

# Who to Call, and What to Say

A professional did this, and they do it for a living. That is not the same as being careless, and it is not why this happened. What matters now is the order of the next few calls, and that order is below. **Work down it. Do not skip to the end.**

It does not matter whether this happened an hour ago, this morning, or last week. **Start at step one anyway.** A pending transfer, a card dispute, a wire recall and a credit freeze all run on different clocks, and several of them are probably still running. People lose more to giving up early than to being slow.

## 1 Start with whatever can still be stopped

Do not begin with money that left months ago if something is moving *right now*. Start with the transaction that might still be interrupted.

- ☐ A bank transfer that **has not settled**
- ☐ A wire that **may still be recalled**
- ☐ A credit or debit charge that **can be disputed**
- ☐ A gift card with an **unused balance**
- ☐ A payment-app transaction that **may be reviewed**
- ☐ A crypto transfer that **has not completed**
- ☐ A check that **has not cleared**
- ☐ A loan or retirement withdrawal **still processing**
- ☐ A package that **has not shipped or been forwarded**
- ☐ A new account, beneficiary change, or authorized user **not yet finalized**

## 2 Make the bank call now

Use the number on the back of your card, a recent statement, or the institution's official website. **Never a number the scammer gave you** — and never a number from a search result, because those get bought too.

### SAY THIS WHEN THEY PICK UP

*"I've been scammed and I need to stop a payment. Please connect me to the fraud department." Then: "Tell me whether the transaction is pending or complete, and whether it can be stopped, recalled, disputed, frozen, or reviewed."*

### THEN ASK EVERY ONE OF THESE

- |                                                                        |                                                             |
|------------------------------------------------------------------------|-------------------------------------------------------------|
| ? Is the transaction pending or complete?                              | ? Can alerts or trusted-contact protections be added?       |
| ? Can a hold, recall, dispute, or fraud review be opened?              | ? Are there other recent transactions fitting this pattern? |
| ? What documents or written statements do you need?                    | ? What is the case or reference number?                     |
| ? Should account numbers, cards, logins, or security questions change? | ? Who should receive additional evidence?                   |

Write down the **date, time, representative's name, case number**, and what the institution said it would do. There is a log for this on the last page.

## 3 Then call by how the money left

Each method has its own clock and its own short list of people who can still act.

|                                    |                                                                                                                                                                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Credit card</b>                 | The card issuer. Report the fraudulent circumstances, <b>ask them to refund the money</b> , ask whether the number should be replaced, and review recent charges for small test transactions.                                                                             |
| <b>Debit card or bank transfer</b> | The bank or credit union, immediately. <b>Ask them to reverse the payment and refund the money</b> . Zelle transfers go through the bank, not a separate company.                                                                                                         |
| <b>Gift cards</b>                  | The company that issued the card, using the number on the card itself. Say it was used in a scam and ask whether any balance remains. <b>Keep the card and the receipt</b> even though the code was shared.                                                               |
| <b>Wire transfer</b>               | The bank or wire company (Western Union, MoneyGram). State clearly that the transfer was <b>induced by fraud</b> and ask for a recall or reversal. Have the recipient name, account, transfer number, amount, date and destination ready.                                 |
| <b>Payment app</b>                 | The app's official fraud process <i>and</i> the linked bank or card issuer. Save the username, payment ID, transaction number, phone number and message history. <b>Do not keep messaging the recipient to negotiate.</b>                                                 |
| <b>Cryptocurrency</b>              | The exchange, kiosk operator or wallet provider. Report it as fraud and ask whether the account or transfer can be flagged or frozen. Save wallet addresses, transaction hashes, QR codes, receipts and screenshots. Crypto is often impossible to reverse — call anyway. |
| <b>A check</b>                     | The bank. A deposited check can appear to clear and be returned as fraudulent weeks later — if money was forwarded from it, <b>the bank may hold the account holder responsible for the shortage.</b>                                                                     |
| <b>Cash by mail</b>                | U.S. Postal Inspection Service, <b>1-877-876-2455</b> . They can attempt to intercept a package that has not been delivered.                                                                                                                                              |

#### 4 Secure the email account before anything else

Email controls everything else. Whoever can read it can reset banking, shopping and cloud passwords — and quietly delete the alerts that would have warned you.

- ☐ Change the email password **from a device you believe is safe**
- ☐ Use a new password that has **never been used anywhere else**
- ☐ Turn on **multifactor authentication**
- ☐ Review recovery phone numbers and backup email addresses
- ☐ Check **forwarding rules, filters, connected apps** and recent logins
- ☐ Sign out of all other sessions and remove unfamiliar devices
- ☐ **Then** change passwords on financial and other important accounts

Do not reuse the new email password anywhere, and do not change any password on a device the scammer may still control — read step 5 first.

#### 5 Check whether someone still has the screen

Scammers talk people into installing software that lets a stranger watch or control the computer or phone. It is usually presented as necessary — to fix an account, verify a transfer, or help with a technical problem.

##### ASK YOURSELF

*“Did anyone ever watch your screen, move the mouse on their own, ask for a code, or say not to touch the computer?”*

- ☐ **Disconnect the device from the internet** if access looks active
- ☐ Do not use that device for new passwords or banking until it is checked
- ☐ Have a trusted technician inspect it and remove remote-access tools
- ☐ Contact financial institutions **from a different device**
- ☐ Screenshot program names, messages and dates **before removing anything**

## 6 Stop money and packages moving *through* you

If you have **received** money or packages for this person, stop before anything else is forwarded. Someone can be used as a money mule without ever understanding that the funds came from other people who were scammed.

- ☐ Do not return money to the person. Do not move it to another account.
- ☐ Do not convert it to cryptocurrency. Do not reship packages.
- ☐ Contact the bank, carrier, merchant, law enforcement or an attorney for instructions

**Once this risk appears, stop improvising and get advice.**

## 7 Save the evidence before it disappears

Profiles get deleted and numbers change fast. Save what you can access lawfully, store copies somewhere the other person cannot reach, and keep the originals.

- ☐ **Full message threads** — not just the screenshots you picked
- ☐ Profile pages, profile links, usernames, numbers, emails, aliases
- ☐ Photographs and documents that were sent
- ☐ Bank, wire, card, gift-card, app and crypto receipts
- ☐ Wallet addresses and transaction hashes
- ☐ Package labels, tracking numbers, shipping records
- ☐ Voicemails, threats, and any request for secrecy
- ☐ A written timeline of promises, payments and meetings that never happened

## 8 Make the reports

Reporting does not guarantee an investigation, and no honest person can promise the money comes back. It still matters — reports connect accounts, numbers, wallet addresses and identities used against many families at once.

|                                                   |                                                                                                                                                                             |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IC3</b><br>ic3.gov                             | The FBI's Internet Crime Complaint Center. File here for any online-enabled fraud.                                                                                          |
| <b>FTC</b><br>ReportFraud.ftc.gov                 | The Federal Trade Commission's fraud report.                                                                                                                                |
| <b>Elder Fraud Hotline</b><br>833-372-8311        | For people age 60 and older. A <b>case manager</b> is assigned and helps with the reporting itself. Free. Monday-Friday, 10am-6pm ET, English, Spanish and other languages. |
| <b>AARP Fraud Watch</b><br>877-908-3360           | A free helpline staffed by trained volunteers. Useful when you want to talk it through with a person before deciding what to do next.                                       |
| <b>IdentityTheft.gov</b><br>FTC                   | If a Social Security number, license, passport, tax return, Medicare or bank information was shared. Builds a personal recovery plan.                                       |
| <b>The three bureaus</b><br>freeze or fraud alert | Equifax <b>888-378-4329</b> · Experian <b>888-397-3742</b> · TransUnion <b>800-916-8800</b> . A freeze is free and does not affect credit scores.                           |
| <b>The platform</b><br>app / bank / social        | Report the account or profile the contact came through.                                                                                                                     |
| <b>Local police</b>                               | For threats, theft, blackmail, stalking or unsafe travel.                                                                                                                   |

**Keep every report number and every agency name.**

## What not to do

- ✗ Do not send **one more payment** to find out whether it was real
- ✗ Do not pay taxes, fees or insurance to release supposed profits
- ✗ Do not pay anyone who **guarantees** they can get the money back — that is the second scam, and it targets people who already lost once
- ✗ Do not let the person use accounts, phone numbers, addresses or identities
- ✗ Do not destroy messages or devices — that is the evidence
- ✗ Do not send a long goodbye, threaten exposure, or bargain for repayment. A final confrontation can trigger guilt, blackmail, or a new invented emergency
- ✗ Do not post intimate or identifying information publicly
- ✗ Do not wait for perfect proof while a transaction is still pending
- ✗ Do not go quiet about it — the people who recover fastest told someone on the first day

### KEEP ONE LOG — IT STOPS REPEAT CALLS AND MISSED DEADLINES

| DATE & TIME | COMPANY OR AGENCY | CASE NUMBER | NEXT ACTION |
|-------------|-------------------|-------------|-------------|
|             |                   |             |             |
|             |                   |             |             |
|             |                   |             |             |

## What a good day looks like

You may not recover a dollar today, and you may not get the whole story straight today either. A good day is smaller than that, and it counts for more:

- ✓ The wire was recalled
- ✓ The gift-card balance was frozen
- ✓ The bank opened a fraud case
- ✓ The email account is secure
- ✓ Remote access was removed
- ✓ No package was forwarded
- ✓ The evidence was saved
- ✓ The profile was reported
- ✓ No additional money was sent
- ✓ You asked someone to help

## The next 72 hours are the ones that decide it

A bank that hears the word **fraud** today treats the account differently than one that hears it on Friday. Some reports carry real deadlines. And every hour the email stays unsecured is another hour someone else can reset a password.

This page gave you the calls and the words. The **Scam Recovery First Aid Kit** gives you the order: what to do today, tomorrow and the day after, which deadlines are real, and what to do when a call goes badly — plus the walkthrough that asks how the money left and builds the sequence around your answer.

[THESCAMHOTLINE.COM/FIRST-72-HOURS](https://thescamhotline.com/first-72-hours)

Nobody honest can promise you will get the money back. Anyone who does is running the second scam. This checklist offers educational information, not legal, financial, medical, or psychological advice, and no outcome can be promised. When the situation calls for an attorney, financial professional, physician, or law enforcement, bring them in. Federal reporting details verified August 2026; confirm current contact information at the agency's own website. · One Buck Capital · © 2026 The Scam Hotline