Investment, Cryptocurrency & Wealth Scams

Responding to Scams for Growing Wealth

These scams occur when criminals deceive you into sending money or assets under the promise of profits, insider access, or protection of wealth. They frequently exploit trust, urgency, and technical jargon, especially around cryptocurrency and "exclusive" investment opportunities.

This guide applies to:

- Investment scams (stocks, bonds, commodities, real estate)
- Virtual currency / cryptocurrency scams
- Romance scams involving "investments"
- AI-generated investment pitches (deepfakes, fake endorsements)
- If money or assets were already sent, act quickly. Quick action can improve recovery options.

Investment Scam – Do This First

Stop All Payments Immediately

- Do not send more money
- Do not "top up" to unlock profits
- Do not pay fees or taxes to withdraw funds. Fake tax or fee payments to unlock withdrawals are a common scam tactic.
- Do not follow new instructions from the scammer

Any request to send more money to recover losses is a red flag.

Secure Financial Access (From a Safe Device)

- Use SEC complaint resources and CFTC/NFA reporting where investment, commodity, forex, derivatives, or crypto-asset investment fraud is involved.
- Contact your bank, card issuer, or payment app immediately
    - Report the transaction as fraud
    - Ask about:
        - Reversals or recalls (if time allows)
    - Freezing linked accounts
- Change passwords for:
    - Email (often the gateway)
    - Financial accounts
    - Crypto exchanges or wallets
- Remove unknown devices or app connections
- Request case or reference numbers.

- No legitimate recovery helper can guarantee return of crypto or require upfront fees.

Preserve Evidence

Before deleting messages or closing apps:

- Screenshot or save:
  - Investment pitches and ads
  - Chat messages, emails, and profiles
  - Wallet addresses and transaction IDs
  - Websites, apps, and URLs
- Record:
  - Dates and times
  - Amounts sent
  - Platforms and payment methods used
- Documentation is critical for reporting and potential recovery.

Common Scam Types & What to Do

Investment Scams (Traditional)

Signs:

- Guaranteed or “risk-free” returns. This is especially concerning with crypto, forex, commodities, or private platforms.
- Pressure to act quickly
- Secret or invite-only opportunities
- Claims of insider access

What to Do:

- Stop payments
- Use Investor.gov, FINRA BrokerCheck, or NFA BASIC as applicable; do not rely on screenshots or links supplied by the promoter
- Report to your bank and authorities

Cryptocurrency / Virtual Currency Scams

Signs:

- Requests to send crypto to a “secure wallet”
- Fake trading platforms showing fake profits
- Withdrawal blocked by “fees” or “taxes”
- Requests to share wallet keys or recovery phrases

What to Do:

- Stop sending crypto
- Contact the exchange immediately

- Preserve wallet addresses and transaction hashes
- Understand that crypto transfers are often irreversible, but reporting still matters

Romance Scams Involving "Investments"

Signs:

- A relationship is built online
- The scammer introduces an "investment opportunity"
- Emotional pressure replaces due diligence

What to Do:

- End contact after preserving evidence
- Do not send more money
- Seek support, emotional manipulation is intentional

AI-Generated Investment Pitches

Signs:

- Deepfake videos or audio of celebrities or executives
- Fake news articles or endorsements
- Highly polished "advisors" with no verifiable history

What to Do:

- Verify claims independently
- Report ads and accounts
- Preserve evidence of AI misuse

Report the Scam

- National Reporting
  - Federal Trade Commission (FTC)
    - Main federal agency for consumer fraud
    - reportfraud.ftc.gov
  - Internet Crime Complaint Center (IC3) – FBI
    - Tracks internet-based financial crimes and scams
    - [ic3.gov](ic3.gov)
  - U.S. Postal Inspection Service
    - If the scam involved mailed checks, money orders, or parcels
    - uspis.gov/report
  - Secret Service Cleveland Field Office
    - Investigates certain cyber-enabled financial crimes; use FTC, IC3, or local law enforcement for routine consumer scam reporting
    - 216-750-2058
- Ohio Resources
  - Ohio Attorney General – Consumer Protection & Identity Theft

   - https://www.ohioattorneygeneral.gov
   - Consumer Protection Hotline: 800-282-0515
- Geauga County
   - Geauga County Sheriff's Office
   - https://www.geaugasheriff.org
   - Local police non-emergency line for documentation
   - Call 911 if threats, coercion, or immediate danger are involved

Recovery – After Reporting

- Monitor financial and crypto accounts daily
- Watch for recovery scams claiming to get your money back (often another scam)
- Keep all reports, case numbers, and correspondence in one place
- Consider professional financial counseling if losses were significant

How to Reduce Investment Scam Risk

- Slow down, urgency is a scam tactic
- Be skeptical of guaranteed returns
- Verify people, platforms, and licenses independently
- Treat unsolicited investment offers as suspicious
- Ask for a second opinion before moving money
- Remember: real investments don't require secrecy
- Add a trusted contact where your financial institution offers it