Matt Green on Recovering $1.5M in USDC in Under Two Weeks: Legal "Nuclear Options" and Peer-to-Peer Strategy

By Matt Green, Partner and Head of Blockchain and Digital Assets and Technology Disputes, at Lawrence Stephens

LawrenceStephens*

As traditional finance houses seek to diversify and enter the decentralised world (bitcoin's value increased by 132% over the last five years), the obvious risks are less technical and more human.

Senior boards are hiring staff whose job specifications are sometimes not fully understood or wildly unfamiliar. Crypto traders often possess specific knowledge that is not widely shared across an organisation, posing a significant risk to business operations.

Little exemplifies this pattern more than a recent UK High Court case (held in private) brought by a London hedge fund that found more than 1.9 million USDC (a stablecoin called Circle, whose value is pegged to the U.S. dollar) drained from their trading account. They had no idea how this happened, no clear leads and no technical vulnerabilities.

This article deals with how lawyers, investigators and blockchain forensic firms helped recover most of the funds within nine working days from being instructed through to recovery, and how the most "nuclear" of legal tools can be used to secure fast and substantial results.

Tracing stablecoins and the smoking gun

The approximately 1.9 million USDC drained was traced by Token Recovery, a blockchain forensics firm that confirmed the funds were consolidated into a single address and remained there for several days. From experience, in the event of a theft, funds are quickly laundered via tumblers and put out of reach by a process known as "smurfing," whereby large sums of money are broken down into smaller transactions to remain undetected by anti-money laundering protocols and to frustrate tracing. The fact that this money remained in one place for several days indicated that the threat actor was likely unsophisticated and opportunistic.

It was suggested that the hedge fund conduct an internal investigation to determine whether any suspicious staff or activity indicated that the theft was an inside job.

The hedge fund found that one employee, a software engineer ("Mark"), had recently resigned, and according to access logs, took a particular interest in the targeted wallets on the day of the theft.

In response to certain behaviours during employment, the hedge fund had implemented human-resources-led monitoring software on his profile, which took a screenshot of his computer every few seconds, creating a video of his activities. The software had largely been forgotten, but was now vital evidence, given the direction of blockchain forensics.

The video showed that Mark:

- Reviewed the balances of the hedge fund's crypto trading accounts.
- Logged into the relevant servers which ran the trading engines.
- Initiated memory dumps of those engines and copied them to his local system.
- Loaded the files into a debugger and immediately navigated to the relevant private keys, which gave any holder the ability to withdraw funds from the relevant account.

- Then, moments later, searched Google for “Metamask” (cryptocurrency wallet management software) and “what is a Polygon wallet,” suggesting he intended to trade the funds on the Polygon market.

In all, this was key evidence, given there was no genuine reason for Mark to navigate to the private keys. It may have taken longer to consider this evidence without the forensics and laundering patterns.

Law enforcement

The incident was reported to police on several occasions, and a crime reference number was provided, to be handled by Action Fraud, a triaging service for law enforcement.

From the pace and manner following reporting, the hedge fund instructed its lawyers, law firm Lawrence Stephens Limited, of which the author is a partner, to make a move more quickly, given the evidence at hand. This is the timeline’s first working day.

Urgent injunctions, nuclear options

On the second working day, the hedge fund and its legal team appeared in the High Court on an urgent basis, seeking highly intrusive court orders.

The first was a proprietary injunction (an order to do or not do something with specific property or its traceable proceeds) over the approximately 1.9 million USDC, which in the meantime had started moving and was being laundered more professionally.

The second was a worldwide freezing injunction over Mark’s assets over £1,000 in value and up to $1.9 million (approximately £1.5 million) in total, preventing him from moving assets or money, except for his capped living expenses, without being in contempt of court.

The third was a search and imaging order (also known as an “Anton Piller”[1] order), which allowed the legal team to search Mark’s premises for relevant documents and electronic devices, gain access to relevant accounts, compel the delivery of information and hardware and image the contents of those devices.

This would ensure that critical evidence could be searched for, seized, recorded and preserved for future use. In short, it prevented Mark from destroying evidence that could potentially prove his liability and reveal to the hedge fund what happened to its stolen USDC.

Anton Piller orders are rare, granted by the courts in limited circumstances and widely viewed as the civil court’s “nuclear option.”There must be an extremely strong prima facie case to persuade the court to make such an order, and the court appoints a supervising solicitor to safeguard a defendant’s interests during the search.

The hearing was on an “ex parte” (without notice) basis, meaning Mark had no knowledge that this was happening. The court issued the orders that night. A private investigator was then hired to follow Mark’s movements and monitor his home.

Working day three was spent preparing documents for service and instructing forensic imaging experts (JS Held) who would image devices, and the supervising solicitors.

Home entry

Execution of the search was planned for working day four, a Friday. Service of documents was limited to between 0930 and 1400. There was always a risk that Mark might not be at home, that he (or any cohabitant) might refuse to open the door, or that he might jump out of the window and run away. In any of those cases, a new court order would likely be required. Had he wilfully refused to open the door, he would have been in contempt of court.

The investigator confirmed that Mark was seen entering the house the night before, and there was no evidence that he had left. The supervising solicitors knocked just after 0930 and woke the house. A relative opened the front door, shortly followed by Mark, who thought it was an Amazon delivery.

Mark was immediately served with the Anton Piller order. He had two hours to seek legal advice before the search party entered and was immediately required to hand over his mobile phone and other relevant electronic devices. He was not to be left out of sight for the day.

Search party

Two hours later, the legal team search party was allowed in. There was no protestation or outward denial of wrongdoing, and Mark granted access to the search party. The incumbents' movements were monitored carefully to mitigate the risk of Mark destroying key documents or dissipating his assets. As the funds are digital, any internet access is high-risk, and 30 seconds locked in a toilet is enough time to put the USDC or other assets out of reach. As ordered by the judge, his phone was imaged on site and returned without delay.

All relevant electronic items were secured, including mobile phones, a PlayStation5, USB sticks, memory cards and a gaming computer. Physical reviews of paper, including receipts and pages of old cheque books, might reveal seed phrases (a collection of innocuous words, which, when input, give access to a crypto wallet) or private keys.

Mark was required to give the forensic imaging team access to all relevant accounts, including financial and crypto trading accounts. He maintained various cryptocurrency accounts with several providers and also held an account for Monero, a privacy-focused cryptocurrency designed to make tracing difficult.

The search lasted until around 1730, a time deemed reasonable to avoid unnecessary intrusion. The next two days were a weekend.

Freezing order

Mark was also served with the worldwide freezing and proprietary orders on the search day. Although he could technically move funds and dissipate assets, if it were found that he had done so after service, he would have been in contempt of court (a criminal offence). The power of that deterrent may have been reinforced by his mother, who happened to be a lawyer. Non-compliance, in his mind, may be outweighed by the value of the assets.

The freezing order also required him to detail all worldwide assets worth more than £1,000 on working day nine. This is vital. If he had the stolen funds or any proceeds, he must disclose them — unless, in limited circumstances, they are incriminating — or face contempt of court.

Settlement negotiations

Settlement offers yield quick results, especially when court hearings are imminent and pressure is greatest. As the first hearing was ex parte, the process required a further hearing two weeks later to allow Mark, the respondent, to seek to amend, discharge or agree to continue the orders. This is called a "return date" and is for the benefit of the respondent following ex parte hearings.

Mark's lawyers made various attempts to settle. However, on working day nine, no agreement had been reached, and Mark was required to disclose his assets by 1730.

This was the overwhelming pressure point for settlement, because without a deal, Mark would now have to disclose his assets.

Eventually, Mark offered to agree to stay proceedings and discharge the orders, after which he would send more than 1.5 million USDC to the hedge fund directly, on a peer-to-peer basis.

Since trust was low, the preferred mechanism was inverse, such that the parties would agree that, upon receipt of Mark's funds, the hedge fund's lawyers irrevocably undertook to file a consent order (agreed by the parties) to stay proceedings and discharge the orders, subject to a short contract detailing terms. Mark was to send the funds in two stages, one dollar first, then the balance, to ensure transaction integrity.

The hedge fund made a take-it-or-leave-it offer: recover the money first, or Mark discloses and the parties proceed to litigation, knowing he had more than 1.5 million USDC that could be paid into the court as security during the proceedings. Mark took the deal.

Peer-to-peer settlement

This was a pure peer-to-peer settlement. The respective lawyers did not hold nor were they in any way in control of the flow of funds. On a call, Mark sent the first dollar, which the hedge fund received. Notably, the sending address was now identifiable, given that the transaction took place, and the hedge fund conducted a cursory review of the address.

Mark then paid the balance directly to the hedge fund.

Upon receipt, the consent order was filed, and proceedings were stayed. This was working day nine.

Decisive action

Understanding blockchain analytics helped to identify Mark, where there were no other obvious targets in the aftermath of an emergency. Convincing evidence of wrongdoing led to draconian injunctions and the Anton Piller order, which put enormous pressure on Mark. The settlement offer resulted in Mark's disclosure of approximately 1.5 million USDC, which was the determining factor.

Within nine business days, the hedge fund's team had changed the position from a complete unknown to obtaining more than 80% of the value of lost USDC, the hedge fund being satisfied that the balance had been dissipated and/or not worth the cost to pursue.

Often, published court proceedings involving lost cryptocurrency have yielded less-than-satisfactory results for victims. Accordingly, it is important to share success stories and show that recovery is real when the facts align and the analytics are well understood.

[1] Anton Piller KG v Manufacturing Processes Ltd [1976] Ch. 55