Crypto Mixer Laundering Case Provides Evidentiary Road Map

By **Peter Hardy and Kelly Lenahan-Pfahlert** (May 22, 2024)

Peter Hardy

Kelly Lenahan-Pfahlert

Tracking and tracing illicit activities conducted through digital currencies is difficult. The process can be very time- and resource-intensive.

Further, the government's ability to secure charges and arrests, and subsequent convictions, often requires the strong support of traditional sources of evidence, such as fact witness testimony and electronic communications.

Nonetheless, blockchain analytics is a key component of the government's ability to investigate and prosecute such cases.

On March 12, a jury in the U.S. District Court for the District of Columbia found Roman Sterlingov guilty on charges of money laundering conspiracy, so-called sting money laundering, operating an unlicensed money transmitting business and violations of the District of Columbia Money Transmitters Act.

Sterlingov allegedly laundered $400 million through Bitcoin Fog, a bitcoin mixing service that can be used to obscure the origins of cryptocurrency transactions.[1]

Shortly before the trial and guilty verdicts, the court issued an order[2] addressing the admissibility of expert testimony related to blockchain analysis software under the factors established by the U.S. Supreme Court's 1993 decision in Daubert v. Merrell Dow Pharmaceuticals Inc. to assess the reliability of expert testimony under Rule 702 of the Federal Rules of Evidence.[3]

Specifically, the trial court addressed proprietary software, Chainalysis Reactor, used by the private digital asset forensic firm Chainalysis, and whether expert testimony by witnesses propounded by the government — Luke Scholl from the FBI, and Elizabeth Bisbee from Chainalysis — could rely upon the Reactor software under Daubert.

Reactor is a software used to dissect bitcoin transactions, utilizing techniques to connect multiple addresses to a single entity. The defense raised multiple concerns about the reliability of Reactor.

The court found the expert testimony admissible under Daubert. Importantly, the court also noted that while Reactor was important to the government's case, it was not the sole basis for the prosecution's theories. Other evidence, such as materials found in Sterlingov's possession, online forum posts, IP analyses and traditional blockchain tracing, also supported the prosecution.

The court's decision has potentially significant implications for future cases involving cryptocurrency transactions and digital currency-related crimes. It establishes a precedent regarding the potential admissibility of evidence derived from such software tools, and underscores the evolving challenges and complexities of investigating financial crimes in the digital age.

As we will discuss, the decision provides a road map for future Daubert motions practice in similar cases, and, more generally, evidentiary arguments regarding whether the defendant committed the illicit transactions at issue.

Bitcoin and Reactor

Bitcoin relies on cryptographic protection and a peer-to-peer network for transactions. Simplifying greatly, bitcoin transactions involve a sending address, a receiving address and a private encryption key. These transactions are recorded on the blockchain, a decentralized and public ledger.

Each address is associated with a public key derived from a private key, with transactions forming a chain that can be verified through digital signatures. When a transaction occurs, it must include the amount of bitcoin, the sending and receiving addresses, and the sender's public key.

The government's experts in this case used Reactor to identify over 900,000 addresses associated with Bitcoin Fog, and allegedly traced substantial amounts of bitcoin transactions to and from Sterlingov, as well as several darknet market sites.

As the court explained, Reactor operates using three primary heuristics. A "heuristic" refers to a computational function or technique used to solve problems or make decisions based on available information. It is essentially a method for finding a solution that might not be perfect, but is practical and efficient.

Heuristics are used to cluster cryptocurrency addresses by identifying patterns or characteristics in the blockchain data that suggest they are controlled by the same entity. These heuristics help identify relationships between addresses and attribute them to specific entities or activities.

This is critical in regard to tracing, because knowing that a crypto transaction involved a certain address does not reveal who, specifically, is associated with that address.

The first heuristic used by the Reactor software, known as Heuristic 1, relies on the co-spend, or common spend, feature of the blockchain, where multiple input addresses are used in a single transaction. Heuristic 1 assumes that multiple addresses funding a single transaction are controlled by a single entity, because sharing private keys among different entities is highly unlikely.

Heuristic 2 observes and tracks specific on-chain behaviors and patterns unique to individual entities, allowing for the clustering of addresses based on these patterns.

Heuristic 3 utilizes off-chain information obtained from sources such as data leaks, court documents and exchanges to attribute addresses to specific entities.

Legal Standards

Rule 702 governs the admission of expert testimony.[4] Criteria under Rule 702 include demonstrating that the expert's knowledge will aid the trier of fact in understanding the evidence or determining a fact at issue, ensuring the testimony is based on sufficient facts or data, confirming the testimony is based on reliable principles and methods, and ensuring the expert's opinion reflects a reliable application of those principles and methods to the

case's facts.

In addition, under Daubert, four flexible factors to assess the reliability of expert testimony include whether the expert's theory or technique has been tested, subjected to peer review and publication, has a known or potential error rate, and has gained acceptance within the relevant scientific community.

Reliability Under Rule 702(c)

The defense challenge to Reactor's reliability focused on Rule 702(c), contending that Reactor "has not been peer reviewed and has no known error rate." Consequently, the defense argued, "any testimony based on Reactor is not the 'product of reliable principles and methods.'"

Despite the defense's concerns, the court found Reactor's reliability supported by sufficient corroborating evidence.

The court noted Scholl's extensive experience as a cybersecurity specialist with the FBI and current role as the lead tracing analyst for the U.S. Department of Justice's National Cryptocurrency Enforcement Team. Scholl detailed his extensive use of Reactor since 2016 in various investigations, attesting to its high reliability based on real-world application.

Specifically, Scholl elucidated how Reactor's clustering was routinely validated through legal processes, such as subpoenas to exchanges. He described a systematic process where the attribution of bitcoin addresses by Chainalysis consistently aligned with exchange records, thereby validating Reactor's clustering accuracy.

According to Scholl, this validation, occurring on a daily basis in blockchain analysis, underscored Reactor's reliability in attributing addresses to specific entities or activities.

Similarly, Bisbee, drawing from her former experience at the U.S. Drug Enforcement Administration and current experience at Chainalysis, emphasized Reactor's consistent clustering accuracy across numerous investigations. According to Bisbee, Reactor's results tend to be underinclusive due to its conservative approach, reinforcing its reliability by erring on the side of caution.

The government offered additional corroboration of Reactor's reliability, pointing to a confidential cooperating defendant's review of clustered addresses. This review revealed an accuracy rate of 99.9146%, affirming Reactor's effectiveness in attributing addresses.

Moreover, Reactor's performance in this case was validated through undercover transactions with Bitcoin Fog, in which Reactor accurately attributed addresses, as confirmed by manual tracing conducted by Scholl. This meticulous manual tracing served as a tangible validation of Reactor's clustering accuracy, solidifying its reliability in practical investigative scenarios.

The court found that Reactor's reliability was corroborated further by evidence presented by the defense. Sterlingov's pretrial testimony, acknowledging Reactor's accuracy in linking Bitcoin Fog to his accounts, aligned with the government's findings, further supporting Reactor's reliability.

Finally, the court found that the defense had received extensive information from the government about how Reactor works and had the opportunity to verify its results.

Analysis of Daubert Factors

In a detailed analysis, the court addressed the defense's argument that Reactor software failed to meet the Daubert factors. The court emphasized that the Daubert factors are not a definitive checklist and that the determination of reliability is within the trial judge's discretion.

Ultimately, the court deemed the government's proffered expert evidence admissible for jury consideration, emphasizing the roles of cross-examination and potentially contrary evidence from the defense.

Regarding the first factor, the court found that Reactor's clustering can be, and has been, tested, citing examples of manual tracing and utilizing competitor software, which produced similar but slightly different results, affirming the testability of Reactor's methodology.

As for the second factor, which considers peer review and publication, the court acknowledged Reactor itself hasn't undergone peer review. Still, the court highlighted the widespread academic approval of the underlying techniques, particularly noting the academic recognition of Reactor's co-spend heuristic.

Additionally, the court found that Reactor's unique algorithms tailored for specific cases would not naturally fit the traditional model of peer review.

Regarding the third factor, focusing on the method's error rate, the court found that although Reactor lacks a compiled error rate due to its conservative approach, the court emphasized the absence of false positives, corroborated by clustering results from other methods.

Lastly, the court evaluated the fourth factor, which considers general acceptance in the scientific community. The court underscored the extensive adoption of blockchain tracing tools like Reactor in both law enforcement and business sectors, citing Chainalysis as an industry-standard tool used by various government agencies and financial institutions.

Takeaways

The court's order provides a road map for future Daubert motions practice in similar cases, and, more generally, evidentiary arguments regarding whether the defendant committed the illicit transactions at issue.

The court's order contains the following points that government counsel can try to emphasize, and defense counsel can try to distinguish, in future cases.

First, both expert witnesses testified that Reactor had a successful track record spanning several years. Not all tracing technologies, however, will present such a track record.

Thus, for any tracing technologies that lack this type of demonstrated track record, defense counsel may be able to attack — under Daubert and Rule 702 — the reliability of the technology upon which the expert is purporting to rely.

Second, Sterlingov allegedly used Bitcoin Fog, a mixing service. But other mixing services can be more complicated and more opaque than Bitcoin Fog. Future cases may involve the use of evolving technologies, such as privacy pools and fully homomorphic encryption, which could make any forensic analysis less reliable than the one performed in the

Sterlingov case.

There are also other, off-ledger digital currencies that do not operate on the blockchain, and other distributed ledgers that are more difficult to trace than bitcoin, if they can be traced at all.

Again, different circumstances may present enhanced opportunities for defense counsel to undermine the reliability of the proferred testimony.

Even if the expert testimony is deemed admissible, such reliability concerns will inform both the weight of the testimony and cross-examination.

Third, according to the court's order, Sterlingov himself assisted the government's analysis. Both parties seemed to agree that the government's theory did not rely primarily on the use of Reactor. Rather, the government's evidence included "materials found in Sterlingov's possession when he was arrested, various posts on an online forum called Bitcoin Talk, [and] internet protocol ('IP') analyses showing an individual accessing accounts directly linked to the Bitcoin Fog administrator and accounts directly linked to Sterlingov in close temporal proximity."

Similarly, the court emphasized that Sterlingov admitted during pretrial testimony that the bitcoin in his account had been mixed in Bitcoin Fog, thereby conceding the main point of the government's theory. Future defendants or investigative targets may not be so obliging.

Fourth, the government's case relied upon a confidential cooperating defendant who confirmed that almost 100% of the addresses clustered by Reactor had been correctly clustered and attributed. Likewise, the government relied upon a sting operation involving undercover transactions directly with Bitcoin Fog.

Future cases may or may not involve fact witnesses, cooperating defendants or undercover operations. Even if they do, their effectiveness can vary. For example, many people involved in illicit digital currency schemes don't know the identities or geographic locations of their conspirators, because of the use of pseudonyms on the dark web, the lack of personal meetings and their avoidance of trackable communication devices.

Fifth, the court's order noted that the defense never obtained a Reactor license to run its own expert analysis to test or refute the government's analysis. Similarly, the court observed that the clustering analysis performed by Chainalysis can be replicated or refuted by the use of competitor software or, on a smaller scale, by manual tracing.

Future litigants, of course, can employ such testing to buttress or undermine the government's evidence.

Ultimately, the court's order highlights how time- and resource-intensive tracing digital currencies can be. Successful tracing can be achieved in specific cases, but often only after years of investigative work by a capable team using proprietary technology, bolstered by multiple sources of evidence.

The implicit lesson is that the vast majority of illicit transactions involving digital currencies — for example, a so-called pig butchering scheme run from abroad that drains the limited savings of multiple retirees — unfortunately will go untraced and unrecovered because it currently is not possible to replicate the forensic investigation in the Sterlingov case on a broad scale.

Peter Hardy is a partner, co-leader of the anti-money laundering team and co-leader of the tax controversy team at Ballard Spahr LLP. He previously served as an assistant U.S. attorney in Philadelphia and as a trial attorney for the DOJ's Tax Division.

Kelly Lenahan-Pfahlert is an attorney at Ballard Spahr.

[1] Compl., US v. Roman Sterlingov, No. 1:21-mj-00400 (D.D.C. Apr. 26, 2021).

[2] Mem. Op. and Order, US v. Roman Sterlingov, No. 1:21-cr-00399-RDM (D.D.C. Feb. 29, 2024).

[3] Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993).

[4] 28 U.S.C. 702.