



Stop the Money Before It Reaches the Mule



SUMMARY

Financial institutions should remain alert to a fraud pattern in which **fraudsters establish new accounts that are later used as mule accounts**, while separately obtaining or compromising legitimate accountholders' online banking credentials.

Receiving accounts may be a newly established mule account within the institution. Monitoring only the compromised account may therefore miss the other side of the fraud.

Connecting these two seemingly unrelated events can create an opportunity to identify and stop the loss before funds leave the institution.

HOW THE SCHEME WORKS

A typical scheme may involve several stages:

- **Mule account is established** – A fraudster uses stolen, synthetic, or fabricated identity information to open a new account.

- **Account builds a low-risk history** – The account may have normal-looking activity initially, allowing it to avoid immediate detection.
- **Victim credentials are compromised** – Fraudsters obtain online banking usernames, passwords, authentication codes, or other credentials through phishing, social engineering, malware, or telephone scams.
- **Fraudster accesses the victim's account** – The compromised credentials are used to initiate transfers.
- **Funds are transferred to the mule account** – The fraudulent new account receives the stolen funds.
- **Funds are rapidly moved or withdrawn** – The mule may transfer funds to another institution, withdraw cash, purchase cryptocurrency, or otherwise move the money before the financial institution can intervene.

RECOMMENDED MITIGATION STEPS

- **Strengthen New Account Monitoring** - Establish enhanced monitoring for newly opened accounts, particularly during the first 30–90 days. A key pattern to watch for is a large inbound transfer followed quickly by outbound movement of funds, cash withdrawals, or cryptocurrency purchases.
- **Monitor First-Time Transfer Destinations** - Apply additional scrutiny when a member initiates a significant transfer to a recipient or account that has never previously received funds.
- **Use Risk-Based Transaction Holds or Delays** - Consider risk-based delays, verification, or additional authentication for unusual transfers, particularly when multiple account takeover indicators are present.
- **Monitor Credential Changes** - Treat password resets, device enrollment, MFA changes, and changes to contact information as potential risk events, particularly when followed by transfers.
- **Connect Device and Session Data Across Accounts** - The same device, IP address, or browser fingerprint appearing on both a newly opened account and a session in an existing accountholder's account can be a strong indicator of coordinated fraud. Institutions may want to assess whether their monitoring can link these signals across accounts.
- **Link Fraud Intelligence** - Ensure information concerning suspicious new accounts is available to fraud, BSA/AML, and operations teams as appropriate. A new account identified as potentially fraudulent should receive heightened monitoring.
- **Restrict Account-to-Account Transfers** - Prohibiting or limiting transfers to unrelated third-party accounts can reduce the risk that compromised online banking credentials are used to move stolen funds into mule accounts. If third-party transfers are permitted, institutions should consider enhanced authentication, transaction limits, and risk-based monitoring before allowing the transfer.
- **Educate Members** - Remind members that the financial institution will never ask them to provide passwords, MFA codes, or security codes to "protect" their funds and that they should not move money at the

direction of someone claiming to be from the financial institution, law enforcement, a government agency, or a fraud department

KEY FRAUD PREVENTION MESSAGE

Mule-account fraud and account takeover are best viewed as connected risks rather than separate ones.

Fraudsters can establish a mule account days or weeks before compromising another accountholder's online banking credentials and transferring stolen funds into that account.

Financial institutions should therefore ask:

"Does our fraud monitoring identify suspicious activity in both the compromised sending account AND the newly opened receiving account?"

The ability to connect new account activity, compromised credentials, unusual authentication events, and suspicious transfers may provide an important opportunity to identify and stop fraud before funds leave the institution.

RISK MITIGATION RESOURCES

- [FBI - Money Mules](#)
- [IC3 - Account Takeover Fraud](#)
- [Officer of the Inspector General - Money Mules](#)
- Visit our [Fraud Prevention Center](#) to learn best practices on protecting against risk to your institution

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.

Stay ahead of fraud threats.

Access risk alerts, expert resources, the Let's Talk Fraud webinar series, and more — all in one hub.

[Explore the Fraud Prevention Center](#)

