Money Mule Intelligence

Identify criminal-controlled bank accounts and disrupt payments to them

Challenge

Criminal activity and cyber targeting take many forms, but they are almost always financially motivated, which means threat actors need a way to cash out stolen funds without being traced. Scams, money laundering chains, account takeover schemes, and more increasingly converge on the same infrastructure: criminal-controlled accounts that receive stolen funds before they are cashed out. Regardless of the specific attack chain, the mule account is often where the money lands.

That convergence is what makes mule accounts so valuable to disrupt, and so difficult to catch. Threat actors attempt to keep regular spending patterns on these accounts so they don't register as dormant or suspicious, letting them blend in with legitimate activity until the funds are already gone.

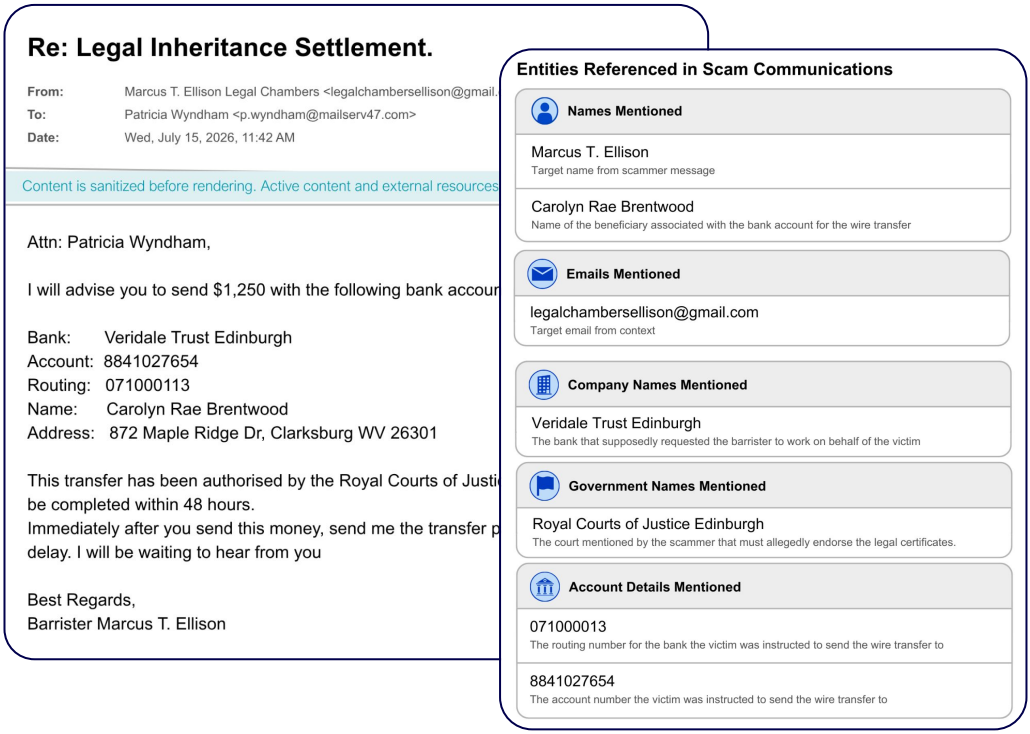
Solution

Money Mule Intelligence delivers verified data on crime-linked accounts so teams can disrupt cashout before funds are lost. This data is collected by CYBERA through direct engagement with threat actors, which means the account details come straight from the criminals themselves, while their operations are still active. That makes it more ready to act on, for both on-bank mule detection and off-bank beneficiary screening.

A single source of verified account data can support intervention across scam, laundering, and takeover scenarios alike. Teams can move with greater confidence at the moment funds are most exposed, before criminals are able to cash out.

Key Use Cases

Screen outbound payments	Verify recipients against mule account lists so payouts, refunds, and disbursements reach the intended party, not a potentially criminal-controlled account.
Catch beneficiary redirection	Flag when a payment destination is changed to a suspected mule account, a common sign of account takeover.
Detect mules in your own base	Surface suspected mule accounts among those you hold so teams can act before stolen funds move.
Strengthen investigations	Enrich reviews of suspicious transactions and activity with intelligence on compromised, abused, and fraud-associated accounts and infrastructure.



Recorded Future is the world's largest threat intelligence company. Recorded Future Intelligence Platform provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,900 businesses and government organizations across more than 80 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com