TNEJC WEEKLY UPDATE

August 24, 2026 | Phone-first scams: robocalls, spoofing, and fake safe-account pressure

THE CALL IS THE HOOK

Caller ID, a government name, or a local number can be fake. The goal is to create panic, isolate the victim, and move money before anyone else can ask questions.

TN focus | Robocalls + texts | Phantom hacker playbook

TOP DEVELOPMENTS

› Tennessee pushes upstream robocall prevention.
Attorney General Skrmetti joined a bipartisan coalition urging the FCC to strengthen Know Your Customer rules for voice providers, arguing illegal robocalls are a tool used to steal from vulnerable people.

› Nearly 29.6 billion scam robocalls/texts.
The TN AG release cites national volume and nearly $2 billion in related fraud losses last year, underscoring why call-blocking alone is not enough.

› Phantom hacker cases keep evolving.
DOJ reported an August 3 guilty plea in a scheme where callers posed as government employees and pushed victims to move funds to fake safe accounts, cash, or gold.

› SafeSeniorTN is moving directly to homes.
DDA and TBI are using meal delivery partners, including an ETHRA pilot, to distribute scam magnets and resource cards to isolated older adults.

› Tampa-area case reinforces the warning.
WFLA reported that Treasure Island Police announced multiple arrests after a victim lost $1.5 million in a complex fraud scheme. Use this as a case example: large losses often follow sustained coaching, fear, and pressure to move assets quickly.

CURRENT TREND TO WATCH

Phone-first fraud is becoming a handoff crime

The first contact may look like a routine robocall, local callback, fake bank alert, computer pop-up, or government warning. The next step is the dangerous part: victims are coached to move savings into cash, gold, wire transfers, cryptocurrency, gift cards, or new accounts. The scammer may stay on the phone while the victim drives to a bank, store, or ATM.

1 Panic | 2 Isolation | 3 Coaching | 4 Transfer | 5 Pickup

TNEJC FIELD NOTE

Treat this as coercive control, not a one-time bad decision. The frontline objective is to create a pause, keep the victim connected to trusted help, and preserve evidence before the transaction becomes irreversible.

Use this phrase: "No one from the government, bank, or police can order you to move money, buy gold, or hand cash to a courier."

PARTNER ACTION ITEMS THIS WEEK

Financial institutions

Add one question to large-cash, wire, gold, or new-payee reviews: "Is someone on the phone telling you what to say or do?"

Senior centers / meals

Share SafeSeniorTN and the senior handout. Encourage members to bring suspicious calls/texts to a trusted staff member before acting.

Law enforcement / APS

Ask for caller ID screenshots, callback numbers, pop-up photos, bank instructions, courier details, receipts, and all coaching language.

Reporting reminder

If money moved: call the bank immediately, ask about recall/hold-harmless options, file IC3.gov, contact local law enforcement, and consider the National Elder Fraud Hotline at 833-FRAUD-11.

TNEJC WEEKLY UPDATE

Operational playbook | Stop the transfer before money leaves

QUESTIONS THAT BREAK THE SCAM SCRIPT

? Who told you the money was unsafe, and how did that person first contact you?

? Are you being told to stay on the phone, keep this secret, or avoid talking with family?

? Did anyone ask you to withdraw cash, buy gold, wire money, use a payment app, or send cryptocurrency?

? Can you hang up and call your bank, law enforcement, or a trusted family member using a number you find yourself?

? Did anyone ask for remote access to your computer, phone, online banking, or email?

? Has anyone promised reimbursement, government protection, or a new safe account?

RECOGNIZE THE HANDOFF

- Caller ID shows a local number, bank, police, FBI, FTC, Medicare, Social Security, or court.
- The caller says your money is not safe and asks you to "protect" it.
- You are told to buy gold, withdraw cash, wire money, open a new account, or use crypto.
- You are coached on what to say to bank staff, family, or law enforcement.
- A courier, rideshare driver, or "agent" is expected to collect money or valuables.

PRESERVE EVIDENCE

Save screenshots of caller ID, texts, pop-ups, emails, wallet addresses, receipts, shipping labels, bank slips, gold receipts, phone numbers, vehicle descriptions, and names used by the caller.

WHERE TO SEND PEOPLE

Immediate danger
911 / local law enforcement

TN elder abuse
APS: 1-888-277-8366

Cyber fraud
IC3.gov

Elder fraud support
833-FRAUD-11

Robocalls
DoNotCall.gov

Medicare fraud
1-800-MEDICARE or SMP

TN prevention
SafeSeniorTN.com

Consumer message of the week: Hang up. Call back using a number you find yourself. No legitimate agency can order you to move money to protect it.

Source links reviewed this week:

- TN AG - Robocall KYC effort
- TDCI elder investor protection
- FTC - Robocalls
- IC3 - Elder Fraud
- DDA/TBI/ETHRA SafeSeniorTN meals pilot
- DOJ - Phantom Hacker guilty plea
- FTC - Imposter scams/WEAAD
- WFLA/Treasure Island PD - $1.5M case