Public Service Alert: Money Mules

The FDIC OIG is warning the public about criminals utilizing "money mules" to commit and facilitate fraud and other illicit activity through the United States financial system. Money Mules can be criminally prosecuted and held financially accountable for victims' losses. Avoid becoming a Money Mule!

What is a Money Mule?

Criminal organizations routinely use "money mules" to move proceeds of fraud, scams, and other illicit activity through the U.S. financial system. A money mule is any person who transfers or receives funds at the direction of another, knowing—or being unaware—that the money is tied to criminal activity. This includes individuals moving funds electronically as well as couriers sent to pick up cash, precious metals, or other assets directly from victims of fraud schemes, a tactic increasingly used in scams targeting the elderly.

Money mule networks enable billions of dollars in losses each year across the United States.[1] The victims whose funds flow through mule accounts are frequently older adults targeted through romance scams, "pig butchering" cryptocurrency schemes, tech support fraud, and government or bank employee impersonation schemes, including FDIC and FDIC-OIG impersonation schemes.[2]

How it Works:

Fraudsters typically utilize money mules in multiple ways:

- **Victim to Mule Transfers:** Criminals convince victims—often elderly, college students, or financially vulnerable individuals—to send money under false pretenses. The funds are directed to mule accounts rather than directly to the criminals to obscure identities. In some schemes, criminals dispatch couriers to physically retrieve cash, gold, or other valuables from victims, sometimes posing as law enforcement or bank officials.
- **Recruitment of Mules:** Criminals recruit money mules intentionally (witting) or through deception (unwitting). Recruitment commonly targets job seekers by

offering convenient remote work opportunities, often as a rebates or payments processor.[3] Criminals often target students, those looking for work, those on dating websites, the elderly, and individuals experiencing financial hardship, but anyone can be approached to be a money mule.[4]

Once a mule receives the funds – or collects physical assets – the individual is instructed to withdraw cash, buy cryptocurrency, purchase gift cards, transfer funds through additional accounts, or send money overseas. These layering transactions conceal the illicit origin of the funds.

Red Flags

Common indicators of money mule activity—both for potential scam victims and for people being recruited—include:

- Being asked to use a personal bank account to receive or move money for someone you have never met in person.
- Job postings involving "payment processing" or "funds transfer" work, especially if they require using your own bank account or opening a bank account specifically for the funds transfer processing.
- Unsolicited messages from strangers – potential romantic partners, investment advisers, or purported government officials – directing you to handle funds.
- Pressure to act quickly, secrecy about the reason for the transaction, or inconsistent explanations.
- Funds arriving from multiple unrelated individuals (often older adults), followed by rapid outgoing transfers.
- Requests to convert funds to cryptocurrency, gift cards, wire transfers, or cash withdrawals.
- Being told to hand over cash, gold, or other valuables to a courier sent to your home, especially when the caller claims to be a government or bank employee.

What Happens if You Participate as a Money Mule

- Prosecution for participating in illegal money-movement activity.
- Personal liability for repaying victims' losses.
- Exposure of personal information that criminals may later misuse.
- Inaccessible bank accounts and potential long-term credit impacts.

Protect Yourself

Individuals can reduce their risk of becoming victims or unwitting participants in a money mule scheme by taking the following steps:

- Never use your personal bank account to receive funds for someone you do not know and trust. Legitimate employers do not require this type of activity.
- Be cautious of unsolicited job offers or online opportunities promising easy money, especially those requiring minimal skills or personal information.
- Verify the identity of anyone requesting financial help or investment activity. Scammers frequently impersonate government agencies, bank employees, and law enforcement.
- Talk to family members – especially older relatives – about romance scams, cryptocurrency investment fraud, and government impersonation schemes.
- Review the available free and online FDIC "Money Smart" resources to learn how to avoid and report identity theft, frauds, and scams.
- Report suspicious activity immediately to your bank and to law enforcement. Early reporting helps limit financial loss and may prevent the use of your account in further criminal activity.
- If you believe you have been recruited as a money mule, stop all transactions at once. Do not send or return funds. Contact your bank and report the incident to the FBI's Internet Crime Complaint Center, the FTC, and the FDIC OIG Hotline.

Additional Resources:

- FTC Money Mule Consumer Alert
- FDIC Money Smart
- United States Computer Emergency Readiness Team
- FBI Money Mule Public Service Announcement

Red Flags for Financial Institutions:

- Unexpected changes in customer account behavior, including large deposits followed by rapid transfers or withdrawal of funds, including out of state or international transactions.

- Use of synthetic, stolen or fictitious identities to open bank accounts, followed by the deposit and immediate funds withdrawal of large checks, which are returned as fraudulent or non-sufficient funds.
- Deposits from multiple seemingly unrelated parties into an individual's account followed by the rapid conversion of funds to cryptocurrency or prepaid cards.

---

[1] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[2] https://www.fdicoig.gov/sites/default/files/document/2022-08/oigimpersonationscamflyer.pdf

[3] https://www.ic3.gov/PSA/2010/WorkAtHome.pdf

[4] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules