ASTRAEA

Inside Access:

How Organised Crime Exploits UK's Financial Services Sector

The UK's banking sector is increasingly vulnerable to insider threats - risks that originate from within the institution itself. Organised crime groups are sophisticated, well-resourced, and highly motivated, and their ability to exploit internal systems and personnel poses a serious challenge to financial institutions. These actors are not only entrepreneurial but also adept at navigating complex compliance environments. To safeguard operational integrity and regulatory standing, banks and non-bank financial services providers (collectively referred to here as 'banks') must deepen their understanding of insider profiles, attack vectors, and investigative methodologies in an ever-evolving threat landscape.

Fraud and Organised Crime: A Critical Nexus

Fraud is a core revenue stream for OCGs. The UK government's Economic Crime Plan 2 for 2023 to 2026 warns that economic crime, including fraud, "fuels the serious organised crime that damages the fabric of society" [1]. This is not just a financial issue; it is a national security concern.

RUSI's recent research, 'Following the Fraud: The Role of Money Mules', reinforces this point, describing fraud as "one of the most profitable crimes" for criminal networks, with low barriers to entry and high returns [2]. These groups exploit the UK's financial system to steal and launder billions, often using money mule networks to obscure the trail. Alarmingly, funds can move through mule accounts in as little as 15 minutes, leaving institutions with a razor-thin window to detect and disrupt illicit flows.

> Economic crime poses a rapidly growing, and increasingly complex, threat to UK national security and prosperity. Criminals continue to seek ways to commit, and benefit from, economic crime including fraud, money laundering, sanctions evasion and corruption. This fuels the serious organised crime that damages the fabric of society.
>
> - HM Government's 'Economic Crime Plan 2, 2023 - 2026

The scale of the problem continues to grow. According to a recently published report by the UK's Home Office, fraud now accounts for over 40% of all crime in the UK, with an estimated 4.1 million incidents in the year ending December 2024 — a 31% increase on the previous year [3]. This upward trajectory, combined with the involvement of sophisticated OCGs, underscores why fraud is increasingly treated as a strategic threat rather than a routine financial crime.

[1] HM Government's 'Economic Crime Plan 2, 2023 – 2026', published in March 2023
[2] RUSI's Report on 'Following the Fraud: The Role of Money Mules', published on 14 August 2025
[3] HM Government's 'Economic Crime Plan 2: outcomes progress report', published 2 September 2025

Who Are the Threat Actors

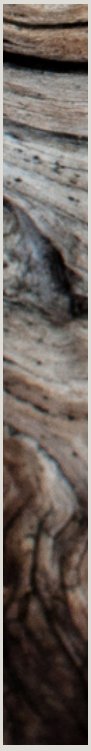
Organised Crime Networks: These groups are at the core of insider threats in banking, often engaging in various forms of criminality, including human trafficking, drug and arms smuggling, tax evasion, sanction circumvention, fraud, and online scams. They infiltrate financial institutions to launder money and enable other criminal activities.

Super-Facilitators: These individuals or entities offer money laundering (ML) services to criminal organisations, enabling them to obscure the origins of illicit funds.

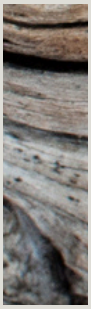
Unregulated Money Service Businesses (MSBs): Controlled by organised crime, unregulated MSBs are increasingly used as vehicles for laundering money and moving illicit funds globally, often into and through conventional banks.

How Do Insider Threats Manifest?

Insider threats can take multiple forms, and banks must be aware of the various methods through which these actors infiltrate or exploit employees:



- Compromised Employees: Some employees, or even disgruntled former staff, may sell sensitive information, access credentials, or even assist in opening fraudulent accounts through the dark web. They might also act as money mules, using their own accounts to move illicit funds.
- Targeted Individuals: Employees can be approached or coerced by criminal networks, often with cash incentives or under duress. This is especially true when employees face financial difficulties or are exposed to external pressures.
- Planted Personnel: Criminal organisations may recruit and insert individuals directly into bank roles to facilitate internal fraud or money laundering schemes.
- Supplier Vulnerabilities: Third-party vendors that service multiple financial institutions may become targets, exposing banks to risk. Insecure or inadequately controlled supply chains can provide opportunities for criminals to infiltrate.



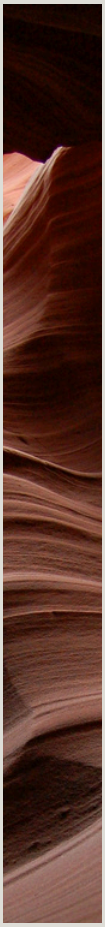
- Community-Based Hiring Risks: Banks often hire from the communities they serve, which is generally positive. However, it can also expose the institution to community pressure or nepotism, increasing the risk of insider exploitation.

- Exploitation of Employee Financial Stress: Criminals may target employees or their families experiencing financial hardship, coercing them into participating in fraudulent activities or providing sensitive information.

> The increased fragmentation of the payments system has made it harder to track the flow of funds, and criminals appear to be able to exploit the relative weaknesses in the financial crime controls of these newer firms.
>
> - RUSI's Report on 'Following the Fraud: The Role of Money Mules'

Investigating Insider Threats

Effectively addressing insider threats requires a multi-layered approach involving monitoring, intelligence sharing, and continuous improvement of controls. Here are some key methods used to investigate insider threats:



- Monitoring & Anomaly Detection: Banks must monitor key performance indicators (KPIs) around account openings, suspicious patterns, and control breaches. Anomalous activities, such as unusual spikes in activity during specific working hours or sudden behavioural changes in staff, can be red flags.

- Intelligence Sharing: Collaborating with external agencies and other financial institutions is crucial for identifying emerging trends and learning from past incidents.

- Look-Back Reviews: When suspicious activity is detected, institutions should conduct detailed look-back investigations. For example, if an account is flagged for funnelling large volumes of funds after being dormant, banks should analyse who opened the account, how it was used, and check if the KYC (Know Your Customer) data has been reused or appears elsewhere.

- Learning from Past Incidents: It is not enough to move on after an issue has been resolved. Banks must continually learn from their experiences and integrate these lessons into stronger controls.

- Control Framework Improvements: Regular updates and improvements to the controls framework are essential to staying ahead of potential vulnerabilities.

- Spot Checks and Audits: A robust internal audit function should conduct regular spot checks, especially on employees and accounts flagged during monitoring.
- Pre-Employment Screening: Comprehensive pre-employment checks, including background screening, can help mitigate risks before they materialize.
- Multi-Domain Surveillance: Banks should employ multiple layers of surveillance, including electronic monitoring, visual checks, and online surveillance of dark web activities and chat forums.
- Whistleblower Framework: A well-publicized and trusted whistleblower reporting framework can encourage employees to report suspicious activities without fear of retaliation.
- Exit Interviews: Conducting detailed exit interviews can uncover issues related to potential insider threats, especially if employees are leaving under suspicious circumstances.
- Thorough Investigations: When red flags are identified, banks must conduct thorough investigations, leaving no stone unturned.

Increasing Threats Amid Global Instability

Geopolitical tensions and trade wars, sanctions, economic downturns, and rising inflation are all exacerbating the risk of insider threats in banking. As individuals face increasing financial pressures, they may become more susceptible to exploitation by criminal networks.

In addition, cash smuggling operations and criminal activity targeting vulnerable financial services such as post offices are on the rise, further complicating the landscape for banking institutions.

Conclusion

Insider threats are a growing concern for UK's financial services sector, driven by increasingly sophisticated organised criminal networks and heightened economic pressures. Banks must remain vigilant, adopt a proactive approach to monitoring and investigating these risks, and continually improve their controls to safeguard against insider threats.

By implementing a comprehensive, multi-faceted strategy, banks can better detect and prevent these threats, ensuring the integrity of their operations and compliance with global regulations.

ASTRAEA

Legal and professional services, from every angle

Astraea is a special situations legal and professional services firm committed to protecting our clients' interests, mitigating risk and unlocking opportunity.

Our areas of expertise include:

- Special Situations Advisory
- Dispute Resolution
- Regulatory and Compliance
- Forensic Investigations and Intelligence
- Reputation Management and Crisis Response
- Fintech and Digital Assets Advisory
- Civil Fraud
- Private Client Advisory

Get in touch

info@astraea-group.com

0208 092 8411

Astraea Group Ltd
7 Down Street, London, W1J 7AJ

Author

Piers Rake
Partner, Astraea

T 0208 092 8411
M 07355 674 158
E piers.rake@astraea-group.com

Piers is the head of Astraea's intelligence & forensic investigations team.

A Solicitor, CEDR Accredited Commercial Mediator, Certified Fraud Examiner, and Forensic Investigator, he has particular experience investigating economic crime and advising regulated businesses on their legal and regulatory obligations, having been global head of financial crime investigations at Barclays Bank Plc.

SRA No. 806283