RECOVERY FRAUD & FAKE IC3 CONTACTS

After the scam, fraudsters may pretend to help - then steal again.

> FBI warns of fake IC3 and FBI contacts
A July 20 IC3 alert says scammers are impersonating FBI and IC3 personnel to deceive and revictimize people who already lost money.
Read the July 20 IC3 PSA

> Recovery promises are the second strike
Victims report contacts by phone, email, social media, ads, and forums claiming funds were recovered or that help is available.
Review recovery scam warning

> AI makes the fake authority more believable
The alert describes AI-generated videos, spoofed sites, fake profiles, and deepfake-style content used to create false trust.
See AI warning signs

> Gold, cash, couriers, and wires remain in play
A July 22 DOJ case alleges a U.S. Marshals impersonation scheme used gold bars, fear, secrecy, and in-person pickup.
Read the DOJ gold-bar case

> Grandparent scams are organized operations
A July 15 DOJ case described a transnational call-center scheme involving more than 400 seniors, cash runners, rideshare drivers, and repeat asks.
Read the DOJ call-center case

TENNESSEE TAKEAWAY

As scammers pivot from crypto ATMs to wires, cash pickup, gold, gift cards, apps, and fake recovery help, every partner should ask: Is this transaction tied to a prior scam or a promise to recover money?
Share SafeSeniorTN resources

THE SECOND STRIKE

LOSS > HOPE > FAKE HELP

The victim is not careless. The victim is often trying to fix the damage, file a report, or recover money. Scammers exploit that hope by pretending to be law enforcement, government, a bank, a lawyer, or a recovery company.

1 First loss → 2 Search for help → 3 Fake IC3/FBI → 4 Pay to recover → 5 More loss

WHAT THEY MAY SAY

- REC — **We recovered your funds.**
- UPD — **Your IC3 report needs an update.**
- FEE — **Pay a tax, fee, deposit, or bond first.**
- SEC — **Do not tell your bank or family.**
- LNK — **Use this link, app, profile, or chat.**

SUSPECT ELDER ABUSE? REPORT IT. Tennessee Adult Protective Services: 1-888-277-8366 | tn.gov/aging

HOW TO BREAK THE SECOND STRIKE

Slow the request. Verify the source. Preserve the proof before money moves again.

RED FLAGS TO RECOGNIZE

- The contact comes after a prior scam, report, or loss.
- The person claims to be FBI, IC3, a bank, an attorney, or a recovery firm.
- You are moved to Telegram, Facebook Messenger, WhatsApp, or another private app.
- A link is sent to "update" a complaint or verify identity.
- A fee, tax, wire, cash pickup, gift card, crypto payment, or gold purchase is required.
- Secrecy and urgency are used to keep family, bank staff, or police out of the conversation.

QUESTIONS THAT CREATE A PAUSE

- Did they contact you, or did you call an official number you already trusted?
- Did you type IC3.gov yourself, or click a link from a message or search result?
- Why would a government agency or recovery service require advance payment?
- Has anyone told you to keep this from your bank, family, or law enforcement?
- Can a local law enforcement officer or trusted financial institution independently verify this?
- What evidence should be saved before any more money moves?

COALITION FIELD NOTE: PROTECT THE VICTIM'S HOPE

A recovery scam works because the victim wants help, wants answers, and may be embarrassed or afraid. Do not lecture. Lead with validation, then create a safe pause.

"You did the right thing by asking for help. Let's verify this through an official channel before anyone sends another dollar."

Frontline objective: keep trust with the victim long enough to stop payment, preserve evidence, and report quickly.

PAUSE
Slow the request before money, gold, crypto, gift cards, wires, or cash leave.

TYPE IC3.GOV
Use the address bar. Do not click a link from a text, email, ad, or profile.

VERIFY
Call a known number for the bank, local law enforcement, or agency.

PRESERVE
Save messages, profiles, URLs, phone numbers, receipts, account and wallet data.

REPORT
Report to local police, IC3, APS, and appropriate victim-support resources.

REPORTING & RESOURCE LINKS

FBI Internet Crime Complaint Center - IC3.gov

National Elder Fraud Hotline - 1-833-FRAUD-11

Tennessee Adult Protective Services - 1-888-277-8366

TBI SafeSeniorTN - SafeSeniorTN.com

FTC ReportFraud - ReportFraud.ftc.gov

QUICK PARTNER ASK

Banks / CUs	Ask if this is about recovering money.
Law Enforcement	Collect contacts, links, profiles.
Aging Network	Share: no real agency charges a fee.
Families	Name one trusted caller before crisis.

Sources: FBI IC3 PSAs; DOJ elder-fraud cases; FTC consumer guidance; TBI SafeSeniorTN resources.

SUSPECT ELDER ABUSE? REPORT IT. Tennessee Adult Protective Services: 1-888-277-8366 | tn.gov/aging