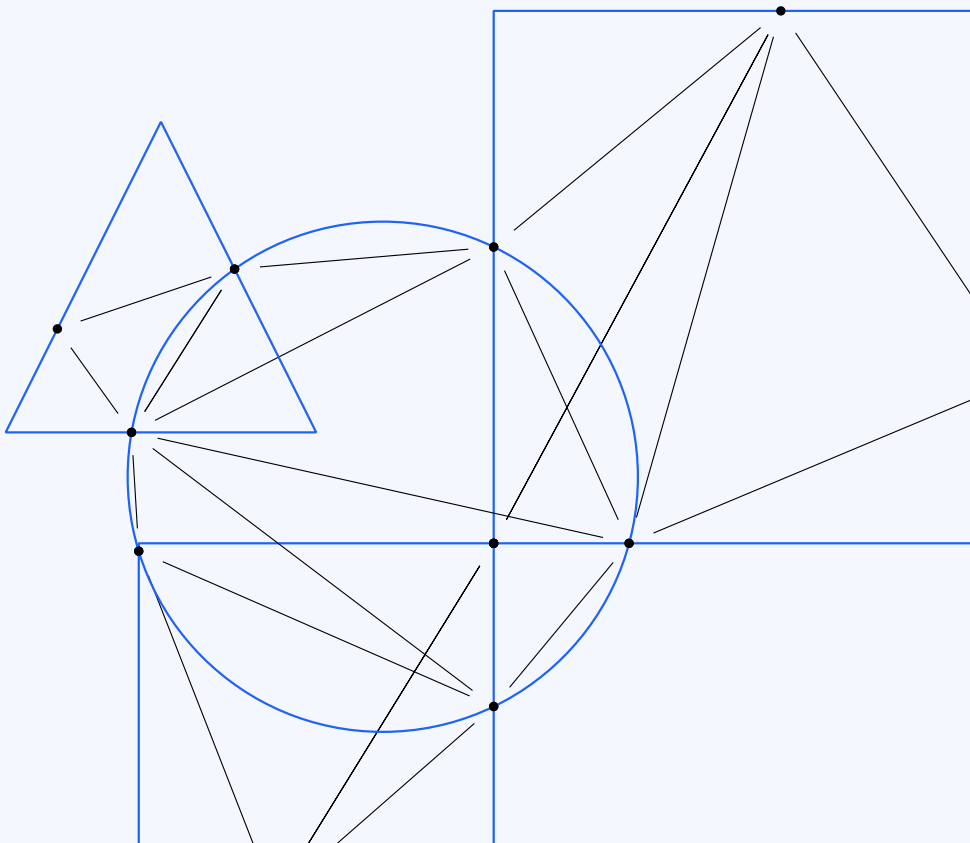
TRM | METROPOLITAN POLICE

WHITE PAPER

AUGUST 2026

Wrench Attacks: Crypto-Enabled Violent Targeting

A threat intelligence and response framework for law enforcement and financial institutions



trmlabs.com

Contents

EXECUTIVE SUMMARY

Key findings

Wrench attacks — premeditated, targeted offences using violence or the threat of violence to steal cryptoassets — represent a converging threat that neither law enforcement nor the financial sector can address effectively alone. This paper, co-authored by the Metropolitan Police Service and TRM Labs, provides an operational framework for each.

- The Metropolitan Police identified 17 reported wrench attack offences in London between March and December 2024. Kidnap was the most common offence type (59% of cases), followed by aggravated burglary (35%) and robbery (6%). The average cryptoasset loss per offence was approximately GBP 660,000.

- Wrench attacks are almost certainly underreported. Offence classification systems do not capture crypto-specific motive, and victims frequently do not report due to fear of repeat targeting, shame, or concern about scrutiny of their own asset holdings.

- In 2025, open-source research suggested that approximately 70 wrench attacks were carried out — more than double the 2024 figure. The trend is international, with significant incidents in the UK, France, the United States, and Canada.

- Post-attack proceeds follow identifiable on-chain patterns — cross-chain bridging, privacy coin conversion, and exchange deposits — that are traceable and, within a narrow time window (depending on how quickly victims report), recoverable.

- Coordinated action between law enforcement and exchanges within hours of an attack is the primary recovery mechanism. Consistent classification, fast escalation pathways, and real-time detection are the three variables that determine whether that coordination happens.

INTRODUCTION

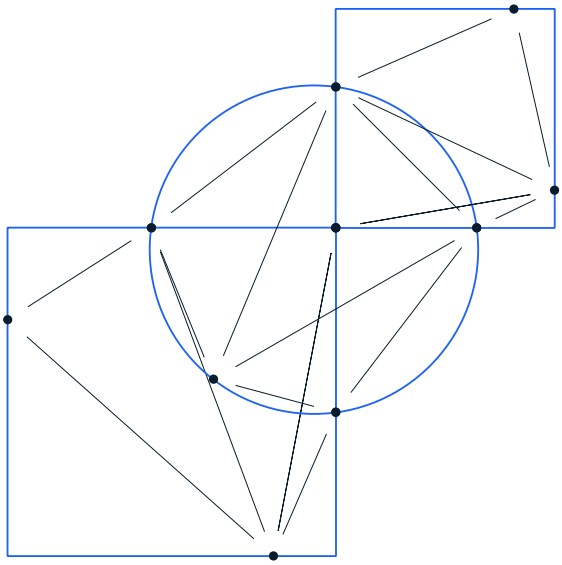
Wrench attacks are on the rise

Wrench attacks apply old methods — violence and coercion — to a new target class. As cryptoasset holdings have grown in scale and public visibility, a pattern of premeditated, targeted violent crime has emerged. Offenders identify individuals as high-value holders, surveil them, and use physical force or the credible threat of force to compel the transfer of digital assets.

For context on the broader crypto crime landscape, see TRM's 2026 Crypto Crime Report, which identified a record USD 158 billion in illicit crypto flows in 2025.

The Metropolitan Police Service (the Met) identified 17 reported offences in London over a nine-month period between March and December 2024; not an official statistic, but a signal of an emerging threat that almost certainly understates the true volume. Globally, open-source research suggested there were 18 attacks in 2023, 24 in 2024, and approximately 70 in 2025. This upward trajectory demands a systematic response.

Wrench attacks are physical crimes, but they are enabled and amplified by financial rails. Consistent recognition of the crypto dimension — in police systems, exchange monitoring logs, and industry reporting — is the foundation of an effective response.



PART 1

Understanding the threat

Definition and scope

A wrench attack is a highly targeted acquisitive offence — which may be charged as kidnap, aggravated burglary, or robbery — that uses violence or the threat of violence to steal cryptoassets, or to compel a victim to disclose access credentials or execute transfers under duress.

Intent and targeting are the defining characteristics, as victims are identified as holding high-value cryptoassets before an attack occurs. And while formal charge classification may vary, the underlying conduct does not.

A wrench attack is	A wrench attack is not
An offence where the primary motive is cryptoasset extraction from a targeted individual, and where reconnaissance, prior knowledge, or deliberate victim selection is evident.	An opportunistic robbery where cryptoassets are discovered incidentally, without prior intent to target a crypto holder.

Prevention and disruption strategies differ substantially between the two offence types.

Why wrench attacks are emerging now

Wrench attacks become more likely when three conditions align: incentive, target discoverability, and execution feasibility.

1. Incentive: The economics of crypto-targeted violence

From an offender's perspective, cryptoassets concentrate characteristics that most other high-value targets do not.

- **Value can be extreme and portable:** A single compromised seed phrase or exchange account can represent seven-figure sums.
- **Transfers can be immediate and irreversible:** Offenders can demand real-time proof of transfer, verify it on-chain, and exit before law enforcement responds. Law enforcement are also limited in the options they have to recover funds held in exchanges outside of their

regulatory regime, and with regards to funds held non-custodially where a suspect has not yet been identified.

- **There is no chargeback mechanism available to the victim:** Asset recovery requires either offender cooperation or law enforcement intervention.
- **Cross-border movement is rapid:** Proceeds can transit multiple services and blockchains within minutes.
- **Self-custody removes institutional safeguards:** There is no teller protocol or branch manager at the point of coercion.

The Met's analysis found that attackers often possessed specific, accurate knowledge of victim holdings before the attack — consistent with deliberate intelligence-gathering. Offenders appear to perceive cryptoassets as harder to trace than fiat currency, lowering their estimated risk of detection and disruption (an incorrect perception).

2. Target discoverability: How victims are identified

The Met identified four primary pathways by which victims came to the attention of offender groups:

- **Voluntary exposure (47% of identified cases):** Public posts about holdings, trading activity, influencer profiles, or visible association with a crypto business. Telegram and Discord groups organised around trading and meetups create concentrated, exploitable exposure for high-value holders.
- **Community exposure:** Crypto events, trading forums, and messaging channels that aggregate high-net-worth individuals and create target-rich environments.
- **Involuntary exposure:** Breach data, SIM swapping, or device theft that provides actionable intelligence about holdings. The Ledger hardware wallet data breach in July 2020 compromised 272,000 customer records, including physical addresses — a documented upstream risk factor in multiple subsequent cases.
- **Associational exposure:** Targeting family members or associates as proxies for reaching the primary holder.

3. Execution feasibility: How attacks succeed

Attacks documented in the Met dataset were coordinated and premeditated, not opportunistic. Most involved groups with defined roles and documented prior reconnaissance.

Kidnap, for example — which comprised 59% of the reviewed offence set — is by design an extreme control mechanism. Detaining a victim removes their ability to seek help, compresses the response window for platforms and law enforcement, and creates conditions where violence produces rapid compliance.

Where offender groups are digitally capable, coercion has included controlling the victim's communications, limiting their ability to raise an alarm, and sustaining pressure over extended periods — including ransom demands relayed through family members. Groups in the Met's dataset have been observed operating across county lines and, in at least one instance, internationally.

What we know about the threat landscape

Wrench attacks in the UK

Offence classification in police systems — which records the formal charge rather than the crypto-specific motive — means wrench attacks are systematically underrepresented in crime indices. Identifying them requires reviewing individual case reports to assess intent, a process that is resource-intensive and inconsistently applied.

Offence breakdown (Met-reviewed set):

Offence type	Share of Met-reviewed cases (March–December 2024)
Kidnap	59%
Aggravated burglary	35%
Robbery	6%

94% of recorded victims were male, ranging from 17 to 58 years old. And the average estimated cryptoasset loss per offence was approximately GBP 660,000. High-value physical assets including watches were also targeted in the same incidents, with an average physical loss estimated at approximately GBP 143,000.

Academic research indicates 50% of victims anticipated being targeted again, and seven out of ten expressed reduced confidence in exchange security measures following an attack[1].

[1] Ordekian, M., et al., 2024.

The 59% kidnap rate in the Met's reviewed dataset points to a threat consistent with organised crime rather than opportunistic street crime. These are coordinated operations with defined objectives, deliberate victim selection, and a willingness to use sustained violence.

Wrench attacks around the world

Open-source research suggests that approximately 18 attacks were carried out in 2023, and 24 in 2024. In 2025, the figure reached approximately 70 — consistent with growing cryptoasset wealth and public visibility.

High-profile incidents include the kidnapping of Ledger co-founder David Balland in France (January 2025, EUR 10 million ransom demand), the attempted kidnapping of a crypto CEO's daughter and grandson in Paris (May 2025), and a US Department of Justice prosecution of a 12-person racketeering conspiracy involving USD 263 million in stolen cryptocurrency.

As cryptoasset adoption grows and holdings become more visible, crypto holders become part of a targetable identity class across jurisdictions, demographics, and custody structures.

PART 2

Wrench attack typologies and how they unfold

Effective response requires understanding how attacks are structured. Response protocols — for both law enforcement teams and digital asset platforms — differ meaningfully across typologies. The five types below are drawn from the Met's reviewed dataset and international reporting.

Type A: Kidnap or mobile captivity coercion

A victim is forcibly moved or detained until assets are transferred. This was the most common offence type in the Met's reviewed set, and likely the preferred method for attackers because it allows the offenders to control the victim from start to finish and delays police involvement.

Attacks are typically organised, with orchestrated communication between suspect groups and clearly defined roles. The objective is to maximize control, minimize the victim's ability to raise an alarm, and sustain coercion until the transfer is verified on-chain.

Response protocols must account for the victim's inability to act independently.

Type B: Aggravated burglary coercion (home invasion)

Offenders gain entry to a victim's home — sometimes via deception — and use weapons, restraint, or threats to compel transfer.

The objective is access to physical devices, recovery phrases, and additional leverage including family members present. This offence type creates a potential for significant physical harm and often generates large evidential footprints (entry method, weapons, witness accounts) relevant to investigation.

Type C: Lure-to-location robbery

A victim is drawn to a location under false pretenses — a purported transaction, for example — and assaulted on arrival. The objective is a controlled encounter without the logistics of prolonged captivity.

In one case the Met handled, a victim was contacted by suspects posing as buyers, lured to a public location, immediately coerced at gunpoint, and held for many hours before a large ransom demand was made to his family.

Type D: Breach-to-violence escalation

An attack begins with digital or informational compromise — breach data, device theft, or SIM swap activity — and escalates to physical coercion once the target is validated as a high-value holder.

The objective is efficient target screening before committing to physical action. The Ledger data breach in 2020, which exposed hundreds of thousands of customer names and physical addresses, is a documented upstream risk factor in this pathway.

Exchanges can reduce their contribution to this exposure through stronger Know Your Customer (KYC) data security practices and rigorous data minimization.

Type E: Repeat victimization and intimidation cycle

The Met's dataset includes cases of repeat targeting and active victim intimidation to suppress reporting. One victim was targeted twice within a single month; another was explicitly threatened to withdraw from the police investigation.

The objective is to treat the victim as an ongoing source of value and deter law enforcement engagement. This typology has direct implications for victim support protocols at exchanges — including responses that a victim may trigger during or immediately after a first attack.

PART 3

The on-chain dimension: Laundering and asset recovery

Wrench attacks are physical crimes. But the proceeds are digital, creating both a challenge and an opportunity. Unlike cash stolen in a conventional robbery, cryptoasset proceeds leave a verifiable on-chain trail. That trail can be traced, and with sufficiently fast coordination, the proceeds can be frozen before they are cashed out or liquidated.

How on-chain proceeds move post-attack

Once an offender obtains access to a victim's cryptoassets, the clock starts for both parties. The irreversible and immutable nature of blockchain transactions means the primary window for asset recovery is typically minutes to hours. After that, proceeds are subject to rapid layering and obfuscation techniques designed to break the on-chain trail.

Common post-attack laundering patterns include:

Cross-chain bridging

Proceeds are moved across blockchains to break the tracing trail and exploit monitoring gaps in specific chains. In a March 2026 case involving approximately USD 24 million in stolen cryptoassets, funds were routed through a cross-chain bridging service toward conversion to Monero (XMR) — a privacy coin that substantially reduces tracing capability.

Privacy coin conversion

Conversion to Monero, Zcash, or similar assets is a common exit mechanism for bad actors. Once converted, on-chain tracing becomes significantly harder and requires specialized investigative techniques.

Mixing and tumbling services

Transaction mixers are used to obscure the origin of funds before further layering or exchange deposits. The use of mixers following a wrench attack is a strong investigative indicator.

Exchange deposits for liquidation

Proceeds are routed to centralized (CEX) or decentralized exchanges (DEX) for conversion to fiat

or other assets. Regulated exchanges are the primary intervention point for asset freezing — and the destination where KYC data can link receiving addresses to identifiable individuals.

Why on-chain intelligence matters for response

Blockchain intelligence fundamentally changes the response model for wrench attacks compared to conventional violent acquisitive crime. In a traditional robbery, once cash is spent, it is typically unrecoverable. But in wrench attacks, four things are different.

1. **The transfer is verifiable:** Law enforcement can confirm the on-chain transaction and establish the precise value taken — including which assets, at what timestamp, and to which address.

2. **The trail is traceable:** TRM Forensics enables law enforcement to follow the movement of funds across chains, into exchanges, and toward identifiable entities — even when offenders use bridging or mixing services.

3. **Freezes are possible:** When funds reach a regulated exchange, coordinated action between law enforcement and the platform can freeze assets before liquidation. The window is narrow — hours, not days — but it is real. Recovery operations have succeeded in multiple cases.

> Beacon Network is the industry's first real-time intelligence-sharing system that helps law enforcement, crypto exchanges, DeFi services, and stablecoin issuers stop illicit funds before they are cashed out. Verified investigators flag illicit addresses, and participating exchanges are alerted when flagged funds arrive on their platform so they can act to freeze them before withdrawal.

4. **Identifying bad actors is achievable:** On-chain tracing, combined with exchange KYC data obtained through legal process, can link receiving addresses to identifiable individuals, supporting prosecution.

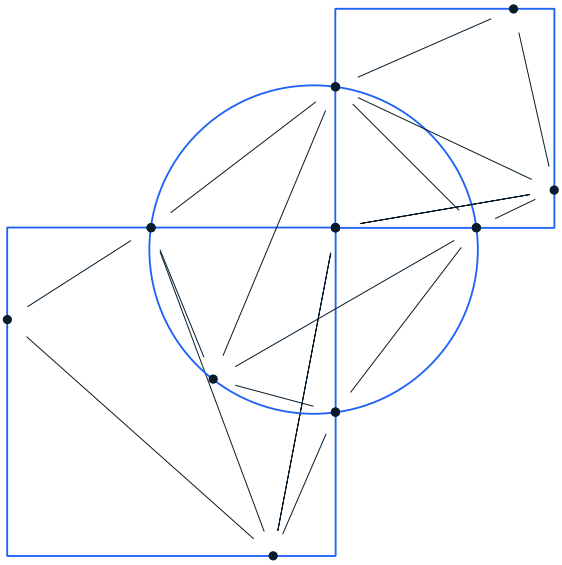
> TRM Labs created a dedicated subcategory — **Physical Theft or Wrench Attack** — in its attribution database in March 2026, enabling consistent tracking and cross-investigation intelligence-sharing. Law enforcement partners can request access to this intelligence through TRM's law enforcement support channels.

The misclassification problem

A critical barrier to effective response is misclassification — in both law enforcement systems and exchange monitoring systems.

When an offender coerces a victim into transferring funds, the on-chain transaction appears to exchange transaction monitoring systems as a voluntary transfer, with no indication of fraud: no unusual sender, no prior alert. The exchange has no way of knowing the transfer was made under duress unless the victim reports it promptly, or unless the exchange has implemented a duress protocol that generates a signal independent of victim action.

The same problem exists in law enforcement systems. As long as wrench attacks are recorded as generic robberies or burglaries — without the crypto-specific motive — agencies lose pattern visibility, and the case for specialized investigative capability, dedicated platform protocols, and resourcing goes unmade. Consistent classification matters for all downstream tools; blockchain forensics, anti-money laundering (AML) monitoring, and cross-agency intelligence-sharing all depend on the underlying data being accurate.



PART 4

A coordinated response model

By nature, the window in which enforcement teams can meaningfully respond to wrench attacks is compressed. The interval between a completed coerced transfer and an irreversible fund movement can be minutes. Effective disruption requires coordinated response between law enforcement, financial institutions and exchanges, and blockchain intelligence providers — not siloed, sequential hand-offs.

What law enforcement needs from crypto exchanges

Predictable, fast escalation pathways

Law enforcement needs a direct line of contact to the right team at each major exchange, reachable 24 hours a day, with authority to initiate an immediate account freeze on authenticated request. Standard legal request queues are not fit for this threat typology.

Operational duress protocols

Exchanges that implement duress signaling (e.g. a secondary PIN, a specific account action, or a silent alert to the exchange's security team) create an actionable signal for law enforcement. These must be operational and clearly documented for victims before an attack occurs.

Friction-based controls on unusual transactions

Law enforcement needs exchanges to create configurable delays on transfers that carry coercion indicators (e.g. sudden large withdrawals, transfers to addresses not previously used by the account, or high-value activity following extended inactivity). A mandatory review window can create the critical interval law enforcement needs to act.

Rapid data access

Investigating a wrench attack requires timely access to transaction records, KYC data, and IP logs for accounts receiving victim funds. Consistent, legally compliant data-sharing pathways — agreed in advance — reduce the delays that cost recovery opportunities.

Consistent victim guidance

When an exchange becomes aware of a wrench attack, it should provide clear documentation of what the victim should and should not do, including actions that could alert an offender during a live coercion event.

What crypto exchanges need from law enforcement

Rapid notification

Exchanges need to know they are holding wrench attack proceeds as quickly as possible. A direct notification pathway — bypassing standard legal request queues — enables action within the recovery window.

Clear authority to act

Exchanges operating across jurisdictions face uncertainty about their authority to freeze funds absent a formal court order. Law enforcement partnerships that clarify existing authority or provide rapid provisional authorization reduce this barrier significantly.

Consistent definitions and shared typologies

Without consistent offence classification, exchanges cannot calibrate transaction monitoring for wrench attack indicators. Shared typologies and definitions, updated as new patterns emerge, are the foundation of better detection.

Platform design principles for crypto exchanges

Financial institutions and exchanges have a platform-level role in reducing both the likelihood and the impact of wrench attacks. The following design principles translate the Met's operational requests into actionable guidance.

Minimize coercion surface area

Limit what an attacker can do quickly once they control a victim's device or account. Configurable withdrawal limits, delays on high-value or out-of-character transfers, and address allowlisting that prevents funds going to new addresses all reduce the coercion payoff.

Build duress protocols that work under pressure

A duress signal must be fast enough to trigger during a live coercion event, robust enough not to activate accidentally, and clearly documented so victims know it exists. The Met specifically

requests a 24/7 high-priority response channel where an authenticated trigger initiates an immediate, platform-wide freeze on the victim's withdrawals.

Treat KYC data as physically sensitive

Customer records — including names, addresses, and asset holdings — can become targeting datasets if compromised. Apply data minimization principles and restrict internal access to high-net-worth customer holding data to personnel with a genuine operational need.

Invest in real-time detection for coerced transfers

Transaction monitoring systems cannot detect duress directly. But behavioral signals — sudden large withdrawals, transfers to new addresses, rapid account changes after extended inactivity — are actionable indicators. Platforms with configurable monitoring, like TRM, can integrate wrench attack-specific patterns into alert logic.

Manage insider risk

Cases in the Met's dataset are consistent with insider exposure — where attacker knowledge of specific holdings suggests data was accessed from within a platform. Apply role-based access controls, audit trails, and anomaly detection on employee access to high-net-worth customer data.

Operation CLAWBACK: Recovering USD 4.1 million after a violent wrench attack

In June 2024, the Met responded to a violent aggravated burglary in Hackney in which a cryptocurrency influencer had USD 4.3 million in digital assets stolen at knifepoint.

Using TRM Forensics, the Met's Specialist Crime Crypto Unit traced the stolen funds in real time — following them through split wallets, a Bitrefill conversion, and a partial move into Monero. A physical search of suspects' addresses uncovered a handwritten note bearing the seed words to a wallet holding approximately 99% of the stolen funds. USD 4.1 million was recovered and returned to the victim.

Three suspects were convicted at Sheffield Crown Court in November 2025, receiving sentences totalling 16 years and 1 month. Operation CLAWBACK — coordinated across six forces — is now a model for crypto fund recovery in the UK.

Read the full case study here →

CONCLUSION

Classification drives resourcing

Wrench attacks represent a convergence that neither law enforcement nor the crypto industry can address effectively in isolation. These are organized, violent crimes that exploit digital infrastructure. Disrupting them requires physical investigative expertise and on-chain intelligence operating together, in real time.

The patterns in wrench attack activity identified by the Met are consistent with an international trend that reached approximately 70 reported cases in 2025 (a figure that likely understates the true volume and frequency of these crimes).

As cryptoasset adoption grows and wealth becomes more visible, the targeting of crypto holders as a class will intensify without a coordinated, sustained response.

About TRM Labs

TRM Labs is the intelligence platform for public safety and national security, built to detect and disrupt the criminal networks that exploit frontier technologies including cryptocurrency and AI. Combining proprietary intelligence, AI-native investigations software, and disruption network infrastructure, the platform is built for high-consequence environments where accuracy, auditability, and security are essential. TRM is trusted by 600+ government agencies and financial institutions across 75 countries to counter fraud, scams, cyber crime, child exploitation, money laundering, and sanctions evasion, among other illicit activities.

To learn more, visit www.trmlabs.com