FREE · THE SCAM HOTLINE

The First 72 Hours.

It just happened. Here is what to do, in order.

A professional did this. They do it for a living, and they are good at it. That is not the same as you being careless, and it is not why this happened.

What matters now is the order of the next few calls. That order is in here: today, tomorrow, and the day after. Work down it. Do not skip to the end.

START WHERE YOU ARE

I think I just sent money to someone I shouldn’t have.

Page 2. Minutes matter.

I think I gave someone information I shouldn’t have.

Page 2, then Day One, step 4.

Someone got into my phone, computer, or one of my accounts.

Page 3, step 5. Then Day One.

It’s my mom or dad.

Everything here works the same. Page 9 is for you.

THESCAMHOTLINE.COM/HELP · 321-NO-SCAMS

THE FIRST HOUR

Start with whatever can still be stopped.

Whether this happened an hour ago 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 are probably still running. People lose more to giving up early than to being slow.

1 Find the thing that is still moving

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** · a new account, beneficiary or authorized user **not yet final**

2 Make the bank call now

Use the number on the back of your card, a recent statement, or the bank's own 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."***
>
> ***"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 a hold, recall, dispute, or fraud review be opened?
- ? What documents do you need from me?
- ? Should my account number, card, login or security questions change?
- ? Can you add alerts or a trusted contact?
- ? Are there other recent transactions that fit this pattern?
- ? What is the case number?
- ? Who do I send additional evidence to?

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

Then call by how the money left.

Each way money moves has its own clock and its own short list of people who can still act.

IF IT WENT BY	CALL THIS, AND ASK FOR THIS
Credit card	The card issuer. Report the fraud, **ask them to refund the money**, ask whether the number should be replaced, and look for small test charges.
Debit card or bank transfer	Your bank or credit union, immediately. **Ask them to reverse the payment.** Zelle goes through the bank, not a separate company.
Wire transfer	The bank or wire company (Western Union, MoneyGram). Say the transfer was **induced by fraud** and ask for a recall. Domestic wires are sometimes recallable in the first hours, international within a day or two. Odds are poor. Call anyway, fast.
Gift cards	The company on the card, using the number on the card. Say it was used in a scam and ask whether any balance remains. **Keep the card and receipt.**
Payment app	The app's fraud process ***and*** the linked bank or card. Save the username, payment ID, transaction number and messages. **Stop messaging the recipient.**
Cryptocurrency	The exchange, kiosk operator or wallet provider. Save wallet addresses, transaction hashes, receipts, screenshots. Often impossible to reverse. Call anyway.
A check	The bank. A deposited check can look cleared and bounce weeks later. If you forwarded money from it, the bank may hold you responsible for the shortage.
Cash by mail	U.S. Postal Inspection Service, **1-877-876-2455**. They can try to intercept a package that has not been delivered.

Not tonight. Not ever.

- × 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 hunts people who already lost once.
- × Do not send a long goodbye, threaten exposure, or bargain for repayment. A final confrontation invites blackmail or a new invented emergency.
- × Do not destroy messages or devices. That is the evidence.
- × Do not let anyone use your accounts, phone number, address or identity, and do not forward money or packages that came to you. See page 8.

DAY ONE · TODAY

Close the doors.

The money call is made or in progress. Now close every door the scammer might still be standing in. Email first, because email controls everything else.

4 Secure the email account before anything else

Whoever can read your email can reset your 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**, to one never used anywhere else
- [ ] Turn on **two-factor authentication** (an authenticator app beats text messages)
- [ ] Check **forwarding rules, filters, connected apps** and recent logins. Remove anything you don't recognize.
- [ ] Sign out of all other sessions. Review recovery phone numbers and backup emails.
- [ ] **Then** change passwords on bank, brokerage, and other important accounts

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 my screen, move the mouse on their own, ask me for a code, or tell me not to touch the computer?"***

- [ ] If yes: **disconnect that device from the internet** and do not use it for passwords or banking until it is checked
- [ ] Restart your phone. Remove apps and profiles you did not install. Review app permissions.
- [ ] Call your mobile carrier and add a **SIM lock / port-out PIN** so your number cannot be moved
- [ ] Have a trusted technician remove remote-access tools. Screenshot program names and dates first.

6 Lock down the rest

Bank and card apps

- [ ] New password, two-factor on
- [ ] Turn on alerts for every transaction
- [ ] Turn off Zelle / Venmo / Cash App for now
- [ ] Look for new payees or linked accounts

Social accounts

- [ ] New passwords, two-factor on
- [ ] Remove unknown logins and devices
- [ ] Tighten privacy settings
- [ ] Warn friends if your account messaged them

The password rule: three different passwords at minimum, for email, banking and social. Never reuse. A password manager makes this painless. Write recovery codes on paper.

7 If you shared information, not just money

A Social Security number, driver's license, Medicare number, passport, tax return, or bank login opens doors for months. Two calls close most of them.

- [ ] **Freeze your credit** at all three bureaus. Free, takes ten minutes, does not touch your score. Equifax **888-378-4329** · Experian **888-397-3742** · TransUnion **800-916-8800**. A freeze is stronger than a fraud alert; do the freeze.
- [ ] **IdentityTheft.gov** if an ID number or tax information was shared. It builds a recovery plan and generates the letters.
- [ ] Medicare number shared: **1-800-MEDICARE**. Ask them to flag the account.

DAY ONE · TONIGHT

Tell one person. Then stop for the night.

The part nobody puts on a checklist. Scams work because the person is scared, rushed and alone. The scammer needed all three. You can take one away tonight.

8 Tell one person

Not everyone. One. A spouse, a sibling, a friend who is good in a crisis. The people who recover fastest, in money and in sleep, told someone on the first day. The people who took the longest kept it to themselves for months. Silence is the scammer's best friend, and it costs you the second set of eyes you need for the next 72 hours.

> *IF YOU DON'T KNOW HOW TO START*
>
> ***"Something happened and I need to tell you about it. I'm not asking you to fix it. I need you to know, and I might need help with a couple of calls."***

9 What is happening in your head right now

You will replay it. You will find the moment you should have seen it. You will feel stupid. Read this part slowly.

Scammers fool doctors, lawyers, engineers, and people who work in cybersecurity. Not because those people are foolish, but because the method does not attack intelligence. It attacks the state you were in. **Stress compresses decision-making. Fear narrows attention. Trust hands authority to whoever sounds like they have it.** A professional built that state on purpose, over hours or weeks, and then made the ask. That is a technique, and it works on almost everyone the first time.

> ***What happened does not define you.***
> ***What you do next does.***

If you need a sentence to say to yourself when it spikes: ***"I'm safe now. I'm taking the right steps. I'm not alone, and I'm not ashamed."*** It feels silly. It also works, because it is true.

10 Save the evidence before it disappears

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

- [ ] **Full message threads**, not just the screenshots you picked
- [ ] Profile pages, links, usernames, numbers, emails
- [ ] Photos and documents they sent
- [ ] Voicemails, threats, any request for secrecy
- [ ] Bank, wire, card, gift-card, app and crypto receipts
- [ ] Wallet addresses and transaction hashes
- [ ] Package labels and tracking numbers
- [ ] A written timeline: promises, payments, meetings that never happened

DAYS TWO AND THREE

The bank, the second time.

Yesterday was the emergency call. Today is the follow-up, and it goes better when you know which of two situations you are in, because the bank treats them differently and so does the law.

A. Someone else moved the money

They used your card number, your login, a code they tricked out of you, or remote access to your screen. **You did not send it.**

This is an **unauthorized transaction**. For bank accounts and debit cards, federal Regulation E applies: the bank must investigate, usually within 10 business days, and often gives provisional credit while it does. Credit cards have their own dispute rights. Your job is to report it fast and in writing.

> *SAY*
>
> ***"I did not make or authorize this transaction. I'm reporting it as unauthorized and I'd like the dispute opened today. Please confirm in writing what you need from me."***

B. I sent it myself

You typed it in, approved the Zelle, bought the cards, or wired it, because someone convinced you it was real. **You were deceived, but you sent it.**

Be honest about this. The bank is not required to refund a payment you authorized, even one you were tricked into, and claiming it was unauthorized when the records show otherwise ends the conversation and can void the claim. What you can do: ask for a **scam claim review**. Since 2023, the major banks on Zelle refund many imposter-scam payments (someone posing as your bank, a government agency, or a business). Many banks also have discretionary goodwill refunds, and asking is free.

> *SAY*
>
> ***"I sent this payment because I was deceived by someone impersonating [who]. I'm asking you to review it as a scam claim, attempt a recall from the receiving bank, and tell me in writing what your decision is and why."***

11 When the bank says no

A first no is not the end. Banks are required to give you a written explanation for a denied dispute, and a written record is what the next step runs on.

> *ASK FOR FOUR THINGS, IN WRITING*
>
> ***"Please send me, in writing: the specific reason for the denial, what evidence you relied on, your appeals process and its timeline, and a contact in your complaints or compliance department."***

Then file two complaints. They cost nothing and banks take them seriously, because a regulator reads them.

- [ ] **CFPB** · consumerfinance.gov/complaint. The bank must respond, usually within 15 days. Denials get reversed at this step more often than people expect, in situation A especially.
- [ ] **Your state attorney general** · search "[your state] attorney general consumer complaint."

In situation B, a complaint will not force a refund the law does not require. It does put a second set of eyes on the goodwill decision.

12 Document everything

Date and time of every call. The agent's name and ID. Case numbers. The exact words they used. Scan every letter. Appeals and complaints are decided on paper, and the side with the better paper usually wins.

The people who call next.

Within days, sometimes hours, you may hear from someone offering to get your money back. A "recovery firm." A "fraud investigator." A lawyer. A hacker. Someone from the "refund department." Your name is now on a list of people who have paid once, and that list is sold.

13 The three laws of fake recovery

- **Law 1. Nobody legitimate finds you.** Real help (your bank, the FBI, the FTC, a lawyer you hired) does not cold-call, cold-text, or slide into your messages. If they found you, that is the tell.
- **Law 2. Nobody legitimate can promise your money back.** Not the bank, not the FBI, not us. Anyone who guarantees it is lying, and they know they are lying.
- **Law 3. Nobody legitimate asks for a fee up front.** Not a "processing fee," not "taxes to release the funds," not gift cards, not crypto. Government agencies never charge a fee to help a victim.

Block the number. Do not explain, negotiate, or say goodbye. If it came from a social account, report and block. If it feels convincing, that is the point; it is the same skill set that got you the first time.

14 Make the reports

Reporting does not guarantee an investigation, and it will not bring the money back by itself. It still matters, twice: it creates a time-stamped record the bank can see, and it connects your case to the hundreds of other families the same crew is working.

Your bank done on day one	The official fraud case. Case number, agent, date. Reference it in every later call.
FBI IC3 ic3.gov · 5 minutes	The federal complaint for any online-enabled fraud. Banks recognize the number. Keep it.
FTC ReportFraud.ftc.gov · 3 minutes	Adds your case to the national fraud database. Some banks ask for this number in disputes.
Local police if needed	For threats, blackmail, theft, or when the bank asks for a police report number (some do above certain amounts). Ask for the report number, not an investigation.
Elder Fraud Hotline 833-372-8311	For anyone 60 or older. A case manager helps you file the reports above. Free, weekdays 10am–6pm ET.
AARP Fraud Watch 877-908-3360	Free helpline, trained volunteers. Good when you want to talk it through with a person.
The platform dating app, social, marketplace	Report the profile or account the contact came through. It gets taken down faster than you'd think.

> *USE THE NUMBERS WHEN YOU CALL THE BANK BACK*
>
> ***"I've filed FBI IC3 report [number] and FTC report [number]. I can provide both for your investigation."***

Verify the numbers above at the agency's own website before calling; they were checked in August 2026.

DAYS FOUR THROUGH SEVEN

You're back in control.

You made the calls. You closed the doors. You did not freeze and you did not hide. That already puts you ahead of most people this happens to. Here is what the next week looks like.

15 What to expect

- [ ] The bank may call back for details. Have your log in front of you.
- [ ] Bank investigations take 30 to 90 days. In situation A, provisional credit often appears within 10 business days.
- [ ] You will check your accounts more often than you need to. That fades.
- [ ] Waves of anger and embarrassment will come without warning, usually at night. Normal. They pass.
- [ ] The scammer will probably not follow through on threats. Once the doors are closed, they move on to someone whose doors are open.

16 If money or packages came *to* you

Some scams turn the victim into a courier. If you received money for someone, or packages to forward, stop before anything else moves. Do not return money to the person. Do not move it to another account or convert it to crypto. Do not reship. Call the bank, the carrier, or an attorney for instructions. Once this risk appears, stop improvising and get advice.

17 Your log

DATE & TIME	COMPANY OR AGENCY	CASE NUMBER	NEXT ACTION / DEADLINE

What a good week looks like

You may not recover a dollar this week, and you may never get the whole story straight. A good week is smaller than that, and it counts for more:

- ✓ Whatever could be stopped, was
- ✓ The bank has a case number
- ✓ Email and phone are yours again
- ✓ Credit is frozen
- ✓ No second payment went out
- ✓ The reports are filed
- ✓ The evidence is saved
- ✓ One person knows

IF IT'S YOUR MOM OR DAD

Help them without taking over.

Everything in this guide works the same when it happened to your parent. Two things change: who makes the calls, and how you talk about it. Get the second one wrong and you lose the cooperation you need for the first.

The first conversation

Your parent was not careless. A professional spent days or weeks building the moment, and it would have worked on you. Say that out loud, early, and mean it. Shame is the scammer's second weapon; it keeps people quiet, and quiet people send more money.

> *TRY*
>
> *"This was done to you by a professional. I'm not upset with you, I'm upset with them. Can we sit down together and make a couple of calls?"*
>
> *"I'm not going to take over your accounts. I want to sit next to you while you make the calls, and take notes."*

- [ ] **Sit beside them, don't call for them.** The bank needs the account holder. You take notes and hold the list.
- [ ] **Ask, don't interrogate.** "Did anyone ever watch your screen?" beats "Did you let someone into your computer?"
- [ ] **Don't impersonate them** or go into their accounts without permission, even to help. It damages the claim and the relationship.
- [ ] **Watch for a second contact.** The scammer often calls back with a new emergency, or a "recovery" offer, within days. Make sure they know to hang up and call you.
- [ ] **Ask about independence out loud.** "What would make you feel safe without me checking your accounts?" Transaction alerts to both phones is a common answer.

The family talk, before the next one

Once the crisis is handled, this is the twenty minutes that changes what happens next time. Four rules, agreed out loud, ideally with the whole family on the same call.

"We don't click links from texts. Ever."

The bank, the package, the toll, the grandchild. We open the app or call the number on the card.

"If someone calls with an emergency, we hang up and call back."

On a number we already have. Every time. A real emergency survives a five-minute callback.

"If something feels off, we check with each other."

Nobody sends money while scared or rushed. Before it moves, one other person hears about it.

"We have a safe word."

A word only the family knows. If a voice on the phone asks for money and can't say it, it isn't them. A familiar voice used to mean something. It doesn't anymore.

> *OUR FAMILY SAFE WORD*
>
> ______________________________ *agreed on* ______________

BEFORE YOU CLOSE THIS

You are not helpless anymore.

You may never stop every scam. Nobody can, and we would be wary of anyone who says otherwise. But you can be harder to fool, faster to respond, and not alone when something feels wrong. Three days ago you didn't know what to do. Now you have done it.

Three things that help from here

Want a check-in each day for the next week? One short email a day, what to look for and what to do that day. Nothing to buy inside them. TheScamHotline.com/help, at the bottom of the page.

The founder's book. I spent a year not telling anyone I'd been scammed. FOOLED is the story of that year and what I learned, written for the night you feel most alone in this. It is a few dollars and you can read it tonight. TheScamHotline.com/book

The free tools. The Scam Detector reads any text or email and names the pressure tactic. Clone Call lets your family hear an AI scam call in your own voice. Both free, no account. TheScamHotline.com/tools

If you want the calls in your order, or a person on the line while you make them, both exist at TheScamHotline.com/help. Everything above is free either way.

The Scam Hotline never

- ☐ Asks for your bank login, account access, or a code
- ☐ Promises your money back
- ☐ Charges a fee to “recover” anything
- ☐ Calls you first

Anyone who does any of those four is running the second scam. Hang up, and tell someone.

Nobody honest can promise you will get the money back. Anyone who does is running the second scam. This guide is 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. Regulation E and bank-refund practices summarized here are general; your bank's decision depends on your facts and your account agreement. Federal reporting details verified August 2026; confirm current contact information at each agency's own website. No method can stop every scam. The goal is a family that is harder to fool and faster to check. · The Scam Hotline · 321-NO-SCAMS (321) 667-2267 · TheScamHotline.com · Lugap Consulting LLC d/b/a One Buck Capital · 312 W. Northwest Hwy, Ste. 128, Grapevine, TX 76051 ·