Red Flags & How to Protect Yourself:

Knowing the signs of a scam can help you avoid it. Here are some **red flags** that apply to almost any scam scenario:

- **Unsolicited requests for personal or financial info:** Be extremely wary if *anyone* contacts you out of the blue (by phone, email, text) asking for sensitive details like your Social Security number, banking account, credit card number, Medicare ID, passwords, etc. Legitimate organizations (banks, Social Security, Medicare) **generally will not contact you unsolicited** and ask for that over the phone or email. If you think the call or email might be real, don't give info right then; instead, independently find the official phone number of that organization and call them to ask if there's an issue. Nine times out of ten, you'll find out your "Medicare account" is just fine and no one from Medicare was actually trying to reach you.

- **Pressure and a sense of urgency:** Scammers want to get you to act *before* you can think. If a message says things like "Immediate action required!" or a caller makes you panicky (threatening legal action, or saying a loved one is in peril), it's likely a scam. **Take a breath.** Real companies or authorities do not threaten to arrest you over the phone, and family emergencies can be verified. When you feel pressured, that's your cue to slow down. It's perfectly okay to say, "I will call you back," and then consult someone or verify the story. **Don't let anyone bully or rush you** into payment on the spot.

- **Requests for payment via gift cards, prepaid cards, wire transfers, or cryptocurrency:** This is a huge red flag. Scammers often instruct victims to pay by gift cards (like iTunes, Amazon, Google Play cards) or by wiring money (Western Union/MoneyGram) or sending Bitcoin. **Any legitimate business or government agency will accept standard payment methods and will NEVER demand gift cards or Bitcoin**. If somebody says, "Go to Target and buy $500 in gift cards and read me the codes," that is 100% a scam. Hang up immediately. The same goes for asking to wire money to a "private account" or an overseas account. These methods are nearly impossible to recover once sent, which is why scammers use them. Remember: **gift cards = scam** in these contexts.

- **Caller ID or email name looks official, but something's off:** Scammers can spoof phone numbers to look like a legitimate agency (**Caller ID can lie**). For example, it might say "IRS" or show a local number. Don't trust that alone. Similarly, emails

may have a sender name like “Account Security” but the email address is something bizarre or slightly misspelled (e.g., security@.com instead of microsoft.com). Always check the actual email address and not just the display name. If the email domain doesn’t match the official organization, it’s a scam (for instance, an email claiming to be from Chase Bank coming from john.smith@gmail.com – clearly fake). Even if it does match, if you weren’t expecting it, be cautious. When in doubt, don’t click links – go to the official website by typing it in yourself.

- **“Too good to be true” offers or winnings:** Unexpected windfalls (prizes, inheritances from unknown relatives, ridiculously cheap deals) are very likely fake. Scammers lure people by appealing to greed or excitement as well. If it sounds too good to be true, it is.

- **Attachments or Links in unsolicited emails:** If you get an email with an attachment (PDF, Word doc, etc.) that you were not expecting – **do not open it**. Likewise, don’t click on links in unsolicited or suspicious messages. These can install malware or lead you to phishing sites. If an email claims to be from a company with an important message (like “Your statement is attached” or “Open this document to sign”), *verify first*. Hover over links to see where they actually go (on a computer, hover your mouse over the link without clicking, and a small URL preview should appear). Many times you’ll see the URL has nothing to do with the supposed sender. When in doubt, delete the email or call the company directly. It’s better to be overly cautious than infected with a virus.

- **Gut feeling or inconsistency:** Finally, trust your instincts. If something just doesn’t feel right or is out of the ordinary, double-check it. Scammers often make mistakes or push too hard. Maybe the person on the phone called you by the wrong name, or an email claiming to be your bank has a spelling error. If anything raises an eyebrow, do not proceed without verification.

What to do if you suspect a scam: Stop engaging with the scammer. If on the phone, hang up. If it’s an email, don’t reply or click (you can delete it). Talk to someone you trust about it – often, explaining it to a friend or family member will quickly reveal if it’s fishy (sometimes just saying it out loud, you realize it sounded phony). You can also look up the scenario online; for example, search “[Grandchild in jail scam]” – you’ll see it’s a known fraud. **Report** scams to authorities if possible: for consumer scams, you can report to the **FTC**

(Federal Trade Commission) at reportfraud.ftc.gov, and for online crimes, to the FBI's **IC3** (Internet Crime Complaint Center) at ic3.gov. Also, AARP has a Fraud Watch Helpline (877-908-3360) that gives advice to seniors about scams. Reporting not only helps potentially catch the scammers, but also helps agencies gather statistics and warn others.

Remember: Being targeted by a scam is not a reflection on you – these criminals are very convincing and prey on anyone. By knowing their tricks, you can avoid becoming a victim. The key takeaways: **never give personal info or money to unexpected callers/emails**, and **always double-check anything unusual or urgent through a separate trusted channel**.

Scam & Fraud Protection Checklist:

- ☐ I will **never** give out personal data (SSN, passwords, bank info) or send money **in response to an unsolicited call, email, or message**.
- ☐ I am alert to **red flags** like pressure to act now, threats of arrest, or requests to pay via gift cards or wire transfer – these are signs of a **scam**.
- ☐ If something seems "off," I will **stop and verify** by contacting the supposed source directly or asking a trusted family member before taking action. It's always okay to hang up or ignore a message until I'm sure it's legitimate.