ICC FraudNet
Global Annual Report 2025

THE STATE OF FRAUD AND ASSET RECOVERY: TIMELESS CRIMES, MODERN APPROACHES

EDITED BY
DR DOMINIC THOMAS-JAMES

ICC FraudNet

Dealing with the Challenge of Encrypted Messaging Apps

Martin Kenney & Harley Thomas
MKS Law

Introduction

Success in asset recovery and criminal accountability will increasingly hinge on adaptive strategies that mirror fraudsters' agility, harnessing technology and international cooperation to overcome substantial evidentiary and jurisdictional barriers.

The revelation that members of the US government shared extremely sensitive military operational information via the Signal messaging app has brought into close focus just how common encrypted messaging has become.1

Journalists, politicians and, of course, the criminal fraternity have all turned to encrypted messaging platforms. These have unfortunately become integral tools in global fraud schemes, too, posing significant challenges for asset recovery professionals. While platforms like Signal, Telegram and WhatsApp provide valuable privacy protections for legitimate users, they have simultaneously evolved into a critical infrastructure for orchestrating and concealing sophisticated financial crimes.

Fraudsters leverage these encrypted architectures with their decentralised communication and limited metadata retention, to perpetrate cryptocurrency scams,

[1] See: https://www.nytimes.com/2025/04/20/us/politics/hegseth-yemen-attack-second-signal-chat.html (accessed 15 June 2025)

investment fraud and advanced asset concealment operations, complicating cross-border investigations and recovery efforts.

Large-scale organised fraud groups frequently take advantage of Telegram's client-side open-source structure, for example. These criminal enterprises exploit the app's expansive private groups, promoting fraudulent investment opportunities and directing victims toward decentralised cryptocurrency exchanges or peer-to-peer transactions.

Conversely, WhatsApp is commonly utilised for intensive, targeted engagement through one-to-one interactions, notably in so-called "pig butchering" (romance) schemes. Victims are meticulously groomed over extended periods, fostering trust and deepening deception, before being persuaded to part with their funds.

Law enforcement agencies face substantial difficulties when securing crucial evidence from any of these encrypted mobile platforms. Investigators typically begin by attempting to access encrypted data directly from seized mobile devices. Yet the challenges posed by device encryption, local storage permissions and auto-deletion features often hinder forensic retrieval.

In the UK, law enforcement can legally access communications through device seizures under existing legislation, via the Police & Criminal Evidence Act 1984, the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. However, practical retrieval is often limited by the technical nature of the layered encryption and remotely stored electronic data ('RSED').

Barriers and hurdles

Legal and evidentiary hurdles compound these technical challenges. There are severe obstacles for investigators dealing with Telegram, for example, while WhatsApp operates under US jurisdiction and for UK investigators, at least, there is the slow pace of mutual legal assistance treaty ('MLAT') processes to navigate.

Consequently, evidence admissibility is frequently contested. For instance, the European Union's General Data Protection Regulation ('GDPR') imposes strict rules on data access and transfer, which can delay or hinder cross-border access to encrypted communications.

Forensic strategies now include a blend of blockchain analytics, open-source intelligence ('OSINT'), and metadata triangulation to mitigate these barriers. Platforms such as Chainalysis, TRM Labs and Elliptic facilitate tracing assets across crypto wallets. Investigators routinely combine these analytical tools with linguistic analysis and device imaging. This allows investigators to construct models revealing links between suspects across platforms, transactions and communication trails. Metadata such as IP logs, device

identifiers and timestamps also provide essential leads even when message content remains inaccessible. Yet criminals are sophisticated too and these specialist companies have varying capabilities and experience when faced with these complex tasks.

Breakthroughs

Recent legal innovations reflect a growing awareness of the need for adaptive procedural strategies. Asset recovery litigators increasingly pursue worldwide freezing orders to halt asset dissipation, targeting exchanges and digital asset custodians that are identified via forensic tracing.

Composite disclosure orders, merging Norwich Pharmacal Orders with international cooperation instruments (such as letters of request/letters rogatory, or Hague Convention requests), enable simultaneous cross-jurisdictional disclosures, significantly enhancing this process.

Additionally, disclosure requests directed at third-party entities, including internet service providers, virtual private network providers, hosting services and payment processors, play a critical role in uncovering crucial metadata.

Courts in offshore jurisdictions, notably the British Virgin Islands and Cayman Islands, have shown growing flexibility in adapting proprietary injunction principles specifically for digital asset recovery. However, compliance with digital sovereignty laws, such as GDPR data protection protocols, means careful coordination is necessary in order to prevent procedural complications or delays.

This is a rapidly evolving landscape. There are procedural innovations emerging, such as the ability to serve legal notices via digital NFTs (non-fungible tokens), as well as the growth of technologies such as smart contracts, which automate the actions required in blockchain transactions. These align potential remedies to the operational realities of digital-native criminal environments.

UK law enforcement agencies also actively collaborate with their international counterparts in this arena, including EC3 (Europol Cybercrime Centre) and JCAT (Joint Cybercrime Action Task Force). Such intelligence sharing, and the use of joint investigative task forces and parallel civil and criminal proceedings, increases the effectiveness of asset recovery efforts.

UK enforcement developments and the EncroChat precedent

Another key development in the fight against encrypted criminal communications, from a UK perspective, has been the relatively recent success of the National Crime Agency ('NCA').

In 2020, working with French and Dutch authorities under Eurojust and Europol coordination, the NCA gained covert access to millions of messages sent via EncroChat, an encrypted phone service used almost exclusively by organised crime networks.

This led to Operation Venetic and thousands of subsequent arrests, as well as seizure of assets and prosecutions. It is deemed a landmark success in this space. The operation demonstrated not only the value of technological infiltration, but also the critical role that international cooperation plays in piercing the veil of encrypted messaging systems.

The UK courts upheld the admissibility of intercepted EncroChat messages, even where live intercepts would typically breach domestic law under the Investigatory Powers Act 2016. This precedent has instigated a broader legal debate around admissibility of digital evidence, interception standards, and the balance between privacy rights and public interest in the digital age.

The EncroChat litigation has underscored the possibility of using intercepted communications as primary evidence in serious and complex fraud and money laundering cases, a key development in prosecutorial strategies.

This success has emboldened UK law enforcement and intelligence agencies to invest further in offensive cyber capabilities and infiltration techniques. The NCA's recent launch of a National Security and Cyber Crime Unit ('NSCCU'), detailed in its 2025 strategy, confirms a shift toward more proactive, intelligence-led operations, particularly targeting crypto-enabled organised crime. The NSCCU's mission includes penetrating encrypted messaging ecosystems, deploying lawful hacking capabilities, and enhancing data acquisition through international alliances.

Notably, UK authorities are increasingly deploying civil recovery powers under the Proceeds of Crime Act 2002 ('POCA') in parallel with criminal investigations. These powers allow the freezing and forfeiture of assets even where criminal convictions are not secured, a vital tool when prosecutorial evidence remains locked behind encrypted systems or foreign legal barriers. Civil asset recovery claims are often paired with disclosure applications and third-party subpoenas to exchanges, custodians, and serviceproviders whofacilitateorunknowinglyhost criminalactivity.

The EncroChat example, combined with the legal flexibility of civil recovery mechanisms and the rising strategic importance of public-private partnerships, points to a future in which UK enforcement agencies take a more active role in combating fraud via encrypted platforms.

These developments also reflect growing judicial comfort with novel evidentiary sources, technical expert input and hybrid legal proceedings. As encrypted messaging

usage proliferates among fraudsters, so too must the legal and technical agility of those charged with pursuing them.

Conclusion

In conclusion, addressing the misuse of encrypted messaging platforms in global fraud schemes demands multi-jurisdictional collaboration, sophisticated technological fluency and continuous procedural innovation.

Success in asset recovery and criminal accountability will increasingly hinge on adaptive strategies that mirror fraudsters' agility, harnessing technology and international cooperation to overcome substantial evidentiary and jurisdictional barriers.

Proactive engagement between law enforcement agencies, regulatory bodies and legal professionals will further strengthen these collaborative frameworks.


ICC
FraudNet


MKS
LAW