Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

December 03, 2021

Alert Number
I-120321-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Money Mules: A Financial Crisis

WHAT IS A MONEY MULE?

Any individual who transfers funds, on behalf of, or at the direction of another. Money mules are recruited to assist criminals with laundering proceeds from illegal activity and are often promised easy money for their participation in moving funds by various methods including:

- Cryptocurrency
- Physical currency (cash)
- Bank transfers (wires, ACH, EFT)
- Money services businesses
- Pre-paid cards

WAYS MONEY MULES ARE RECRUITED

- Unsolicited emails or other communications requesting to open a bank account, cryptocurrency wallet, or business in their name
- Romance/confidence scams
- Employment scams promising easy money
- Non-payment/non-delivery scams
- Lottery scams where personal information is collected

Money Mule: COMPLICITY

Unwitting or unknowing mules: not aware that they are involved in a bigger criminal scheme. These individuals are typically recruited via scams such as romance scams or more recently, employment scams due to the COVID-19 pandemic. Generally, these individuals genuinely believe they are helping someone who is acting as their romantic partner or employer.

Witting mules: ignore warning signs of criminal activity or are willfully blind to the financial activity they are participating in. They may have received warnings from bank personnel but continue to open multiple accounts. These individuals generally begin as an unwitting mule.

Complicit mules: aware of their role as a money mule and complicit in the larger criminal scheme. They might regularly open bank accounts at various institutions with the intention of receiving illicit funds or openly advertise their services as a money mule and actively recruit others.

WHO IS AT RISK?

Anyone can be recruited to be a money mule; however, targeted populations include the elderly, college-aged students, and newly immigrated individuals. Cyber-expertise or knowledge is not required

the money mule will be directed how to open accounts and process various transactions.

RECENT TRENDS

In 2020 into 2021, the IC3 received an increase in complaints relating to COVID-19 related fraud and online scams involving cryptocurrency, such as business email compromises, extortion, employment scams and confidence/romance scams. The increases in these scams could be the result of isolation due to COVID-19 quarantine restrictions, the loss of employment due the COVID-19, and increases in remote work which allowed criminals to instruct money mules to provide copies of their personal information online.

Money mules were also asked to provide copies of their personal information or to directly open cryptocurrency accounts and wallets as part of online scams such as romance fraud, extortion, non-payment/non-delivery, or investment scams. These accounts opened in the money mule's name could then be later used in other scams to target victims of business email compromises, tech support, and other online scams.

CONSEQUENCES FOR ACTING AS A MONEY MULE

Individuals acting as money mules are putting themselves at risk for identity theft, personal liability, negative impacts on credit scores, and the inability to open bank accounts in the future. Furthermore, they and their families could be threatened by criminals with violence if they do not continue to work as a money mule.

In addition, these individuals face prison sentences, a fine or community service, even if unwitting. Particularly in the United States, potential Federal charges include: Mail Fraud, Wire Fraud, Bank Fraud, Money Laundering, Transactional Money Laundering, Prohibition of Unlicensed Money Transmitting Business, and Aggravated Identity Theft. These charges come with fines reaching $1,000,000 and up to 30 years in prison.

TIPS FOR PROTECTION

If you believe you are being used as a money mule:

- STOP communicating with the suspected criminal
- STOP transferring funds or items of value
- Maintain receipts, contact information, and communications (emails, text messages, voicemails) so the information may be passed to law enforcement
- Notify your bank or payment provider
- Notify Law Enforcement. Report suspicious activity to the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov and contact your local FBI field office

Federal Bureau of Investigation
Public Service Announcement

To prevent yourself from being recruited as a money mule:

- Do not accept job offers that ask you to receive company funds into your personal account or ask you to open a business bank account
- Be suspicious if a romantic partner asks you to receive or transfer funds from your account
- Do not provide your financial details to anyone (e.g., bank account information, logins, passwords)
- Do not provide copies of your identification documents to anyone (e.g., driver's license, social security number)
- Conduct online searches to corroborate any information provided to you
- Reach out to your financial institution with banking questions or concerns about financial transactions in your account

For additional information on Money Mules, please view:

FBI Scams and Safety: Don't Be a Mule: Awareness Can Prevent Crime
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules

For additional information on internet-enabled crime, please visit:

https://www.fbi.gov
https://www.ic3.gov
https://www.justice.gov/topics