Trends and Developments

Contributed by:
Evelyn Baltodano-Sheehan, David H McGill, Benjamin J A Sauter and Amanda Tuminelli
Kobre & Kim see p.27

Old Dog, New Tricks: Innovating Traditional Asset Recovery Tools to Recover Crypto-assets

Whether through civil channels or government seizure, it is getting easier for private parties to claw back fraudulently obtained cryptocurrency and make their asset portfolios whole again. For example, just recently, in February 2022, the US Department of Justice (DOJ) announced that they had seized USD3.6 billion in stolen cryptocurrency that was directly linked to the 2016 hack of the British Virgin Islands (BVI)-based crypto-exchange, Bitfinex (the now-infamous "Croc of Wall Street" case); victims of the hack are likely to eventually recover their lost funds through criminal restitution proceedings. The DOJ was able to trace the funds using blockchain analysis tools that pointed them directly to the couple accused of laundering the crypto-assets obtained from the Bitfinex hack. While this type of blockchain analysis uses new technology, it employs classic principles of asset tracing that follows implicated funds from their current location all the way back to the original wrongdoer. As these tools become more readily available to the legal community, the path for private individuals and companies to use them to recover stolen or wrongfully obtained cryptocurrency becomes clearer and easier to follow.

Because of cryptocurrency's intrinsic nature on a public and historically accurate blockchain, most cryptocurrency transactions that happen on-chain can be efficiently and effectively traced with advanced forensic toolkits. The blockchains for the most popular cryptocurrency networks such as Bitcoin and Ethereum serve as a ledger of every transaction that has occurred using that particular network, including the sending and receiving of addresses, among other information. This data can be used in conjunction with forensics tools to group addresses under common control, graphically display connections among addresses, and, in many cases, identify which entities control those addresses.

Fundamentally, tracing cryptocurrency transactions is not all that different from tracing transactions involving traditional assets. While traditional asset tracing includes "following the money" by pouring over financial records such as bank account statements, payment ledgers, and trading history, tracing cryptocurrency assets uses the same principles but employs sophisticated software that analyses and graphically displays transactions on the blockchain in a fraction of the time. Proper use of such tools can efficiently lead to the identification of entities and/or individuals, and produce compelling evidence for use in civil and criminal litigation, which may ultimately provide the basis for victims to recover their assets.

Undoubtedly, tracing crypto-transactions comes with its own challenges. Certain techniques exist to try to cover one's tracks on the blockchain. Additionally, not all cryptocurrency exchanges (or other crypto-services) collect quality "Know Your Customer" (KYC) information or comply with legal requests, which can impede the ability to ultimately link transactions to persons of interest.

In addition, because of the industry's nascency, international governance rules related to crypto-currency are constantly evolving. In the United

States, the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), DOJ and Financial Crimes Enforcement Network (FinCEN) – among various other agencies – have jostled over authority and competed with each other for scarce enforcement resources. Even more so, internationally, the lines delineating jurisdictional responsibilities are not neatly drawn.

However, regardless of these challenges, effective recovery and enforcement mechanisms do exist and are being deployed with increasing effectiveness. In 2021 alone, the Internal Revenue Service (IRS) announced that they had seized USD3.5 billion worth of cryptocurrency, with the DOJ instituting a significant number of investigations and successful seizures of stolen cryptocurrency. The US government has already recovered USD3.6 billion from the Bitfinex seizure at the beginning of this year. Both globally and domestically, successful asset recovery campaigns are only increasing in number, demonstrating that traditional jurisprudential frameworks relating to asset recovery are continuing to be repurposed and developed for the recovery of cryptocurrency. As such, while challenges remain present, the various methods outlined below exist for obtaining compelling evidence as a basis for recovery efforts, and identifying practical uses of the law and the government to assist victims in swiftly recovering their assets.

Civil Asset Recovery

While the DOJ has seized increasing amounts of cryptocurrency over the years and generated flashy headlines in the process (ie, the takedown of Silk Road in 2013, the "Croc of Wall Street" case, etc), even the DOJ has limited resources when it comes to crypto-asset recovery campaigns. As such, victims are well advised to consider civil recovery options as part of an overall recovery strategy.

Civil asset recovery procedures

One such strategy involves the use of freeze letters and civil complaints, which – in tandem – can be used to warn fraudsters and custodians against dissipating assets and initiate legal action against those assets for eventual recovery. Even in cases where the identity of the fraudster may remain anonymous, victims may file "John Doe" complaints (ie, a complaint against persons unknown), in order to encourage or compel cryptocurrency exchanges to assist with identifying the wrongdoer. For example, in White v Sharabati, the plaintiff, Elizabeth White, a resident of New York, agreed to sell Ripple to Mr Sharabati (who was anonymous to her at the time) in exchange for bitcoin. While she sent her Ripple, she never received bitcoin in exchange. White realised she had been duped, but she didn't know the identity of the person who had duped her. With the assistance of Kobre & Kim, White immediately filed a "John Doe" complaint describing the fact pattern and drawing upon statutes permitting the recovery of treble damages and attorneys' fees to amplify her civil claims. After conducting further forensic analysis and tracing the funds to two crypto-exchanges, Bittrex and Poloniex, White subpoenaed the exchanges to determine Mr Sharabati's identity and amended the "John Doe" complaint to specify and name Mr Sharabati as a defendant. After obtaining a default judgment in her favor, White sought enforcement of her judgment and ultimately made a sizeable recovery.

Relatedly, temporary restraining orders (TROs) and preliminary injunctions have also shown merit as US court-ordered legal instruments that can prevent the movement of fraudulently siphoned crypto-assets. In contrast to freeze letters and "John Doe" complaints, TROs and preliminary injunctions have proven useful when the identity of the perpetrator is already known and they are directed against a known custodian of the cryptocurrency, such as an exchange or a

hosted wallet site. However, obtaining this type of relief requires a substantial showing. Indeed, to succeed in obtaining a preliminary injunction, a plaintiff must "establish that they are likely to succeed on the merits, that they are likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in their favor, and that an injunction is in the public interest."

Relatedly, in common law jurisdictions – such as the United Kingdom – similar remedies have led to similarly successful results. For example, in ION Science Ltd and Duncan Johns v Persons Unknown, Binance Holdings Limited and Payward Limited, the claimants – alleging fraud of over GBP570,000 through various crypto-investments – filed an ex parte application for a worldwide freezing order against the assets and a disclosure order against Binance and Payward. The court granted the freezing order and disclosure orders compelling the exchanges to disclose the identities of the alleged fraudsters. The judgment was also significant because it considered the lex situs (location) of Bitcoin, holding that because the defrauded crypto-asset owner was domiciled in the UK and therefore the relevant participant in the Bitcoin network controlling the assets was located in the UK, the lex situs of a cryptocurrency is the jurisdiction in which the owner is domiciled. Furthermore, in the BVI, Norwich Pharmacal orders (court orders that force the disclosure of documents or information), which are also obtained ex parte, may be a similarly utilised means of securing key intelligence related to the beneficial ownership of a given entity. Importantly, the information gathered from such orders may be used to pursue a fraudster without notice to the wrongdoer, so long as the applicant applies, and the court agrees, to append a seal and gagging provision to the order.

Think globally

It is important to think about how these procedural mechanisms can tie in to a globally coordinated effort to recover assets. For example, the strategies outlined above were implemented by Kobre & Kim to bring a lawsuit in the US on behalf of a Swiss company while local Swiss counsel pursued criminal charges in Switzerland. In this case, the clients sought the recovery of over USD50 million-worth of Ethereum sitting in their former CEO's cold wallet. With the help of in-house blockchain forensics tools to identify where the assets were located and who had access to the wallet, Kobre & Kim filed a complaint in the Southern District of New York (SDNY) requesting that the cold wallet (and therefore, the funds) be returned to the exchange immediately. Although the representation was for a Swiss company, the SDNY was the appropriate jurisdiction because (a) the former CEO resided in New York City, and (b) an affiliated entity of the company that was involved in the dispute was also based in New York City. In tandem with the complaint, the legal team filed a preliminary injunction and a temporary restraining order to immediately prohibit the former CEO from intentionally dissipating the assets. At the same time, Swiss counsel aggressively pursued local criminal proceedings to inflict further lawful pressure. Due to the lawful pressure exerted on the former CEO, they were forced to come to the settlement table, turn over the cold wallet, and eventually provide a full recovery of the assets. This example shows that when victims have been defrauded of their cryptocurrency in a foreign jurisdiction, it is important to think strategically about how to leverage multiple pressure points quickly and efficiently.

An application pursuant to 28 US Code 1782 ("1782") provides an additional method for victims of a given crypto-related fraud to obtain key evidence in support of cross-border enforcement and recovery campaigns. More specifically, a

1782 application may be deployed in connection with a foreign proceeding to obtain discovery in the US and gather evidence from exchanges, individuals, or any related party located in the US. Although the evidence is obtained in the US, the 1782 application grants victims the opportunity to submit key findings as evidence in a non-US proceeding where the fraudster or other players may be located. Alternatively, because 1782 applications may subject targets to subpoenas or force them to give testimony, they may be utilised defensively when entities or individuals have suspicious claims lodged against them. For example, in its representation of a cryptocurrency fund based outside the US, Kobre & Kim filed a 1782 application in the relevant federal district in order to force the other party to face a subpoena to support their factual contentions. As a result, the legal team used its expertise in cross-border discovery proceedings to identify the tight window in which the target would be traveling to the US and served the subpoena on them then.

Finally, where a plaintiff or victim is looking to trace or seize assets from a bankrupt adversary, there are a number of useful tools that US Bankruptcy Code Chapter 15 ("Chapter 15") may provide in domestic and foreign bankruptcy proceedings. For example, when an exchange has been hacked and cryptocurrency is believed to have been directed to (or through) the US and there is a foreign insolvency proceeding pending, Chapter 15 may allow foreign insolvency representatives to obtain discovery rights in the US via Rule 2004 Discovery, which grants interested parties in bankruptcy proceedings the right to obtain broad discovery from adversarial parties. Moreover, with respect to recovery efforts, Chapter 15 allows foreign insolvency representatives to assert avoidance actions under the insolvency laws of foreign jurisdictions in an effort to recover crypto-assets or other property that were once transferred into the US.

In its representation of a UK-based crypto-exchange, Kobre & Kim – in part – utilised Chapter 15 filings and related discovery measures in order to bolster the exchange's international recovery efforts. Specifically, the Chapter 15 petition requested recognition of the client's ongoing UK creditors' voluntary liquidation proceedings as the "foreign main proceeding" for the purposes of obtaining relief under Chapter 15 of the US Bankruptcy Code. The petition was granted by the judge after receiving no objections to the recognition request, and thus, the liquidators were granted relief in a USD32 million cybertheft.

It should be noted that Chapter 15 proceedings may also be used defensively. For example, a foreign creditor can apply for an automatic stay of the bankruptcy proceeding or other litigation within the US, and block attempts to seize the debtor's assets in the US. More concretely, in the middle of US proceedings against Mt. Gox – a Japan-based bitcoin exchange that ceased operations in 2014 due to extensive losses and theft – it filed for Chapter 15 bankruptcy protection, which supplemented the primary court proceedings in Japan and stayed the ongoing US litigation against the exchange, including a class action filed on behalf of US customers.

Government Seizures

While recovering stolen crypto-assets through traditional civil litigation mechanisms has proven successful in many instances, plaintiffs or victims may also benefit from seeking to have the US government file charges and/or seize assets against a given fraudster or wrongdoer. Importantly, choosing to present the case to law enforcement allows victims to pursue recovery of their stolen assets and take advantage of the government's jurisdictional reach and discovery resources without the burden of civil litigation expenses.

Contributed by: *Evelyn Baltodano-Sheehan, David H McGill, Benjamin J A Sauter and Amanda Tuminelli,* ***Kobre & Kim***

While the United States remains the global leader in crypto-asset seizures and has shown an even greater commitment to further asset recovery efforts, as evidenced by the launch of the National Cryptocurrency Enforcement Team in February 2022, other foreign jurisdictions, such as the United Kingdom and Hong Kong, are actively – in conjunction with the DOJ – looking to develop jurisprudence and increase resources given the growing prevalence of global crypto-fraud.

In the United States, perpetrators of crypto-fraud may be held criminally liable for stealing assets, laundering stolen funds, misrepresenting the nature of cryptocurrency-related investments, or otherwise violating securities laws. Often, the government will institute an investigation and immediately seize or freeze certain assets at issue. Under general asset forfeiture provisions, "any property, real or personal, which constitutes or is derived from proceeds traceable," to a violation of Section 1030 (relating to computer fraud) or Section 1343 (relating to wire fraud) is subject to confiscation by the US under either the general civil or criminal forfeiture provisions. Furthermore, if a crypto-asset is deemed to be "involved in" a violation of the US money laundering laws, then it, too, may be subject to criminal asset forfeiture proceedings by the US government (and laundering offenses allow commingled assets to be forfeited alongside the traceable proceeds).

Unlike an individual plaintiff who may not be able to afford to launch a full-scale investigation into a hack that targets hundreds or thousands of people, the government can use the vast investigative resources (including international co-operation treaties) at its disposal to benefit all victims. For example, if the perpetrators – or the assets themselves – are in a foreign jurisdiction, the government may seek assistance of those jurisdictions through traditional mutual legal assistance treaty (MLAT) requests, which allow the government to obtain documentary evidence that may otherwise be unavailable to an individual plaintiff. As just one of many examples, in November 2020, pursuant to an official MLAT request by the Brazilian federal authorities for assistance in a major internet fraud investigation, the US government seized crypto-assets valued at USD24 million that was sitting in the US. In Kobre & Kim's own experience representing a UK-based insurance company that was targeted by a ransomware attack – which resulted in its company's clients losing significant sums of cryptocurrency – the DOJ initially seized a de minimis value of assets domestically in the US. However, through MLATs and other foreign co-operation channels with Canada, the DOJ and Canadian authorities were able to freeze upwards of USD15 million in ransom funds.

Once the government identifies and charges an individual or entity who is allegedly engaged in criminal activity, victims may pursue the recovery of their assets through the government's criminal restitution proceedings. Victims may formally seek "victim status," which allows for victims to be granted statutorily mandated crime victim rights and permits them to have a more open line of communication with the prosecution team. Additionally, unlike narcotics matters – for example – once a criminal defendant is convicted of a crime involving seized assets, the US government is obliged to return the assets to the victims.

The US government's obligatory return of seized funds may come in one of three flavors:

- remission – when the Attorney General exercises discretion in returning recovered funds to a given victim of the fraud underlying the seizure or forfeiture;
- restoration – when the Attorney General permits the transfer of forfeited funds to a

criminal court for the ultimate fulfillment of a restitution order; and
- restitution – when a court orders a given defendant to directly compensate the victim for damage and injury, often paid for by the forfeited funds.

In total, since 2000, the DOJ has returned upward of USD11 billion in assets to victims of fraud. Specifically with respect to crypto-related fraud, the DOJ has outwardly highlighted that their 2022 budget requests include USD150.9 million more in resources to expand crypto-enforcement capabilities. Motivated by the proliferation of crypto-hacks and associated extortion activity in 2020, in April 2021 the DOJ formed a targeted task force to curtail ransomware attacks affecting the US. Beyond the expansion of resources dedicated to stopping crypto-related crimes, the DOJ has demonstrated success in recovering assets in high-profile matters. In addition to the Colonial Pipeline matter and the Bitfinex matter, in November 2020 the DOJ seized more than USD1 billion-worth of bitcoin in relation to Silk Road, the dark web marketplace on which users were able to buy and sell illicit goods – like narcotics and ransomware – with bitcoin.

As an advocate for a victim of a crypto-related crime, strategising regarding the right time to approach the government about an ongoing criminal action is crucial to an engagement's success. Unsurprisingly, earlier is always better. Generally, if a government investigation stalls, the government will have limited resources and reduced interest in re-engaging their recovery efforts. Thus, when it comes to recovering stolen assets, time is of the essence, and engaging counsel to assist in a given asset recovery campaign should come as soon as possible after the fraud occurs, in order to preserve all available recovery options.

As an added challenge with respect to government investigations, individual actors may often have little to no control over the investigation, its timing, or the manner in which the government makes its decisions. Furthermore, although the government's seizure powers are strong, the pace at which victims will actually receive their stolen crypto-assets may be slow, as it could take years for a criminal case to result in a conviction or for a civil forfeiture to be fully adjudicated. All of this is to say that – to mitigate the risks of recovering crypto-assets solely through government action – victims should consider parallel civil asset-recovery efforts for an added layer of security and efficiency.

Often, the public-private co-operation mentioned above has led to some of the most fruitful results for Kobre & Kim's clients. For example, in its representation of the liquidators to a New Zealand-based crypto-exchange, Kobre & Kim was able to assist the government in identifying the relevant fraudsters and lead the authorities to the stolen, laundered crypto-assets, by utilising enhanced forensic tracing capabilities and existing co-operation channels with the government.

Conclusion

As detailed above, when it comes to recovering stolen crypto-assets, victims and potential plaintiffs have many options at their disposal. Enhanced blockchain forensic tracing capabilities have made it easier to identify relevant fund flows and pathways for recovery. In addition, from a civil litigation standpoint, many of the traditional instruments in the asset recovery toolkit with which practitioners are already familiar may be applied to crypto-asset recovery as well, so long as the advocate understands blockchain technology and the forensics tools available. The future of asset recovery will necessarily include merging the old with the new and continuing to innovate as the technology rapidly develops.

Contributed by: *Evelyn Baltodano-Sheehan, David H McGill, Benjamin J A Sauter and Amanda Tuminelli,* ***Kobre & Kim***

Identifying counsel who has deep experience with asset recovery strategies and emerging blockchain technology is key to assessing the most viable criminal and civil litigation solutions for clients seeking to recover cryptocurrency assets.

Contributed by: *Evelyn Baltodano-Sheehan, David H McGill, Benjamin J A Sauter and Amanda Tuminelli,* ***Kobre & Kim***

Kobre & Kim is an Am Law 200 global law firm focused exclusively on disputes and investigations, often involving fraud and misconduct. Recognised as the premier firm for high-stakes cross-border disputes, the firm has a particular focus on financial products and services litigation (including digital currencies), insolvency disputes, intellectual property litigation, international judgment enforcement and asset recovery, and US government enforcement and regulatory investigations. Its specialised, integrated product offerings – International Private Client and Claim Monetization & Dilution – allow the firm to pursue aggressive and creative solutions to clients' underlying problems, whether they are financial, commercial or reputational. With more than 150 lawyers and analysts located in multiple jurisdictions throughout its 16 locations around the world, Kobre & Kim recognises the value of incorporating diverse perspectives and professional disciplines to generate the most effective solutions for its clients.

AUTHORS

Evelyn Baltodano-Sheehan is a former US Department of Justice (DOJ) prosecutor who focuses her practice on advising high-net-worth individuals, institutional clients and their executives in cross-border investigations, government enforcement actions and related asset forfeiture matters. She has experience in high-stakes matters where there is tension between parallel asset forfeiture and insolvency proceedings. Ms Sheehan also has an active international asset recovery practice, including the enforcement of judgments and arbitration awards and the representation of victims of crime. Her matters regularly involve legal actions across multiple jurisdictions and mobilising both public and private remedies. She has unique experience designing recovery strategies for claimants and insurers in the cryptocurrency industry.

David H McGill is a versatile litigator and investigator whose practice resides at the intersection of finance and technology. He frequently acts as lead counsel for companies and individuals involved in complex disputes, often with significant regulatory implications. His practice also includes conducting confidential internal investigations in response to whistle-blower claims and defending clients in government enforcement matters. Known as an aggressive advocate, he is often retained by hedge funds and proprietary trading firms in disputes involving allegations of spoofing and market manipulation, as well as other matters involving financial products. He recently obtained the first-ever dismissal of a criminal spoofing scheme charge in United States v Bases and Pacilio, No 18 CR 48 (ND Ill), and leading publications regularly quote him as a thought leader on matters involving algorithmic trading and digital currency regulation.

Contributed by: *Evelyn Baltodano-Sheehan, David H McGill, Benjamin J A Sauter and Amanda Tuminelli, **Kobre & Kim***

Benjamin J A Sauter aggressively defends clients in the cryptocurrency and commodity derivatives industries against high-stakes government enforcement actions. He has represented many of the most important companies and individuals in this space in many of the most important enforcement matters over the last several years. Clients, ranging from major cryptocurrency exchanges to leading proprietary trading firms, company founders and executives, turn to him for creative defence strategies when government investigations have festered or escalated and they are ready to adopt a more aggressive, trial-ready stance. In these representations, Mr Sauter is often deployed in a special-counsel role to enhance negotiation dynamics with regulators and prepare for contested litigation.

Amanda Tuminelli aggressively defends institutional clients and high-net-worth individuals against high-stakes criminal and regulatory investigations and enforcement actions. She also advises and defends clients in the digital currency industry, with particular focus on investigations relating to fraud and other allegations of misconduct. Ms Tuminelli also has an active asset recovery practice. She regularly designs aggressive and creative strategies to increase leverage and monetise high-value claims, and to plan and pursue global asset recovery campaigns. These strategies often include co-ordinating efforts across multiple international jurisdictions, analysing litigation risks posed by different governing bodies, and leveraging her experience tracing digital assets and cryptocurrency to arrive at public and private remedies.

Kobre & Kim

800 3rd Avenue
New York
New York 10022
USA

Tel: +1 212 488 1200
Email: kobrekimllp@kobrekim.com
Web: www.kobrekim.com

KOBRE & KIM