BRIDGING TECHNOLOGIES ATL

THE DIGITAL SELF-DEFENSE PLAYBOOK

FRAUD REPORTING & RECOVERY EDITION

Recognize the Scam. Stop the Threat. Report the Fraud. Protect the Next Person.

COMMUNITY PROTECTION EDITION

A free reference for seniors, families, and community members.



TALK TECH WITH CHET | 180ANGLES | ASK CHET

SENIORS FIRST. FAMILIES ALWAYS.

Edition 2.0 • Contacts reviewed November 11, 2026

OPEN THIS PAGE FIRST

What do I do RIGHT NOW?

Find the situation that matches yours. Start with the immediate action, then report.

Someone is in immediate danger

A person is threatening you, or someone is arriving to collect cash, cards, or valuables. Do not confront them.

CALL 911

Money was sent or a charge appeared

Call the real bank, card issuer, transfer service, or payment app immediately. Ask whether it can stop, dispute, trace, or reverse the payment.

PAYMENT PROVIDER FIRST

A password, code, or identity information was shared

Use a trusted device to secure accounts, and contact affected businesses through numbers you found independently.

SECURE ACCOUNTS NEXT

You spotted a scam but lost no money

End the contact, keep the evidence, and make a report. The attempt still matters.

REPORT TO THE FTC

IMPORTANT: A government report does not reverse a payment. Contact the payment provider first.

YOUR FIELD GUIDE

How to use this playbook

You do not need to memorize every agency. You need a reliable first move.

Three rules to remember

01 You may hang up. You do not owe a stranger an explanation or an immediate answer.

02 Verify outside the conversation. Use a number or website you find independently, never the contact details supplied in the suspicious message.

03 An attempt still counts. Even when you lose $0, a suspicious scam attempt can be reported.

Find what you need

- Pages 2–6: Immediate actions and reporting routes
- Pages 7–9: FTC, FBI IC3, Georgia, and elder protection
- Pages 10–17: Payment, identity, health, mail, and specialized fraud
- Pages 18–22: Reporting details and 180Angles practice
- Pages 23–26: Worksheet, protection plan, sources, quick contacts

> **NO SHAME. NO BLAME. JUST THE NEXT SAFE STEP.**
>
> You can ask a trusted friend, family member, or counselor for help completing a report. Never give them a password, PIN, or one-time code.

OUR DIGITAL SELF-DEFENSE BADGE Education • Self-Awareness • Critical Thinking • Action. Learn, recognize, verify, and take the next safe step.

ACTION SYSTEM

The five-move response

Use these moves for a suspicious call, email, text, website, or in-person approach.

01 STOP. Hang up or stop replying. Do not send money, codes, screenshots of IDs, or remote-access permissions.

02 SAVE. Keep the original message, number, sender address, date, screenshots, receipts, and transaction details. Do not reopen suspicious links.

03 SECURE. If you paid or shared information, contact the bank or affected company immediately through a trusted channel. Change exposed passwords.

04 REPORT. Use the FTC for consumer scams. Use FBI IC3 for internet crime. Add a specialized agency only if it fits.

05 FOLLOW UP. Record case numbers, monitor accounts, and question anyone who promises to recover money for a fee.

> **Do not try to investigate the scammer yourself.**
>
> Do not confront a courier, send a “test” payment, or install software to help someone “verify” an incident.

REPORT THE ATTEMPT

No money lost? Report it anyway.

An ignored scam call or suspicious email can still be useful information for investigators.

Federal Trade Commission (FTC)

Consumer scams and suspected attempts: fake prizes, impostors, romance, shopping, tech support, bogus charges, and more.

877-382-4357

Official website: ReportFraud.ftc.gov

A simple reporting statement

You can say:

“I want to report a suspected scam. It happened on [date]. The person claimed to be [name/company]. I did not send money. I saved the message and phone number.”

Before reporting, save what you know

- Approximate date/time and how the person reached you.
- The name or organization claimed, and any fake urgency.
- Phone number, sender email, website address, or social-media profile.
- Money requested and whether anything was actually sent.

If it was only an unwanted phone call

The FTC also provides DoNotCall.gov for reporting unwanted calls without financial loss. For a clear consumer scam attempt, ReportFraud.ftc.gov is a useful starting point.

CHOOSE YOUR LANE

Where should I report?

Choose one good starting point. Add another agency only when it clearly applies.

General consumer scam or attempted scam

Federal Trade Commission (FTC).

877-382-4357

Official website: ReportFraud.ftc.gov

Internet / email / social media / crypto

FBI Internet Crime Complaint Center (IC3).

Online reporting

Official website: IC3.gov

Threats, courier, stolen cash, or local crime

Local police or sheriff. Use 911 if immediate danger.

911 only for emergencies

Georgia consumer scam

Georgia Attorney General Consumer Protection Division.

404-651-8600

Official website: consumer.georgia.gov

Age 60+ and need guidance? DOJ Elder Fraud Hotline: 833-372-8311. See page 9.

NATIONAL REPORTING

The FTC and FBI IC3

These two agencies are broad, trusted starting points—but their jobs are different.

FTC: ReportFraud

For consumer scams, including attempts. It helps authorities spot patterns and may provide next-step advice.

877-382-4357

Official website: ReportFraud.ftc.gov

FBI: Internet Crime Complaint Center

For cyber-enabled crimes: online impersonation, email, scams involving digital transactions, cryptocurrency, fake investment platforms, and more.

Submit online

Official website: IC3.gov

Be alert for fake IC3 investigators.

The real IC3 says it does not directly contact complainants to ask for money or information. People claiming they can recover lost funds for an upfront fee may be scammers.

Bank first if money moved.

Use the card, statement, or banking app you already trust. File government reports after taking urgent steps with the payment provider.

GEORGIA RESPONSE

Police and the Georgia Attorney General

Local reporting is important when a scam affects your home, finances, or safety.

Local police or sheriff

Report threats, cash collection, theft, suspected crimes, and serious losses. Ask whether an incident report is appropriate.

911 for immediate danger

Georgia Attorney General

Consumer fraud affecting Georgians, such as home-repair fraud, telemarketing schemes, fake businesses, and deceptive offers.

404-651-8600 / 800-869-1123

Official website: consumer.georgia.gov

Reporting is not the same as a refund.

The Georgia AG can review complaints and use them to identify patterns, but filing does not guarantee reimbursement or a specific investigation.

If you live outside Georgia

Use your own state attorney general and adult protective services agency. The national FTC, IC3, and DOJ contacts still apply.

PROTECT OLDER ADULTS

Elder fraud and exploitation

Financial exploitation by a caregiver, friend, or relative may need a different response from a random scam call.

DOJ National Elder Fraud Hotline

For adults 60+ who want help understanding fraud and reporting options. Monday–Friday, 10 a.m.–6 p.m. Eastern.

833-372-8311

Official website: justice.gov/elderjustice

Georgia Adult Protective Services (APS)

For suspected abuse, neglect, or exploitation of a person 65+ or an adult 18+ with a disability living in the community. APS is not an emergency responder.

866-552-4464 • Press 3

Official website: aging.georgia.gov

If someone is in danger, call 911.

For problems in nursing homes or other licensed care facilities, Georgia directs reports through different channels; use the Division of Aging Services site to find the right agency. If APS does not return your message, follow up.

FINANCIAL FIRST AID

If money moved: bank, card, or wire

Call the company that moved the money immediately—even if you plan to file a police or federal report.

01 Debit or bank account. Call your bank's fraud department. Ask it to block access, review unauthorized transactions, and determine available dispute options.

02 Credit card. Use the number on the back of the card. Ask to dispute the charge and replace a compromised card if needed.

03 Bank wire. Ask immediately whether the transfer can be recalled or traced. Have details ready, but share them only with the real bank.

04 Save your reference number. Record the date, representative's name (if provided), case ID, and the next action or deadline.

Language to use

"I believe this payment involved fraud. Please connect me with the fraud department and tell me whether the transaction can be blocked, disputed, traced, or recalled."

OTHER WAYS SCAMMERS GET PAID

Payment apps, gift cards, crypto, and cash

Recovery options differ by payment method; there is no guaranteed refund.

Payment apps

Report the transaction inside the legitimate app. Contact your linked bank or card issuer too, when applicable.

Gift cards

Contact the card issuer right away. Keep the card and receipt in a secure place. Ask whether any remaining value can be frozen or refunded.

Cryptocurrency

Contact the exchange or ATM operator promptly and report to the FTC and FBI IC3. Keep transaction IDs privately. Transfers are often difficult to reverse.

Cash pickup or mailed cash

If someone is coming to collect money, follow local police guidance and call 911 if in immediate danger. For cash sent by U.S. Mail, contact USPIS quickly: 877-876-2455.

Recovery scams are a second attack.

Never pay an upfront “release,” “tax,” “verification,” or “recovery” fee to someone promising to retrieve stolen money.

ACCOUNT PROTECTION

If a password, code, or access was exposed

Work from a device you trust and an independently verified website or app.

01 Change the affected password. If you reused that password anywhere else, change it there too. Use a new, unique password.

02 Turn on multifactor authentication. Prefer an authenticator app or passkey when supported; protect recovery options and backup codes.

03 If you gave a one-time code, contact the real account provider immediately. Review device sessions, recovery methods, and recent activity.

04 If you installed remote-access software, disconnect that device from the internet, contact your financial institutions from another device, and seek trusted technical help to secure or reset the device.

05 Look for other changes. Check forwarding rules, unfamiliar logins, new payees, and changed account recovery details.

> **Never share your recovery codes or passwords**
>
> Neither government investigators nor a legitimate technology helper needs your one-time verification code to review a suspected scam.

IDENTITY DEFENSE

If your identity information was exposed

If someone used your identity, use the FTC's dedicated recovery process.

IdentityTheft.gov

Personal identity theft recovery steps, an FTC Identity Theft Report when applicable, and guidance for exposed Social Security numbers or other information.

877-438-4338

Official website: IdentityTheft.gov

Protect your credit

- A credit freeze is free. You must contact Equifax, Experian, and TransUnion separately to freeze all three files.
- A fraud alert is also free; for an initial fraud alert, contacting one bureau is enough to notify the others.

Official free credit reports

Review your reports for unfamiliar accounts and inquiries.

877-322-8228

Official website: AnnualCreditReport.com

Keep records secure.

Never write your full Social Security number, account number, date of birth, passwords, or verification codes in this printed playbook.

GOVERNMENT IMPOSTORS

Social Security and IRS threats

Government letterheads, real-looking caller IDs, and agency names can all be faked.

SSA Office of Inspector General

Report fake Social Security calls, texts, messages, and suspected program fraud.

Report online

Official website: oig.ssa.gov/report

IRS tax-related scams

For suspicious IRS emails, texts, letters, websites, or tax-related identity theft, use IRS reporting guidance.

Report online

Official website: irs.gov/help/report-fraud

TIGTA: Fake IRS calls

Report someone impersonating the IRS and threatening arrest or demanding immediate payment.

800-366-4484

Official website: irs.gov

Practice this response

“I will not pay or provide information on this call. I will look up the agency myself and call the official number.”

HEALTHCARE DEFENSE

Medicare, Medicaid, and medical equipment

Review Medicare notices and statements for care, equipment, or charges you do not recognize.

Medicare: Suspected fraud

For Medicare claims you do not recognize, services you did not receive, or suspicious equipment billing.

800-633-4227

Official website: medicare.gov

Georgia Medicaid / PeachCare fraud

Report suspected Georgia Medicaid or PeachCare program fraud to the state Department of Community Health OIG.

800-533-0686

Official website: dch.georgia.gov

Georgia SHIP: Free Medicare counseling

Unbiased help understanding coverage, notices, and bills. Counseling is not the same as filing a fraud complaint.

866-552-4464 • Option 4

Official website: aging.georgia.gov/georgia-ship

HHS Office of Inspector General

Suspected fraud, waste, or abuse in federal HHS health programs, including Medicare and Medicaid.

800-447-8477

Official website: oig.hhs.gov/fraud/report-fraud

MAIL, CALLS, AND TEXTS

Different channels, different reports

Caller ID and the name displayed on a text message can be spoofed.

U.S. Postal Inspection Service (USPIS)

Suspected scams involving U.S. Mail, mailed checks or cash, lottery mailings, or mail theft.

877-876-2455

Official website: uspis.gov/report

FCC: Unwanted calls or texts

Reports of unwanted robocalls, texts, or spoofing help enforcement. The FCC generally does not resolve individual unwanted-call complaints.

File online

Official website: consumercomplaints.fcc.gov

Your mobile carrier: 7726 (SPAM)

If supported, forward suspicious texts to 7726 to help your carrier detect spam. For serious fraud, also report to the FTC or IC3, as appropriate.

7726

Never act on caller ID alone.

If a “bank,” “police officer,” or “agency” contacts you unexpectedly, hang up and independently find the correct contact details.

SPECIALIZED REPORTING

Investments, financial products, veterans

These are add-on routes when the subject fits. The FTC and IC3 remain useful starting points.

SEC: Securities and investment fraud

For Ponzi schemes, fake investment offerings, broker misconduct, or possible securities law violations.

Submit online

Official website: sec.gov

CFTC: Commodities, forex, derivatives

For suspected scams involving regulated commodities, futures, swaps, forex, and some digital-asset schemes.

866-366-2382

Official website: cftc.gov/complaint

CFPB: Financial services complaints

For complaints about banks, credit cards, loans, money transfers, credit reporting, and other consumer financial products.

855-411-2372

Official website: consumerfinance.gov/complaint

VA program or benefit fraud: VA OIG • 800-488-8244 • va.gov/oig/hotline

REPORT WITH CONFIDENCE

What information should I gather?

You do not need every detail before reporting. Share what you know accurately.

01 What happened? Explain the story in your own words: who contacted you, what they claimed, and what you were told to do.

02 When and where? Date, approximate time, text/email/phone/website, and platform or physical location, if known.

03 Who or what? Names used, phone numbers, sender addresses, websites, user IDs, and other identifying clues.

04 What changed hands? Amount requested or paid; payment method, date, and any bank or provider case number.

05 What evidence exists? Screenshots, receipts, transaction IDs, messages, and voicemails. Keep originals when possible.

After you report

Write down confirmation or complaint numbers. Check for legitimate follow-up through the agency's official website. A government report does not guarantee a personal response or a refund.

180ANGLES: CORE SKILL

Verify outside the conversation

Do not let the suspicious person choose the source that supposedly proves the story.

01 NOTICE. Is someone creating panic, secrecy, pressure, or an urgent problem?

02 DISCONNECT. Hang up, stop the chat, or close the suspicious page.

03 FIND YOUR OWN SOURCE. Use a number on your bank card, a bookmarked app, or an official website you type yourself.

04 CHECK. Ask the real organization whether the charge, account problem, notice, or request exists.

05 DECIDE. If it is suspicious, do not comply. Save evidence and report through the proper channel.

Two examples

A fake purchase email gives you a “cancellation” phone number. A fake bank employee sends a “security” link. Do not use either. Go to the company independently.

Practice with 180Angles: Break the Play

Visit: Community Protection Hub: bridgingtechnologiesatl.com/protect

SPOT THE PLAY

Six red flags to recognize

A polished website, real logo, familiar voice, or correct personal detail is not proof.

01 BORROWED TRUST. “I am from your bank, Medicare, Social Security, or your family.”

02 FALSE URGENCY. “You must act in ten minutes or lose everything.”

03 SECRECY. “Do not tell your family, bank teller, or anyone else.”

04 UNUSUAL PAYMENT. “Move funds to a safe account or use gift cards, cash, or crypto.”

05 ACCOUNT ACCESS. “Read me the code, give me the password, or install this app.”

06 CONTROLLED VERIFICATION. “Call only the number I gave you, and do not hang up.”

Default move

STOP → VERIFY INDEPENDENTLY → REPORT WHEN SUSPICIOUS

BREAK THE PLAY | ROUND 1

Two practice scam reviews

Answer each question before reading the safer move.

PLAY 1: The $429 charge

An email says you purchased a $429 item and offers a phone number to cancel. You do not remember buying anything. What is your next move?

Safer move

Do not call the number in the email. Use the real retailer or financial app independently to check. Save and report the suspicious message.

PLAY 2: The Social Security threat

A caller says your Social Security number is “suspended” and police will arrest you unless you pay today. What is your next move?

Safer move

Hang up. Do not pay. Verify through Social Security’s official site if needed, then report the impersonation to SSA OIG and/or the FTC.

Discuss with a partner

Which red flag did you spot first? What independent source would you use?

BREAK THE PLAY | ROUND 2

Two more decisions to practice

Scammers often mix a believable story with instructions that move your money or take control of your phone.

PLAY 3: The “safe account”

Someone claiming to be bank security says criminals have your savings. They insist you move the money today to a new “safe account.” What do you do?

Safer move

End the call. Do not move money. Call your bank directly through the number on your card or a trusted app. If you already transferred money, tell the bank immediately.

PLAY 4: The helpful technician

A caller says your phone has a virus. They ask you to download an app so they can “fix it,” then request a verification code. What do you do?

Safer move

Refuse the download and code request. If you already gave access, disconnect the device and seek trusted support; contact the bank from another device if financial information may be exposed.

Practice is protection

For more scenarios, return to the Community Protection Hub and use Break the Play.

PRIVATE WORK PAGE

My fraud reporting worksheet

Use this to organize a report. Do not email or upload this filled-in page to an unfamiliar person.

What happened? (Brief summary)

When? (Date and approximate time)

How did the person reach me? (Call / text / email / web / in person)

Name, phone number, website, or account used

Money requested or sent (if any)

Agency, provider, or police report number / next step

PRIVATE INFORMATION RULE

Do not write passwords, PINs, one-time codes, full Social Security numbers, complete financial account numbers, or recovery phrases here.

TAKE OWNERSHIP

My personal protection plan

Protection is a skill you can keep practicing.

The next time I receive a suspicious message, I will:

- Pause rather than respond to pressure.
- Verify outside the conversation.
- Ask a trusted person for help when uncertain.
- Save the evidence and report a scam attempt, even if I lose no money.

One trusted person or organization I can contact

One digital safety skill I will practice this month

MY DIGITAL SELF-DEFENSE COMMITMENT

I will protect my independence by slowing down, asking questions, verifying claims independently, and reporting suspicious activity. I can help protect others by sharing what I learn.

Signature (optional): _____ Date: _____

SOURCE AND PUBLICATION NOTES

Official sources, verified contacts

The playbook points to official government reporting sites. Keep its phone numbers current.

Primary reporting sources

Federal Trade Commission — reportfraud.ftc.gov

FBI Internet Crime Complaint Center — ic3.gov

DOJ Elder Justice — justice.gov/elderjustice

Georgia Attorney General — consumer.georgia.gov

Georgia Adult Protective Services — aging.georgia.gov

Medicare — medicare.gov

FTC Identity Theft — identitytheft.gov

U.S. Postal Inspection Service — uspis.gov/report

About this edition

Published by Bridging Technologies ATL | Talk Tech With Chet | 180Angles | Ask Chet. Edition 2.0. Contacts independently reviewed November 11, 2026. Agency procedures and numbers can change; always confirm through official websites.

Educational resource only—not legal, financial, healthcare, or law-enforcement advice. No report guarantees an investigation, refund, or personal response. This guide is free to download and share intact.

BRIDGING TECHNOLOGIES ATL

KEEP THESE CONTACTS HANDY

YOUR FIRST FIVE ROUTES

1 GENERAL SCAM / ATTEMPT

FTC • 877-382-4357 • ReportFraud.ftc.gov

2 ONLINE CRIME

FBI IC3 • IC3.gov

3 IMMEDIATE DANGER

Call 911. Otherwise contact your local police or sheriff.

4 SENIOR FRAUD GUIDANCE

DOJ National Elder Fraud Hotline • 833-372-8311

5 GEORGIA CONSUMER FRAUD

Georgia Attorney General • 404-651-8600

BRIDGING TECHNOLOGIES ATL COMMUNITY PROTECTION HUB

bridgingtechnologiesatl.com/protect

SENIORS FIRST. FAMILIES ALWAYS.

