NORTON ROSE FULBRIGHT

“Cryptocurrency Crime: Examining Age-Old Fraud With a Modern Twist”

Celia Cohen and Matthew Niss, *New York Law Journal* — June 24, 2022

As cryptocurrency has become a ubiquitous part of modern finance, so too has it become the latest tool for criminals. While this new currency may seem disorienting to newcomers who are still grappling with the underlying technology, the crimes surrounding cryptocurrency are as basic as they come. Most fraudulent cryptocurrency schemes bear a striking resemblance to conventional frauds with which society is all too familiar, from Ponzi schemes, to investment scams, to basic theft. Where we used to see bank robberies, now we see hacking of crypto wallets and exchanges. In 2021 alone, crypto fraudsters absconded with over $14 billion worth of cryptocurrency, up from $7.8 billion in 2020. See MacKenzie Sigalos, Crypto scammers took a record $14 billion in 2021, CNBC.com (Jan. 6, 2022). But as described by Newton’s Third Law of Motion, for every action, there is an equal and opposite reaction. Law enforcement has responded to the rising incidence of fraud by increasing resources to prosecute cryptocurrency scams, and regulators are similarly focused on imposing regulations to curb the fraud and protect investors. While investigating and prosecuting such crime presents obstacles as the law and enforcement technology races to catch up, novel technologies are increasingly allowing investigators to overcome the pseudonymous nature of cryptocurrency.

Modern Cryptocurrency Frauds Take Several Forms, but Frequently Resemble Conventional Frauds. Cryptocurrency frauds often differ little from conventional frauds, aside from the type of assets involved. Some cryptocurrency fraudsters operate what are essentially classic Ponzi schemes. For example, in February 2022, the founder of cryptocurrency platform BitConnect was indicted for allegedly operating a “global Ponzi scheme” where early BitConnect investors were paid “with money from later investors.” See BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme, DOJ (Feb. 25, 2022). Similarly, QuadrigaCX, a Canadian cryptocurrency exchange, collapsed due to a massive fraud perpetrated by the now deceased CEO. See AquadrigaCX, A Review by Staff of the Ontario Securities Commission. The Ontario Securities Commission found that the exchange was essentially a Ponzi scheme and called it “an old-fashioned fraud wrapped in modern technology.” Id.

Celia Cohen is co-head of financial institutions, United States, at Norton Rose Fulbright US LLP. **Matthew Niss** is an associate at the firm.

Of course there is also the straight up theft method. Instead of robbing a house, a bank, or a pocket, these criminals hack cryptocurrency wallets or cryptocurrency exchanges without ever entering a physical space. See, e.g., *Strivelli v. Doe*, No. 22-2060, 2022 WL 1082638 (D. N.J. April 11, 2022) (victim's cryptocurrency and smart contract assets stolen from "hot" wallet by hacker); Statement of Facts, *United States v. Lictenstein*, No. 1:2-mj-000022, ECF No. 1-1 (D. D.C. Feb. 7, 2022) (defendants arrested after allegedly hacking into cryptocurrency exchange and stealing billions in cryptocurrency).

Other cryptocurrency scams involve variations on conventional securities fraud. The well-known "pump and dump" scheme, sometimes referred to as "scalping," has been used in the cryptocurrency space. In this scheme, a group of investors holding a large amount of an asset attempt to inflate its price, often by spreading misleading information about it. When the price rises high enough, the fraudsters rapidly sell their holdings and pocket the profits, causing the asset's price to collapse, and leaving the other investors to bear the losses. This fraud was allegedly used by John David McAfee, founder of the McAfee antivirus software company, in a scheme using altcoins, a type of cryptocurrency. See *United States v. John David McAfee*, 21 cr. 138 (S.D.N.Y., unsealed March 5, 2021). According to the indictment, after purchasing large quantities of the altcoins, McAfee allegedly used his vast social media following to artificially inflate their price through misleading messages, and then sold his altcoins during this temporary price increase. Id.

False statements claiming promises of high returns are also used in the crypto space to fraudulently induce investors to enter the crypto investment market. For example, such false statements allegedly were made to lure investors to invest in a cryptocurrency mining and investment program with "guaranteed returns." Instead of returns, the investors funds were subsequently diverted to the CEO and his co-conspirators. See Department of Justice, CEO of Mining Capital Coin Indicted in $62 million Cryptocurrency Fraud Scheme (May 6, 2022); see also *SEC v. Barksdale*, No. 1:22-cv-1933 (S.D.N.Y. March 8, 2022) (founders of Ormeus Coin allegedly lured investors by misrepresenting the duration and size of Ormeus Coin's digital asset mining operation, and then used millions of dollars of investor money for their own personal benefit). Other fraudulent offerings are referred to as a "rug pull." A rug pull often occurs on a decentralized exchange, where newly-listed coins are infrequently audited and anyone can offer a new coin, often pseudonymously. Such coins may be promoted aggressively by their creator to induce investors to swap other assets for the new coins. The creator of a new coin often holds the majority of the supply of coins, limiting liquidity in the market for the new coin, and thus other investors' ability to sell their positions in the newly offered coin. When the price rises sufficiently high, the creators sell their holdings of the new coin, taking investors assets for themselves and abandoning the coin offering, leaving its price to collapse. See, e.g., Squid Game crypto token collapses in apparent scam, BBC.com (Nov. 2, 2021).

Enforcement Agencies Direct Additional Resources to Combat Cryptocurrency Fraud. Perhaps unsurprisingly, enforcement agencies have responded to the rise in cryptocurrency fraud by directing additional resources to address these scams. The Securities and Exchange Commission announced in a May 3, 2022 Press Release that it would nearly double the size of its cryptocurrency and cybersecurity enforcement unit to address cryptocurrency fraud. The same month, the IRS and its international partners announced that they were pursuing more than 50 crypto-tax crimes, including one potentially $1 billion Ponzi scheme. See Tax Investigators Identify Potential $1 Billion Crypto Ponzi Scheme, Bloomberg (May 13, 2022). And most recently, the government brought a criminal prosecution against a defendant for allegedly using cryptocurrency to avoid sanctions. See Case No. 22 mj 067 (ZMF D.C.D.C).

Challenges in Investigating Cryptocurrency Fraud. Although cryptocurrency frauds often resemble conventional scams, certain unique aspects of cryptocurrency introduce challenges that law enforcement must overcome to recover stolen funds and to find perpetrators. Most significantly, it is difficult to "follow the money" in the pseudonymous world of cryptocurrency. The increasing prevalence of blockchain analysis software, however, has assisted crypto fraud investigations. Blockchain analysis software analyzes the vast amount of publicly available transaction data stored on the blockchain to detect patterns in seemingly unrelated transactions. Id. at *3. As a result, this software is sometimes able to trace pseudonymous cryptocurrency transactions back

to an identifiable, natural person. In fact, at least one court has remarked that it is "exponentially easier to follow the flow of cryptocurrency over fiat funds." See *In re Search of Multiple Email Accounts Pursuant to 18 U.S.C. §2703 for Investigation of Violation of 18 U.S.C. §1956 et al.*, 2022 WL 406410, at *2 (D.D.C. Aug. 26, 2021) (hereinafter, In re Search). Yet, cryptocurrency "mixing" or "tumbling" services, which break the connection between a wallet address sending digital currency and the addresses receiving them, make it harder for money to be traced. Although these mixing services make it more difficult for individual crypto wallets to be hacked, they also help criminals hide their identity and limit the ability to trace assets.

Law enforcement's efforts to trace cryptocurrency have been assisted by the judiciary's acceptance of blockchain analysis software. Courts have held that the warrantless use of blockchain analysis software does not violate the Fourth Amendment's proscription against unreasonable searches and seizures. Id. at *10-11; *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020). In addition, courts have repeatedly found that private blockchain analysis software is reliable. See In re Search, 2022 WL 406410, at *13; *United States v. Dove*, 2020 WL 9172971, at *3 adopted at 2021 WL 838737 (M.D. Fla. March 5, 2021).

Despite the capabilities afforded by novel technologies, challenges remain. Even where a perpetrator of cryptocurrency fraud can be identified, apprehending that person can prove challenging due to the often global nature of cryptocurrency transactions. Moreover, even where cryptocurrency assets can be recovered, a victim nevertheless may not be made whole. Cryptocurrency's value is notoriously volatile. See, e.g., How More than $1 Trillion of Crypto Vanished in Just Six Months, Wall Street Journal (May 13, 2022). A victim may recover their assets only to find that they are worth a fraction of their previous value.

Conclusion

Practitioners and investors need to keep apprised of the rapid developments in cryptocurrency. Cryptocurrency may be the wave of the future, but as with any new technology, wrinkles need to be ironed out and the law needs to evolve up. Eventually, a new equilibrium will be reached: Investing in cryptocurrency will become more ordinary; regulations and technological tools will increase or evolve; and with that evolution, the ability to combat fraud and abuse will fall more into line with conventional industries.