022, U.K. regulators issued a joint statement signaling that financial sanctions do not differentiate between cryptoassets and other types of assets. The statement made clear that the use of cryptoassets to circumvent economic sanctions is a criminal offense under the Money Laundering Regulations 2017 and regulations made under the Sanctions and Anti-Money Laundering Act 2018. The FCA confirmed that it had written to all registered cryptoasset firms and those holding temporary registration status to highlight the application of sanctions to various entities and individuals.

More recently, the May 2022 Queen's Speech outlined a new Economic Crime Bill under which the authorities will gain more tools to halt illicit finance in the U.K., including the power to seize cryptoassets. No implementation timetable has been provided yet.

¹⁰ *United States v. Twenty-Four Cryptocurrency Accts.*, 473 F. Supp. 3d 1 (D.D.C. 2020).

¹¹ *Id.* at *3-4.

⁹ *United States v. Glenn Acaro*, No. 21CR02542-TWR. (S.D. Cal.), Complaint.

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Criminal Forfeiture

There are a number of tools available to U.K. law enforcement to address cryptoasset-related crime. These include orders to restrain, seize, forfeit and confiscate assets, as well as orders to obtain information about potential wrongdoers.

Law enforcement can secure a restraint order under s41 Proceeds of Crime Act 2002 (POCA) to prohibit a person from dealing with any “realisable property” held by them, provided that certain conditions are met. This includes, for example, where a criminal investigation or proceedings relating to an offense have started in England and Wales and there are reasonable grounds to suspect that the alleged offender has benefitted from his criminal conduct.

A restraint order freezes assets wherever in the world they are and prevents assets from being moved or dissipated. Given the nature of the order, it is usually obtained without notice to a defendant. Non-compliance with a restraint order is a contempt of court, and in extreme cases, may be treated as perverting the course of justice.

In a mark of flexibility, courts have found cryptocurrency to meet the definition of “realisable property” for the purposes of POCA. In the recent case of *Lavinia Deborah Osbourne v (1) Persons Unknown (2) Ozone Networks Inc. trading as Opensea* [2022],¹² the High Court recognized NFTs as legal property over which a freezing injunction could be ordered, thereby extending to NFTs the courts’ previous framing of cryptocurrencies as proprietary assets. The NFTs here were two unique digital artworks, stolen from the claimant’s digital wallet in January 2022, and traced to two wallets. An urgent freezing order was granted in March 2022, freezing the assets until the end of proceedings. This landmark case confirmed that NFTs should be treated as standalone assets, separate from the underlying pieces that they represent.

English courts have been willing to grant not only restraint and freezing orders relating to cryptoassets, but also confiscation orders where certain conditions are met, namely:

- a defendant is convicted for an offense in proceedings before the Crown Court, or committed to the Crown Court for sentencing and/or confiscation, and
- the prosecutor asks for a confiscation order to be made, or the court believes it is appropriate for it to do so.

When making a confiscation order, the court must decide whether the defendant has a criminal lifestyle and whether he has benefitted from general or particular criminal conduct.

In *R v Teresko* [2018],¹³ the defendant was convicted of drug and money-laundering offenses. In related restraint proceedings, the police were permitted to restrain the defendant’s cryptoassets and convert seized bitcoin into sterling. The court subsequently made a confiscation order over the defendant’s bitcoin, worth £975,000.

Similarly, in *R v West* [2019],¹⁴ the defendant was convicted of hacking into company databases, selling the data on the dark web and converting the funds into cryptocurrency. He was ordered to pay a confiscation order that included cryptocurrency valued at £922,978.

Together, these examples reflect that English courts are prepared to use conventional tools in novel contexts in aid of criminal justice.

However, challenges may arise when it comes to enforcement. For example, successful seizure of cryptoassets usually depends on obtaining the owner’s private key. Prosecutors are likely to have greater success in obtaining a private key where it is held by a bank or crypto exchange on a person’s behalf. However, where the key is held by the individual owner, the prosecutor may have to rely on the cooperation of the defendant or further court proceedings.

In Ireland, the so-called “Fishing Rod Case”¹⁵ demonstrated the challenges that can arise in seizing cryptoassets without the private key. A defendant hid the key for his cryptoassets, worth an estimated £45 million, in a fishing box that was thrown away by his landlord while he was in police custody. While the digital wallets were seized by the Irish state, without the secure key, the assets are unobtainable.

Another key challenge is the issue of anonymity. Cryptoassets are attractive for unlawful conduct because they can be held and transferred anonymously. Unless there is proof a defendant is dealing or concealing illegal cryptoassets, the court may find it difficult to make an order. In *Teresko*, the key for the defendant’s bitcoin wallet was found during a search of his property, and in *West*, the defendant was arrested while he was using his computer, allowing the police to access his virtual wallet and provide evidence to the Crown Prosecution Service.

It is not just cryptocurrency that can be seized. On February 13, 2022, HMRC used its POCA powers to seize NFTs as part of a £1.4 million VAT fraud investigation that involved around 250 allegedly fake companies. HMRC was the first U.K. agency to seize an NFT. HMRC Deputy Director Economic Crime Nick Sharp said this confiscation case should deter the view that cryptoassets serve “to hide money from HMRC.”

¹³ *R v Teresko (Sergejs)* [2018] Crim. L.R. 81.

¹⁴ *R v West* [2019], unreported, 28 September 2019, Southwark Crown Court.

¹⁵ *DPP v Collins* [2020], unreported, February 2020.

¹²The full High Court judgment is yet to be published.

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Civil Asset Recovery Enforcement Actions

Alongside the criminal orders under POCA, U.K. law enforcement also has the power to recover assets in the civil courts on the civil standard (*i.e.*, balance of probabilities) under POCA. A prosecutor can seek a civil recovery order, which provides that specific property is recoverable on the basis that it represents the proceeds of unlawful conduct. In effect, this is a confiscation order without the triggering conviction.

DPP v Briedis and Reskajs [2021]¹⁶ is a prime example of this procedure in action. There the Director of Public Prosecutions sought a freezing order under s245A POCA (civil recovery powers) against two respondents covering cash in various currencies, money in bank accounts, personal items and cryptocurrency. The court was satisfied that cryptocurrencies fell within the wide definition of “other intangible property” under POCA s316(4).

That case referred to the reasoning in *AA v Persons Unknown* [2019],¹⁷ in which the claimant paid a bitcoin ransom to a hacker in exchange for decryption software and, following recovery of the encrypted files, the claimant took steps to recover the ransom. Given that the court in this case was prepared to recognize cryptocurrency as property under POCA provisions related to property freezing orders, it is likely that a civil recovery order could also have been obtained over it.

Going further, if a prosecutor obtained a civil recovery order, it could, in theory, also obtain an Unexplained Wealth Order (UWO) on cryptoassets pursuant to s362A POCA. However, they are unlikely to be the tool of first choice, given that cryptoassets are less readily identifiable than a tangible asset. A UWO application requires a description of the property and the suspected owner, which may be difficult in cryptoasset cases.

Conclusion

The trend toward greater regulation of cryptoassets and more enforcement in cases of wrongdoing is likely to continue as authorities respond to the growth in cryptoasset use. Commenting on the high degree of fraud involving the asset class, [SEC Commissioner Hester Peirce said at a conference in May 2022](#)

¹⁶ *DPP v Briedis and Reskajs* [2021] EWHC 3155 (Admin).

¹⁷ *AA v Persons Unknown* [2019] EWHC 3556.

that the United States has “dropped the regulatory ball” and has “got to get working” to target fraud and play a more positive role in cryptocurrency innovation.

To manage cryptoasset-related legal and compliance risk stemming from efforts to seize and forfeit cryptoassets, organizations can take a number of steps including:

- Organizations should ensure they have clear procedures in place to deal with subpoenas and other court orders, both civil and criminal, that can be obtained regarding cryptoasset-related wrongdoing. Those within an organization responsible for handling such orders should be trained to respond promptly and properly.
- Cryptoasset businesses should promote a culture of compliance and ensure company-wide awareness of legal and compliance requirements with clear, tone-from-the-top messaging.
- Businesses should be sure to include potential cryptoasset-related crime when conducting risk assessments, and compliance programs should include efforts to mitigate against the risks identified through the assessments, including the risk that cryptoassets will be subject to seizure or forfeiture by government authorities or in connection with private litigation.

Prior Skadden articles on related topics

- [Cryptocurrency Insider Trading Case Could Have Broader Ramifications for the Industry](#) (July 26, 2022)
- [Regulatory Actions and Legislative Proposals Signal Growing Consensus on Parameters for Stablecoins](#) (June 29, 2022)
- [A Closer Look at the New SEC Crypto Assets and Cyber Unit \(Video\)](#) (June 28, 2022)
- [‘Insider Trading’ and NFTs: What Should Companies Be Doing?](#) (June 16, 2022)
- [Regulatory Approaches to Nonfungible Tokens in the EU and UK](#) (June 15, 2021)

Cryptoasset Seizures and Forfeitures: US and UK Enforcement Overview

Contacts

Alessio Evangelista

Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Andrew M. Good

Partner / London
44.20.7519.7247
andrew.good@skadden.com

Jessie K. Liu

Partner / Washington, D.C.
202.371.7340
jessie.liu@skadden.com

Elizabeth Robertson

Partner / London
44.20.7519.7115
elizabeth.robertson@skadden.com

Bora P. Rawcliffe

Counsel / London
44.20.7519.7139
bora.rawcliffe@skadden.com

Devaanjana Goel

Associate / London
44.20.7519.7239
devaanjana.goel@skadden.com

Rebecca M. Murday

Associate / London
44.20.7519.7242
rebecca.murday@skadden.com

Jason Williamson

Associate / London
44.20.7519.7093
jason.williamson@skadden.com

Trainee solicitor **Clara Rupf** contributed to this article.