M

Money Mule Scams: Warning Signs and What to Do

A money mule receives and transfers funds for criminals, sometimes without understanding the scheme. Recruitment often uses fake jobs, romance, or easy profit.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How money mule recruitment works
02 Common money mule stories
03 Warning signs
04 Why it is dangerous
05 What to do if you were recruited
06 How to verify a job or request
07 Source

Quick answer: A money mule is a person who receives, transfers, converts, or withdraws money for criminals. Some participants know the purpose; others are recruited through fake jobs, romance scams, investment schemes, or promises of easy commission. Do not

move the funds onward. Stop contact, preserve evidence, notify the bank, and report the scheme.

01 How money mule recruitment works

Criminals need accounts that separate stolen money from the original fraud and make recovery harder. They recruit people to receive payments into personal or newly created business accounts, keep a percentage, and forward the rest through wire transfer, payment app, cash, gift cards, cryptocurrency, or parcels.

The incoming money may come from account takeover, business email compromise, romance fraud, card theft, benefit fraud, or another victim. A transfer appearing successfully in an account does not make the funds legitimate or final. Banks can reverse fraudulent payments, freeze accounts, or investigate the recipient.

02 Common money mule stories

- **Fake remote job:** “payment processor,” “financial agent,” or “local representative” uses the employee’s personal account.
- **Romance or friendship:** an online contact asks the victim to receive money or packages because of travel, military service, banking problems, or an emergency.
- **Overpayment:** a check or transfer exceeds the purchase price and the recipient is told to refund the difference.
- **Investment or crypto opportunity:** the victim moves funds between accounts or wallets for guaranteed profit.
- **Student recruitment:** social media promises quick commission for lending a bank account, card, phone, or identity.

03 Warning signs

The FBI warns against unsolicited offers promising easy money, employers using ordinary webmail, vague duties, instructions to open an account, and requests to transfer company funds through a personal account. Other signs include pressure to act quickly or secretly, communication only through encrypted messaging, receiving money from unrelated names, splitting transfers, withdrawing cash, or converting funds to cryptocurrency.

A contract, business registration, professional-looking website, or copy of someone's identity does not prove the operation is legitimate. Those materials can be fabricated or stolen.

04 Why it is dangerous

Moving criminal proceeds can expose a person to account closure, debt after reversals, loss of money, identity theft, civil claims, and criminal investigation. Laws and legal outcomes vary by jurisdiction and knowledge, so anyone involved should obtain advice from a qualified local professional. Ignoring the problem or sending one final transfer can increase the harm.

05 What to do if you were recruited

1. Do not accept, withdraw, convert, spend, return, or forward additional money. Do not follow the recruiter's instructions for "fixing" it.
2. Contact the bank or payment provider through its official fraud channel. Explain that you may have been recruited as a money mule and follow its instructions for handling funds.
3. Preserve messages, email headers, usernames, phone numbers, job advertisements, transaction records, wallet addresses, receipts, and dates.
4. Stop contact and do not warn or negotiate with the recruiter after the bank or law enforcement advises you how to proceed.
5. Report to appropriate local law enforcement or national fraud-reporting service. In the United States, the FBI directs victims to local police or the FBI.

6. Secure exposed accounts and identity documents. Change passwords, revoke sessions, enable MFA, and monitor credit or financial records where appropriate.

06 How to verify a job or request

Contact the company through independently found details and confirm the person and role. Search official registries and the exact domain, but remember registration alone is not approval. A legitimate employer does not need an employee's personal bank account to transfer company or customer money. Never provide online-banking credentials, one-time codes, a payment card, or remote access.

07 Source

Recruitment signs and reporting guidance are based on the FBI's money muling warning and Europol's online financial scam guidance.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com