Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

Money Mule & Recruitment Fraud

SUMMARY

Money mules are individuals recruited to open accounts at your financial institution or use an existing account. These recruits are found in various ways such as employment ads, social media posts, romance scams, unhoused individuals, college campuses, at festivals, and other well-populated events. Once identified, these recruits are instructed to use an existing account or open accounts online or in-person at a branch, then use various methods to transfer or withdraw funds.

Financial institutions should remain cautious when opening new accounts due to the increase in this type of fraud.

WHAT IS A MONEY MULE?

A money mule is someone who – at another individual's direction – receives and moves illegally obtained funds, usually receiving a benefit for it. Upon receiving the funds, the money mule withdraws the funds through various means, including in-person withdrawals at a branch, ATM/ITM, POS (usually to purchase gift cards), cash app, online banking, ACH, debit card, and at casinos.

Some individuals unknowingly become money mules after being told they have won a sweepstakes or upon engaging in an online relationship. Although the stories money mules are told vary by scheme, fraudsters will ask that the person receive money from people they do not know and then forward the money on.

Money mule operations can be established at a small scale, with criminals recruiting mules themselves. Large scale money mule operations usually involve money mule recruiters, sometimes also referred to as "mule herders" and "pickers".

MONEY MULE RECRUITMENT FRAUD IN ACTION

Recently, a group of money mule recruiters targeted individuals attending a festival in Michigan, giving the recruits U.S. Treasury checks. The scheme was for the recruit to deposit the check into their existing account at their financial institution in exchange for a free cell phone. The US Treasury checks were fraudulent and multiple Michigan credit unions suffered significant losses as a result. It's worth noting that the US Treasury has an 18-month reclamation period.

At the same time, money mule recruiters were recruiting individuals to open new

accounts, adding online banking and a debit card. The recruit was instructed to perform an account-to-account ACH debit (pulling funds into the new account from another financial institution). Once the funds were deposited, the recruit was advised to use the newly issued debit card tied to a cash app to transfer funds to the recruiter less an agreed upon percentage for their efforts. The funds obtained via ACH debit were stolen from accounts at other financial institutions. As a result, the ODFI (Originating Depository Financial Institution) suffers the loss.

RISK MITIGATION STEPS

- Financial institutions should remain cautious when opening new accounts due to the increase in this type of scheme (review the *Significant Uptick in New Account Fraud* risk alert). Behavioral indicators are crucial to identify potential money mules, as they often exhibit unusual transaction patterns that involve frequent, large deposits and immediate withdrawals or transfers.
- Use common sense and reasoning. Does it make sense that the person or business is opening an account at your financial institution? Are they depositing a large check or government check (review the *Beware of Fraudulent United States Treasury Check Deposits* risk alert). Is the business a new business? Is the accountholder local to a branch? The US Treasury has a year and six-month reclamation period.
- Use a name matching solution if you allow accountholders to perform ACH debits and implement dollar limits. The ODFI suffers the loss. Note: the financial institution where the money is withdrawn from has 60 days to recall the funds.
- Financial Institutions can use machine learning link analysis tools to identify money mules by connecting large amounts of data and looking for patterns of behavior. These tools can examine devices, IP addresses, and emails to see if there are links to other accounts at your financial institution.
- Consider limiting access to online banking and debit cards to all new members.
- Carefully review account histories, especially for large checks deposited.

RISK MITIGATION RESOURCES

- Check out Allied's Risk Resource Library.
- Review the *Significant Uptick in New Account Fraud* risk alert.
- Review the *Beware of Fraudulent United States Treasury Check Deposits* risk alert.

The information presented in this document 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 document.

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.