# Financial Account & Payment Fraud

*Responding to Scams Impacting Money and Payments*

Financial account and payment fraud occurs when money is taken, payments are misdirected, or financial accounts are misused without your authorization. This can happen through scams, account takeovers, deception, or technical compromise.

This guide applies to:

- Card fraud (credit or debit cards)
- Overpayment / refund scams
- Subscription & free trial traps
- Unauthorized bank transfers
- Payment app fraud (Zelle, Venmo, Cash App, PayPal)

If fraud is ongoing or escalating, act immediately. Delays reduce recovery options.

## Financial Fraud – Do This First

### Stop Further Loss Immediately

- Do not send more money
- Do not refund or return funds sent by a stranger
- Do not follow new instructions from the person involved
- Pause all related transactions

If someone is pressuring you to act quickly, that is a red flag.

### Contact Your Financial Institution Right Away

- Using a known, official number:
    - Call your bank, card issuer, or payment app
    - Report the transaction as fraud
- Ask them to:
    - Freeze or secure the account
    - Reverse or stop pending transactions (if possible)
    - Issue new cards or credentials
    - Request a case or reference number

Time is critical, many reversals are only possible within hours or days.

### Secure Related Accounts

From a safe device:

- Change passwords on:
    - Banking accounts
    - Payment apps
    - Email (often the gateway)
- Review:
    - Linked accounts
    - Authorized devices
    - Recovery contact information

## Common Types of Financial Fraud & What to Do

### Card Fraud (Credit / Debit Cards)

Signs:

- Charges you don't recognize
- Small "test" charges followed by larger ones

What to Do:

- Report immediately to the card issuer
- Dispute unauthorized charges
- Request a new card number
- Monitor statements closely

### Overpayment / Refund Scams

Signs:

- Someone sends you money (often a fake check or payment)
- Asks you to send back the "extra"
- The original payment later reverses

What to Do:

- Do not send money back
- Contact your bank or payment app
- Preserve all messages and transaction records

### Subscription & Free Trial Traps

Signs:

- Unexpected recurring charges
- Difficulty canceling
- Charges after a "free" trial

What to Do:

- Cancel through official account settings
- Dispute unauthorized or deceptive charges
- Monitor for additional subscriptions

## Unauthorized Bank Transfers

Signs:

- Money moved without your approval
- New payees or routing details added

What to Do:

- Contact your bank immediately
- Ask about transfer recall options
- Secure online banking access
- Monitor for further activity

## Payment App Fraud (Zelle, Venmo, Cash App, PayPal)

Signs:

- Fake "refund" or "mistaken payment" requests
- Urgent impersonation scams
- Requests to send money to "fix" a problem

What to Do:

- Report fraud in-app immediately
- Contact linked bank or card issuer
- Do not send additional funds
- Save all transaction IDs and messages

## Preserve Evidence

Before deleting messages or emails:

- Screenshot:
    - Transactions
    - Messages or instructions

    - Payment confirmations
- Record:
    - Dates and times
    - Amounts
    - Accounts or apps involved

This documentation supports disputes and investigations.

## Report the Fraud

- 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
    - U.S. Postal Inspection Service
        - If the scam involved mailed checks, money orders, or parcels
        - uspis.gov/report
    - Secret Service Cleveland Field Office
        - Main federal agency for financial crimes
        - 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 the Fraud Is Contained

- Monitor bank and payment accounts daily for several weeks
- Review credit card and bank statements carefully
- Watch for follow-up scams referencing the incident
- Consider fraud alerts or credit monitoring if advised
- Fraudsters often attempt repeat targeting.

## How to Reduce Financial Fraud Risk

- Slow down, urgency is a common tactic
- Never send money to "fix" a problem
- Treat unexpected payments as suspicious
- Verify independently before moving money
- Ask for a second opinion before acting under pressure
- Add a Trusted Contact to all financial accounts