



Customer Advisory: Beware Offers to Receive and Forward Money

The Commodity Futures Trading Commission advises the public that criminals may try to recruit people to accept fund transfers into their digital wallets, trading accounts, or other financial accounts, and then forward the funds on to someone else, sometimes offering a percentage of the money moved as payment. This financial shell game is a form of money laundering and it's against the law.

The criminals call them “money mules” — people who, at someone else’s direction, receive and move money obtained through fraud or other crimes. Some money mules know they are assisting criminal activity, while others may not. Moving money for illegal activities can lead to serious consequences, including civil and criminal charges.

Wedded to Romance Scams

The rapid growth of romance scams, as well as other frauds involving crypto-asset and over-the-counter foreign currency trading means the criminals must find more ways to launder the funds, and get so-called cleaned money into their accounts. Moving the money through many legitimate accounts opened by people with no criminal past makes it more difficult for law enforcement to trace.

Romance frauds have caused a significant increase in complaints to the CFTC and other federal agencies in recent years. In 2022, romance fraud losses reported to law enforcement and other federal agencies were at least \$1.3 billion, matching losses in 2021, but nearly twice the amount reported in 2020.¹ Actual losses are likely much higher because many frauds go unreported.

Unwitting money mules may also be victims of crime themselves. Romance fraud victims are sometimes convinced to share account or digital wallet information with criminals, who then transfer funds into or out of the accounts. Other times, victims are told they need to assist with a pressing business matter, respond to some sort of emergency, help with a personal crisis that could harm their relationship, or

How to Recognize and Avoid Romance Scams

Romance fraud commonly begins with a contact through a dating app, a new friend on social media, or a random “wrong number” text or instant message. The fraudsters begin texting regularly and talk about their wealth, high-profile jobs, charity work, and success trading crypto assets or over-the-counter foreign currency or gold contracts. Conversations may extend to phone calls or video chats, but never face-to-face. Eventually, the criminals convince victims they are in lasting relationships, and offer to help them make money trading.

The victims are instructed to convert their money to crypto assets and move the funds to an unregistered, offshore trading platform. Fake trading returns, rapidly growing balances, and pressure from the fraudsters encourage victims to invest more and more. But when the victims ask for withdrawals, they are refused.

Remember:

- **Don't** give money to people you meet and only know online.
- **Do** restrict conversations to social platforms or dating apps.
- **Don't** chat with strangers who randomly contact you.
- **Do** check to see if trading platforms have U.S. offices and are registered with the Financial Crimes Enforcement Network ([FinCen](#)).
- **Don't** trade in markets you don't fully understand or with money you can't afford to lose.

To learn more, visit go.usa.gov/xtfYA

¹ These figures are based on reports to the Federal Trade Commission's Consumer Sentinel Network and the FBI's Internet Crimes Complaint Center (IC3). Losses reported to the CFTC are not publicly reported.



given other reasons to accept and conduct the transfers.

Students and Job Seekers Also Targeted

Money mule activities extend beyond romance scams though. Students or job seekers looking to earn extra money are also targeted. The jobs are advertised through social media posts or online job boards and are often poorly defined — entailing little more than opening accounts, sending or receiving packages, and moving money. Other warning signs include:

- Unsolicited email or social media messages that promise easy money for little or no work.
- The “employer” uses web-based email services (such as Gmail, Yahoo, Hotmail, Outlook, etc.).
- Employees are asked to open personal bank accounts or create companies and open business accounts to receive and transfer money.
- Employees are asked to receive funds in their bank accounts and then “process” or “transfer” funds via wire transfers, ACH, mail, or other means.
- Employees receive packages containing cash.
- Funds are sent to the employees’ digital wallets and they are asked to convert crypto assets to cash and transfer it to others.
- Employees are allowed to keep a portion of the money they transfer.

Protecting Yourself and Your Community

According to the Department of Justice and the International Criminal Police Organization (INTERPOL), money mule recruiters have also been connected to international crime organizations, and the illegal funds could come from a number of criminal activities, including malware, ransomware, other swindles targeting businesses, and theft of government funds earmarked for pandemic relief. Remember:

- Never agree to move money for someone you have never met face-to-face.
- If you are approached online and asked to move money, immediately stop communicating with the person.
- If you have already received money or crypto assets from a person you met online, do not send it onward to anyone. Instead, notify your financial institution and consider changing accounts, especially if you have provided any personally sensitive information about yourself, bank or crypto-asset trading accounts.
- Immediately notify the FBI’s Internet Crime Complaint Center (IC3) at [ic3.gov](https://www.ic3.gov), and contact your **local FBI field office**.

What the CFTC is Doing to Protect the Public

The CFTC joined the 2023 Money Mule Initiative, an annual international effort to disrupt money mule networks. During the three-month initiative, participating agencies took more than 4,000 actions against suspected money mules. Together with other law enforcement agencies and as part of its ongoing mission to promote the integrity of U.S. derivatives markets, the CFTC will continue to take steps to identify and address money mule activity related to derivatives markets and disrupt fraud schemes that target customers.

This advisory was prepared by the Commodity Futures Trading Commission’s Office of Customer Education and Outreach. It is provided for general informational purposes only and does not provide legal or investment advice to any individual or entity. Please consult with your own legal advisor before taking any action based on this information. The CFTC cannot attest to the accuracy of information contained in any non-CFTC references or websites. Reference in this advisory to any organizations or the use of any organization, trade, firm, or corporation name is for informational purposes only and does not constitute endorsement, recommendation, or favoring by the CFTC.