Money Mule Accounts and Account Leasing: The Hidden Infrastructure Enabling Financial Crime

Executive Summary

Money mule accounts and account-leasing arrangements have evolved from peripheral fraud concerns into the critical financial infrastructure of modern organized crime. These accounts serve as the bridge between victim deception and criminal monetization, allowing illicit proceeds from scams, cyber-theft, and business email compromise (BEC) to be fragmented and extracted.Key takeaways for financial crime (FinCrime) professionals include:

- **Infrastructure as a Service:** Criminal networks now utilize "money-laundering-as-a-service," where "mule herders" recruit, test, and manage large fleets of accounts, treating them as expendable assets.
- **The Rise of Account Leasing:** Genuine customers are increasingly permitting third parties to use their accounts—voluntarily, via deception, or through coercion—effectively making criminal activity resemble legitimate customer behavior.
- **Detection Challenges:** The "cold-start" problem of new accounts and the speed of digital payments create significant blind spots for institutions.
- **A Shift in Strategy:** Effective disruption requires moving beyond simple account closures. Institutions must adopt a "lifecycle intelligence" approach that combines network analytics, behavioral biometrics, and cross-institution data sharing to dismantle the underlying criminal operating models.

The Mechanics of Mule Accounts and Account Leasing

Money mule accounts provide the necessary logistics for converting victim payments into movable criminal proceeds. Without these receiving accounts, even sophisticated fraud operations cannot monetize their activities at scale.

Defining Account Leasing

Account leasing describes arrangements where a legitimate customer allows another party to use their bank account in exchange for payment, inducements, or under duress. This access can range from:

- **Transaction Facilitation:** The customer receives a transfer and sends it onward.
- **Total Relinquishment:** The customer surrenders online banking credentials, physical cards, security tokens, and one-time passwords (OTPs).
- **Operational Windows:** Accounts are sometimes used for a very short duration to process funds rapidly and complicate detection efforts.

The Recruitment Population

Mule networks do not consist of a single type of offender. Recruitment targets diverse groups through social media, job advertisements, and romance scams:

- **Deliberate Facilitators:** Individuals knowingly renting their accounts for commission.

- **Exploited Individuals:** Students, migrants, and the financially vulnerable who are targeted with language like "rent your account" or "receive a business payment."
- **Deceived Victims:** People manipulated through romance fraud or fake employment opportunities who believe they are performing a legitimate service.

Industrialization of the Mule Model

Criminal actors have moved from ad-hoc recruitment to industrial-scale operations that separate the predicate offender from the financial transaction.| Feature | Description || ------ | ------ || **Mule Herders** | Specialized service providers who recruit account holders, coordinate access, and replace blocked accounts. || **Corporate Mule Accounts** | A shift toward using business accounts for BEC and investment fraud to provide a façade of legitimacy that matches the scam pretext. || **Laundering-as-a-Service** | Organized networks that offer mule-based transfer and withdrawal services for a percentage of the proceeds. || **Layering Tactics** | Use of "chains" of accounts across multiple institutions, splitting and recombining funds through ATMs, remittance firms, and virtual assets. |

Strategic Challenges to Detection

Several factors allow mule infrastructure to scale efficiently while evading standard banking controls:

1. **Replacement Economics:** Mule accounts are treated as expendable. Criminal groups only need an account to survive long enough to disperse funds; if one is blocked, the next payment is simply redirected to a new account.
2. **The "Cold-Start" Problem:** Behavioral models struggle with new accounts because there is no baseline of "normal" activity. High-velocity pass-through activity can occur before the bank has established a profile for the customer.
3. **Authentic Onboarding:** Many mules pass initial Know Your Customer (KYC) checks using genuine identity documents. The risk only emerges later when control is transferred to a criminal network.
4. **Institutional Fragmentation:** Detection is hampered when the sending bank, receiving bank, and downstream institutions do not share information. The UK FCA noted that firms often fail to respond to alerts involving later-generation recipients of funds.

Statistical Scale (UK Context)

- **UK FCA Reporting:** 25 firms offboarded 194,084 money mules between January 2022 and September 2023.
- **Cifas Data:** Recorded over 106,000 "misuse-of-facility" cases in 2025.
- **Intelligence Gaps:** Only 37% of offboarded mules were reported to the National Fraud Database during the FCA's study period.

The Resilient Control Stack

To combat account leasing, financial institutions must move from static rules to a multi-layered, risk-sensitive approach throughout the account lifecycle.

1. Risk-Sensitive Onboarding

Incorporate device profiling, geolocation, and behavioral biometrics. The goal is to determine if the relationship is plausible based on the customer's stated occupation, income, and business purpose.

2. Early-Life and Inbound Monitoring

New or materially changed accounts require intensified monitoring. Critical patterns include:

- Unexpected credits from unrelated parties.
- Deposits exceeding stated turnover.
- Immediate dispersal of funds and near-total balance depletion.
- Rapid creation of new beneficiaries.

3. Control-of-Account Analysis

Firms must reconstruct the sequence of events. A combination of a phone number change, a new device registration, and a password reset followed by sudden pass-through activity is a high-risk indicator of a transferred account.

4. Network and Graph Analytics

Treating accounts as nodes in a system rather than isolated cases allows firms to:

- Trace later-generation beneficiaries.
- Identify shared devices or contact points across unrelated customers.
- Expose "fan-out" payment patterns used by herders.

5. Rapid and Proportionate Response

Speed is essential as proceeds dissipate within minutes. Institutions need playbooks that balance the need to freeze funds with the reality that some mules are coerced or manipulated victims who require safeguarding.

Conclusion: Lifecycle Intelligence

The right way to approach the money mule threat is as a connected enterprise risk involving fraud, AML, digital identity, and customer vulnerability. Strong KYC at account opening is no longer sufficient; the decisive capability is **lifecycle intelligence** .By focusing on who controls an account and how that account connects to wider networks, financial institutions can move beyond processing alerts and begin attacking the profitability of the organized crime groups that rely on this hidden infrastructure.