PRETEXT STORIES

THE FAMILY KIT
FREE SAMPLE

Four pages from the full kit: two scams from the Scam Gallery, the fridge poster and the large-print pocket cards.

Get the full kit (44 pages, a Word family agreement and large-print cards) at pretextstories.com/family

SCAM 1 OF 11

THE FAMILY EMERGENCY CALL

Per the FBI, senior citizens are targeted in grandparent scams. The FTC says the caller can claim to be any family member or close friend.

Over $5 million FBI IC3: claimed losses to "distress" scams in 2025

A caller who sounds like a relative says they are in trouble and need money fast. The voice may be cloned by AI.

HOW IT WORKS

- The FTC says a scammer could clone a loved one's voice using a short audio clip, perhaps from content posted online, and a voice-cloning program.
- The FTC says the scammer will say it is urgent and that you are the only one who can help, and may ask you to keep it secret.
- The FTC says some scammers pose as an authority figure, such as a fake lawyer, police officer or doctor, to sound more convincing.
- The FBI describes a second scammer posing as the grandchild's attorney, asking for legal fees, bond money or medical expenses.
- The FTC says scammers insist on payment that is hard to recover: wire transfer, cryptocurrency, payment app, or gift card numbers.

WARNING SIGNS

- The caller says it is urgent and that you are the only one who can help.
- You are told to keep it secret from other family members.
- Payment is demanded by wire, cryptocurrency, payment app or gift card numbers.
- A lawyer, police officer or doctor joins the story.
- Cash is to be mailed or handed to a courier at your door.

WHAT TO DO

- The FTC says do not trust the voice, even if it sounds like your relative. Hang up, then call them on a number you know is right.
- The FTC says you can ask a question only the real person would know, or call another relative or friend, even if told to keep it secret.
- The FBI suggests creating a secret word or phrase with your family to verify their identity.
- The FTC says if you already sent money, the sooner you act, the better. Report it at ReportFraud.ftc.gov.
- Common practice: agree on a family code word now, and tell older relatives about this scam before a call comes.

> *"I'm going to hang up and call you back on the number I already have. If it's really you, I'll reach you in a minute."*

Common practice phrase. **Report to:** The FTC at ReportFraud.ftc.gov; the FBI asks victims to report to its Internet Crime Complaint Center at www.ic3.gov.

Sources: FBI IC3 2025 Annual Report (Artificial Intelligence section) (2025 report year (no publication date in the text)); FTC Consumer Alert: Scammers use AI to enhance their family emergency schemes (March 20, 2023); FTC Consumer Advice: Scammers Use Fake Emergencies To Steal Your Money (September 2023); FBI IC3 PSA I-120324-PSA: Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud (December 3, 2024); FBI IC3 PSA I-111723-PSA: FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers (November 17, 2023)

SCAM 2 OF 11

THE BANK FRAUD DEPARTMENT CALL

Anyone with a bank, credit union or investment account. The contact can arrive as a text, call or email, per the FBI and the FTC.

Over $262 million FBI: account takeover fraud losses reported since January 2025

A caller or text claims to be your bank's fraud team, then asks for a code or tells you to move your money.

HOW IT WORKS

- The FTC says some of the costliest impersonation scams start with a fake security alert, often from a bank, and push people to move money to "protect" it.
- The FTC says these scams involve someone supposedly spotting fraud on your account, offering to "protect" your money, and telling you to move it.
- The FTC says scammers trick you into sharing a verification code. With it they can log in and transfer money out of savings or investment accounts.
- The FBI says criminals may text, call or email as bank support, or send people to a fake login site, to get login details and passcodes.
- The FBI says funds are wired quickly to criminal-controlled accounts, many linked to cryptocurrency wallets, so they are hard to trace and recover.

WARNING SIGNS

- Anyone asking for your verification code or one-time passcode.
- Being told to move money to a "safe" or "protected" account.
- A text or call about suspicious activity or a charge you did not make.
- Being told to lie to anyone who asks why you are moving money.
- A caller who stays on the phone while you go to the bank.

WHAT TO DO

- The FTC says never move or transfer your money to "protect it." Your money is fine where it is.
- The FTC says never share a verification code. No caller, even one from your bank's fraud department, will ask for it.
- The FTC says to call your real bank using the number on your statement, never the number the caller gave you.
- The FBI says not to trust caller ID: hang up, verify the correct number, and call it yourself.
- The FTC says if you moved money or shared a code, tell your bank or fund right away, then report to the FTC.

> *"I'll hang up and call my bank on the number printed on my card. I won't share any code or move any money."*

Common practice phrase. **Report to:** Your bank or fund right away, then the FTC at ReportFraud.ftc.gov. The FBI asks for reports at www.ic3.gov.

Sources: FBI IC3 PSA I-112525-PSA: Account Takeover Fraud via Impersonation of Financial Institution Support (November 25, 2025); FTC Consumer Alert: Never move your money to "protect it." That's a scam (March 5, 2024); FTC Consumer Alert: What's a verification code and why would someone ask me for it? (March 7, 2024); FTC Consumer Alert: Did someone tell you to move or transfer your money? It could be a scam (January 19, 2024); FTC Press Release: FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025 (June 15, 2026)

PRETEXT STORIES · THE FAMILY KIT

STOP.
HANG UP.
CALL BACK.

1 · Hang up. Call back on a number you already have.

2 · Never give a code, password or PIN.

Not to the bank. Not to "tech support".

3 · No gift cards, wire transfers or crypto machines.

Not for anyone who contacted you.

4 · Slow down. It can wait ten minutes.

"Right now" and "tell no one" are warning signs.

5 · Tell someone. There is no shame.

Call first: _____ ☎

PRINT, CUT, KEEP

POCKET AND PHONE-SIDE CARDS

Print on card stock at 100%. Keep one beside the phone and one in the purse or wallet.

THE FIVE RULES

1. Hang up. Call back on a number I already have.
2. Never give a code, password or PIN.
3. No gift cards, wires or crypto machines for anyone who contacted me.
4. Slow down. It can wait ten minutes.
5. Tell someone. No shame.

FOUR WARNING SIGNS

- **Urgency.** "Right now!"
- **Secrecy.** "Tell no one."
- **New way to pay.** Gift cards, wires, crypto.
- **A fee to get my own money.**

MY FAMILY CODE WORD

Ask: "What's our word?"
No word? Hang up and call back.

Word: _____ (do not write it here if others will see this card)

WHO I CALL FIRST

Name: _____

Phone: _____

Bank (from my card): _____

Report a scam: _____