Grant Thornton

Where fraud meets money laundering

Decoding the money mule and the case for a unified fraud-AML response in banks

Content

The problem sitting between two teams

In many banks, fraud and money laundering are still treated as separate challenges: Fraud teams focus on losses, chargebacks and customer harm; AML teams focus on typologies, suspicious activity reporting and regulatory scrutiny. They often operate through different reporting lines, systems and language, and exchange intelligence only after the damage is done.

Money muling activity shows why that separation no longer works. A mule account can be both the endpoint of a fraud and the start of a laundering chain. When a scam victim sends a payment, the funds may land in a mule account and be moved onward within minutes, withdrawn as cash, spent by card or transferred into a virtual-asset wallet. The fraud team sees a recall request. The AML team sees activity inconsistent with the customer profile. Neither team, on its own, sees the full pattern.

Mule activity cannot be controlled through fraud prevention or AML monitoring in isolation. Effective control requires the combined use of payee verification, behaviour-based monitoring, device and network analytics, targeted cash controls and stronger source-of-funds enquiry. The direction of travel is clear: institutions need to move beyond asking whether something is a fraud case or an AML case. They need to ask what the account is telling them, what the wider network shows and who needs to act.

Why the mule connects fraud and AML

A mule performs an essential laundering function, often using funds that originate from fraud, drug trafficking or another serious predicate offence. That has three practical implications:

1. **The predicate offence may be fraud, drug trafficking or another serious financial crime.** In fraud cases, the first signal may sit with the fraud team through recalls, indemnity claims and victim reports. In drug-trafficking or other predicate-offence cases, the signal may emerge through cash activity, behavioural monitoring or law-enforcement intelligence.
2. **Laundering makes the fraud profitable.** Mules provide the cash-out and layering capacity. Disrupting the network can make the underlying fraud less viable.
3. **The signals are shared.** Rapid pass-through, salary accounts with no salary, dormant accounts reactivating, shared devices, recycled phone numbers and beneficiary-name mismatches may sit across fraud and AML systems. Individually they can be weak; combined they can be compelling.

Mule networks exploit this seam deliberately. A fraud rule designed for card misuse may miss a transfer that looks like a family payment. An AML scenario calibrated only to a broad customer segment may miss a student moving many times their declared income. In many cases, the issue is not the controls as existing on paper , but the implementation across both dimensions and the underlying coordination between them.

While the most visible trigger may be fraud or money laundering, the same mule infrastructure can also elevate wider CFT and CPF risk where funds, accounts or counterparties intersect with higher-risk networks.

Reading the typologies as fraud-AML intersections

The key typologies are best understood as joint-control indicators: they reveal a fraud symptom and a laundering symptom at the same time.

Account profile, onboarding and authentication

Account profile, onboarding and authentication controls are often the first place where fraud and AML indicators converge. Personal accounts used for quasi-business activity, turnover materially above declared income, salary accounts with no salary and beneficiary-name mismatches all matter because they may point to both the receiving end of a fraud and the beginning of a laundering chain. Verification of Payee and behavioural monitoring can help identify scam proceeds entering the account, while also detecting layering activity that is inconsistent with the customer's expected profile. At onboarding, granular capture of occupation, source of funds and expected activity creates the baseline needed to identify later deviation. Biometric and liveness checks for high-risk events, supported by device analytics, reduce the risk of account takeover and third-party operation.

Multiple accounts, dormancy and network behaviour

Multiple accounts, dormant accounts and network behaviour should not be assessed in isolation, because mule activity is often deliberately fragmented. Unjustified multiple or multi-currency accounts, dormant accounts returning to life and digitally recruited mule networks require more than single-account monitoring. Linking accounts by device, IP address, phone number, email address, physical address and counterparty can reveal fragmentation, shared control and organised recruitment that would otherwise be missed. Fraud device intelligence and AML link analysis should therefore feed one consolidated network view.

Cash-out, source of funds and virtual assets

Cash-out behaviour, source-of-funds weaknesses and virtual-asset movement show the laundering function of the mule account in practice. Rapid ATM withdrawals, structured cash deposits, unexplained high-value purchases, shell entities with high in-and-out flows and rapid fiat movement to or from virtual-asset platforms may represent extraction, layering and integration in action. Velocity monitoring, risk-based limits, adequate surveillance retention, stronger source-of-funds enquiry and enhanced due diligence for businesses without genuine operations give both fraud and AML teams the evidence needed to intervene, escalate or exit.

The cross-cutting requirement

The cross-cutting requirement is the ability to combine behavioural and network analytics across every typology. Behavioural analytics identify activity that is inconsistent with the declared customer profile, including pass-through flows, salary mismatches, dormant-account spikes and unusual early-life activity. Network analytics map relationships that account-by-account monitoring cannot see. When both are fed by fraud alerts, recall notices and law-enforcement feedback, the bank can move from closing individual accounts to disrupting the network behind them.

The regulatory expectation is therefore not just to recognise the typologies, but to test whether current controls are aligned to them. Institutions should be able to evidence how expected activity is captured, how actual activity is compared against that baseline, how documentation expiry and event-driven review triggers are managed, and how identified weaknesses translate into timely remediation.

Five considerations for assessing an AML programmes against money-mule risk

1. Governance across the fraud-AML seam.

Is there a single accountable owner, or a formal joint forum, with a clear mandate across fraud and AML? Fragmented ownership is a common cause of control failure. Someone must own the complete risk: escalation, decisions, remediation and outcomes.

2. Intelligence sharing and feedback loops

Do confirmed frauds, recall requests, indemnity notices and law-enforcement feedback flow promptly into transaction-monitoring tuning, investigations and customer risk re-rating? Intelligence trapped in one team is a lost detection opportunity.

4. Mule-specific detection and intervention

Have key typologies such as rapid pass-through, salary-account inconsistency, early-life spikes, dormant reactivation, structured cash-in and cash-out, and rapid movement to virtual assets been translated into live scenarios, thresholds and intervention rules? Are scenario logic, calibration decisions, threshold changes and feedback loops documented and reviewed? Coverage on paper is not coverage in production.

3. Behavioural and network analytics

Can the bank identify material deviations from expected activity and link accounts through devices, IP addresses, contact details, addresses, employers and counterparties? Mule activity is rarely visible through a static customer risk rating or a single-account lens.

5. Effectiveness and consequence management

Does assurance test whether controls fire on known mule patterns through above- and below-the-line sampling, alert conversion analysis and case review? Once activity is detected, are risk ratings, enhanced monitoring, restrictions, reporting and exit decisions applied consistently? Are post-STR/SAR controls formalised, including customer risk re-rating, time-bound enhanced monitoring and clear consequence management? Detection without action leaves the network intact.

The bottom line

Money mules are neither an AML problem with a fraud flavour, nor a fraud problem with an AML tail - they prove that the two disciplines are different facets of the same threat. Banks that keep the walls up will continue closing individual accounts while networks recruit replacements. Banks that share intelligence, unify analytics and test whether controls work can disrupt the scheme rather than chase the symptom. The choice, and the residual risk that follows, sits squarely with the board.

How Grant Thornton can help

Grant Thornton UAE can help financial institutions strengthen their resilience against money mule risk through an integrated fraud, AML and financial crime framework. Our specialists assess fraud and financial crime can help assess and enhance governance, controls, data, analytics and operating effectiveness across the fraud-AML lifecycle to enhance risk management. We support clients in implementing mule-specific detection scenarios, strengthening intelligence sharing, leveraging advanced behavioural and network analytics, and conducting independent effectiveness reviews to ensure controls not only detect suspicious activity but also drive timely intervention, regulatory compliance and sustainable risk reduction. The result is a more connected, intelligence-led AML programme capable of identifying, disrupting and preventing mule networks before they facilitate broader financial crime.

Aakash Bassi

Partner
Risk & Regulatory Advisory
(Forensics & Restructuring)

T +971 4 388 9925
E aakash.bassi@ae.gt.com

Alexandra Will

Partner
Risk & Regulatory Advisory
(Financial Crime Compliance)

T +971 4 388 9925
E alexandra.will@ae.gt.com

Zarik Nawaz

Director
Risk & Regulatory Advisory
(Financial Crime Compliance)

T +971 4 388 9925
E zarik.nawaz@ae.gt.com

Grant Thornton UAE offices

Abu Dhabi

Unit 2, Level 14
Sila Tower
ADGM Square
Al Maryah Island
PO Box 41255
Abu Dhabi, UAE

T +971 2 666 9750
F +971 2 666 9816

Dubai

The Offices 5
Level 3
Office 303
One Central, DWTC
PO Box 1620
Dubai, UAE

T +971 4 388 9925
F +971 4 388 9915

Sharjah

Level 5
City Gate Tower
Al Etihad Street
Al Taawun
PO Box 1968
Sharjah, UAE

T +971 6 525 9691
F +971 6 525 9690

Follow us on LinkedIn