THE DANGER OF SYNTHETIC MONEY MULES

Fraudsters have an increasingly popular and successful tactic – creating synthetic identities to open accounts that are then used to receive or move illegally acquired funds. This tactic is quickly replacing the use of a "traditional" money mule.

WHAT IS A 'TRADITIONAL' MONEY MULE?

A money mule is someone who receives or moves illegally acquired funds at the direction of someone else. Some money mules know that they have been recruited to assist with criminal activity, but some do not, as they might be responding to a job posting that looks to be legitimate, for example. By receiving funds or items of value from a person they don't know and then forwarding the value on to another recipient, they may help criminals profit, run the risk of criminal charges or lose their own money. Conversely, some money mules intentionally take these risks to financially benefit from a fraud scheme.

Money mules help criminals more successfully move illegally obtained funds through the financial ecosystem, as the use of mules makes it harder to follow the trail of money and tie it back to the criminal. Money mules enable money laundering, terrorist financing and human trafficking.

SYNTHETIC IDENTITIES AND MONEY MULES

Involving more people in the web of deceit increases risk for the fraudsters. A money mule could make a wrong move and get caught, or the money mules may not transfer funds to the fraudsters. Recruiting and managing real individuals to move money on the fraudsters' behalf requires both time and costs. For these reasons and others, fraudsters increasingly use synthetic identities to "mule" the money themselves. In this case, criminals have more control over the funds transfer process, are anonymous and don't have to pay fees to real-person money mules.

Synthetic identities are created by using a combination of personally identifiable information (PII) to fabricate a person or entity. These identities are easy to create on a large scale, given the availability of stolen data on the dark web. Criminals can buy a stolen Social Security number for as little as $1 or purchase batches of stolen data for a similarly low price. Once created, these identities can be used to open deposit or investment accounts across multiple institutions.

THE DANGER OF SYNTHETIC MONEY MULES

One digital identification provider ***estimates*** that 1% to 3% of bank accounts in the U.S. were opened using synthetic identities. Based on this estimate, upwards of 2.5 million synthetic identities are hiding in U.S. bank accounts, which is an astonishing number of accounts that potentially can move illegal funds. Historically, synthetic identities were used to build up credit lines, max out the credit line, and then "bust out," or disappear without paying. The newer trend of using synthetics to create mule accounts introduces additional risk to financial institution portfolios, as there is no actual person to pursue for payment when fraud occurs.

PREVENTION IS KEY

Prevention continues to be the best defense for your portfolio against synthetic identities. Onboarding controls continue to be your best defense against having synthetics in your portfolio. However, if these identities are used to open accounts, the ongoing monitoring process becomes even more crucial. Monitoring accounts throughout the relationship and performing routine validation of the account holder, transactions and account activity can help identify a synthetic. Financial institutions that have deployed tools to detect synthetic identities in the onboarding process and during the account lifecycle may benefit by using a combination of approaches, such as document validation, behavioral analysis, alternative data, biometrics and selfie verification.