TRM

Operation CLAWBACK: Recovering $4.1M After a Violent Wrench Attack

METROPOLITAN POLICE

Metropolitan Police

Region
Europe

Industry
Law Enforcement

Products Used
TRM Forensics

Problem

A prominent cryptocurrency influencer had $4.3 million in digital assets stolen at knifepoint during a home invasion in Hackney. The suspects fled up the motorway while the stolen funds began moving across the blockchain.

Problem

- $4.1M in stolen cryptocurrency recovered and returned to the victim
- Three suspects convicted; sentences totaling 16 years and 1 month handed down
- Six UK forces coordinated under Operation CLAWBACK, now a model for crypto fund recovery

The attack: A $4.3 million heist in Hackney

On 17 June 2024, Emergency Response Patrol Team officers from the Metropolitan Police's Central East Basic Command Unit responded to reports of an aggravated burglary in Hackney. The victim, a well-known influencer in the cryptocurrency community, alleged that $4.3 million of cryptocurrency had been taken in a wrench attack: his hardware wallet forcefully stolen under physical duress, alongside cash, bank cards, and his car.

The attending officers had limited experience with cryptocurrency, but they did something critical. They recorded the victim's wallet details and escalated immediately to a specialist team.

Detective Constable Jonathan Leung, who investigates serious and complex offenses at Central East BCU, described the challenge these cases present: "This case highlights the growing challenge of investigating so-called 'wrench attacks,' where criminals use threats or violence to force victims to hand over digital assets. Unlike typical cybercrime, these cases combine a violent home invasion with complex digital financial investigations."

Following the funds: From split wallets to gift card receipts

With the victim's car flagged on the Police National Computer as stolen and the suspects caught on CCTV using a stolen bank card at a motorway service station, a multi-force response unfolded quickly. Officers from the National Police Air Service, Northamptonshire Police, and Leicestershire Police helped bring the suspects to a stop. But by then, the funds were already moving.

Detective Sergeant Stephen Bourne, who leads specialist digital-asset threat response for the MPS Specialist Crime Crypto Unit and serves as the force's Op Wrench lead, was brought in immediately. "The good news is that the team receiving the initial call knew that cryptocurrency was involved and their instinct was to look for advice," Bourne said. "Thankfully they came through to us."

Using TRM Forensics, Bourne traced the flow of ETH and tokens in real time. "Using TRM showed us a few things," he explained. "Firstly, we saw the funds being split into two discrete wallets. It's unclear why. This is speculation, but I suspect that the group committing the wrench attack were being directed and may have seen an opportunity to take most of the money for themselves."

Some moved into Bitrefill and MEXC; another portion converted into Monero, where the trail went cold. But the Bitrefill thread was far from finished.

"Seeing the funds move into Bitrefill and MEXC meant it was very easy to conduct quick follow-up inquiries," Bourne noted. Those inquiries revealed that the suspects had used the stolen funds to purchase Argos gift cards. "The suspects, making our work rather easy, ordered high-end electronics to their home address," Bourne said. New warrants were obtained and the team went back.

How a handwritten note led to 99% of funds recovered

During searches of the suspects' addresses in South Yorkshire, coordinated with South Yorkshire Police, officers found a handwritten note bearing the seed words to a crypto wallet containing approximately 99% of the stolen funds.

What followed was, as Bourne described it, a race against time. "At that point, it's a race against the clock to move those funds. You don't know who else might have access. It's a balance between speed and making sure you get things right. But very quickly we were able to move the funds to a wallet under police control."

Bourne was unequivocal about the note's significance: "Kudos to the officers who found it. It's the difference between a victim being hugely out of pocket or getting the majority of their money back."

How gift cards launched Operation CLAWBACK

The discovery that the suspects had ordered electronics to their home addresses using stolen funds prompted Operation CLAWBACK, a second wave of Metropolitan Police warrants in South Yorkshire to recover the purchased items and re-arrest the suspects under the Proceeds of Crime Act.

The case demanded the kind of persistence Bourne describes as essential: "The challenge here is about having the resilience to leave no stone unturned. You need to persevere and follow up when funds are seen to move from one wallet to another. When you see funds flying off in a few directions it might be tempting to follow some and ignore others. The reality is you don't know which line of inquiry is the important one."

Across the full investigation, six forces and units worked in coordination: the Metropolitan Police, South Yorkshire Police, Northamptonshire Police, Leicestershire Police, the National Police Air Service, and the MPS Specialist Crime Crypto Unit.

How blockchain evidence secured three convictions

Bourne prepared detailed blockchain visualizations from TRM Forensics, walking the court through each phase: the initial theft, the split wallets, the flows to Bitrefill and MEXC, the conversion to Monero.

"Presenting this evidentially is made much easier by using the charts that are created in TRM," he said. "Cryptocurrency might be easy to understand for those working with it frequently, but I was mindful that this would boil down to presenting in court. So along with a big introduction explaining that nodes are wallets and the lines connecting those nodes represent transfers, it's about making this understandable for potentially less technically minded individuals."

On 7 November 2025, all three suspects were convicted at Sheffield Crown Court. One 18-year-old received 67 months for aggravated burglary, transferring criminal property, dangerous driving, and theft of a motor vehicle. A second 18-year-old received 46 months for aggravated burglary, theft of a motor vehicle, and possession of a knife. A 17-year-old received 80 months for aggravated burglary, possession of criminal property, and theft of a motor vehicle. Their sentences total 16 years and 1 month in custody.

The outcome: Funds returned, a victim left to rebuild

Officers believe the victim was targeted after a data leak exposed his personal details alongside his high-profile presence in the crypto community. He received the recovered funds back, but recovery of funds does not erase the full impact.

Leung put it directly: "Wrench attacks weaponize fear. Victims aren't just hacked, they are physically threatened or assaulted in the real world, often suffering long-term trauma, loss of

security and oftentimes, financial devastation." The victim subsequently moved out of London and later left the country.

Bourne reflected on what the recovery meant: "I can totally understand that victims in these situations want two things. Firstly, they want us to catch the criminals. And secondly, they want us to get their money back. So, it was great to achieve this for the victim who understandably was really concerned that he might never see his funds again."

For law enforcement agencies beginning to encounter this threat, Operation CLAWBACK offers a replicable framework: specialist crypto knowledge, cross-force coordination, and physical searches conducted with blockchain awareness. As Bourne put it: "Crypto investigation without a tool like TRM is virtually impossible."

Protecting against wrench attacks: Advice from the Metropolitan Police

Detective Constable Anastasia Bezanidou of the Fraud and Digital Assets Team emphasizes that the first line of defense is keeping a low profile. Cryptocurrency holders should avoid publicizing their holdings online, and be mindful that routine decisions, like registering a business at a home address, can make that address publicly searchable through resources like Companies House.

Spreading assets across multiple wallets and storage methods, and enabling multi-signature authentication for high-value transfers, removes the single point of failure that attackers look for.

In public, situational awareness matters just as much as digital hygiene. Being alert to shoulder-surfing, limiting what travel plans and personal information are shared, and staying cautious about who is nearby during any transaction are habits that meaningfully reduce exposure.

For in-person cryptocurrency transactions, Bezanidou advises never meeting unknown parties alone or in isolated locations, keeping transaction amounts minimal, and being prepared to delay or relocate if circumstances feel unsafe. The goal, she stresses, is to become a harder target before an attack is ever planned, because once a wrench attack is under way, the window for prevention has already closed.

Watch the story

Looking for more? Explore all our case studies.