YOUR FRAUD FIGHTER GUIDE

ROBOCALL SCAMS THAT TARGET OLDER PERSONS

PROVIDED COURTESY OF NOMOROBO AND
FRAUD PREVENTION STRATEGIES, LLC

INTRODUCTION

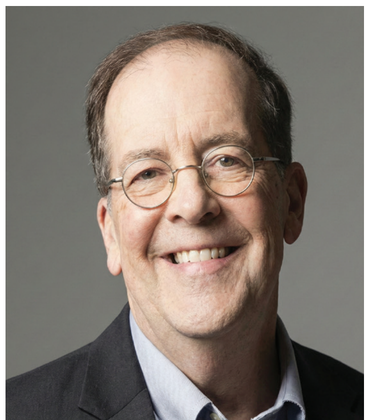
To say that consumer fraud is a growing problem is a gross understatement. According to the Federal Trade Commission (FTC), consumer fraud complaints increased a whopping 25% from 2024 to 2025 with losses in the billions of dollars.

Older persons are particularly hard hit in the fraud wars. According to the FTC, older person fraud losses have increased more than 300% in the last four years and total losses could be as high as $80 billion dollars a year (FTC,2025). The FTC also reports that the highest individual dollar losses among seniors came as the result of a phone call.

In this pamphlet, we provide a set of tools older persons can use to better detect and resist scam attempts. By knowing the common psychological tactics scammers employ, adopting a "Fraud Fighter" mindset and using technology to "harden the target" and block such malicious attacks, you can dramatically reduce your chances of losing money. We also summarize the top robocall scams flooding into the United States in 2025 that target older persons. The source of these calls: Nomorobo's 300,000 phone line "Honeypot" digital tracking system which records and transcribes over five million robocall messages per year. From those transcripts, we have identified over one million robocall scam attacks and have summarized those most likely to reach older consumers.

MATT MIZENKO

GENERAL MANAGER
Nomorobo



DOUG SHADEL

MANAGING DIRECTOR
Fraud Prevention Strategies, LLC

Our strong belief is that if you can see a scam coming from a distance, you have a much better chance of defending against it. We hope this volume helps provide a roadmap for spotting and stopping fraud in its tracks. We also hope you will share this information with friends and family members so we can all stay safe.

HOW TO BECOME A FRAUD FIGHTER

Anyone, no matter what your age, can become a fraud fighter and virtually eliminate the chance of being scammed. There are several key practices fraud fighters employ on a regular basis to ensure they are protected.

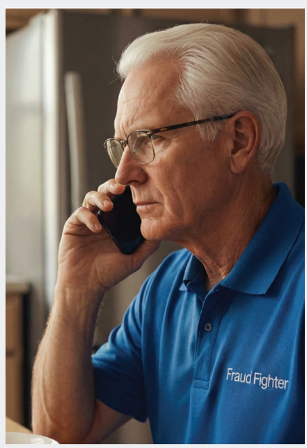
LEARN THE PERSUASION TACTICS USED BY SCAMMERS.

ADOPT A "FRAUD FIGHTER" MINDSET.

HARDEN THE TARGET.

LEARN THE SCAMMER'S PERSUASION TACTICS

Decades of research has revealed several core persuasion tactics that scammers employ to steal victims' money. Here is a quick review of the core tactics to look for.



HIGH AROUSAL LANGUAGE

Robocall scammers use high arousal words to get victims into a heightened emotional state so they can be more easily exploited. Examples include high arousal positive words like "winner", "thrill" and "celebrate" and high-arousal negative words like "scare", "arrest" and "emergency".

THREATS OF LOSS

Robocall scams are much more likely to contain threats such as loss of money, loss of credit, danger to a loved one and even imprisonment as a tactic to get fraud targets to comply with their requests.

PROMISE OF GAIN

Robocall scams contain more promises of gain, especially financial gain such as claims that the fraud target won the lottery or that the government has free grant money or that they can receive a discount on their phone or utility bill.

GOVERNMENT IMPOSTORS

Robocall scammers frequently pretend to be calling from credible government agencies such as Social Security, the IRS or Medicare in order to gain the fraud target's trust.

TIME PRESSURE

Robocall scammers use time pressure or urgency significantly more often than general sales calls in order to force the fraud target to make a quick decision, one they may later regret.

ADOPT A FRAUD FIGHTER MINDSET

When it comes to fraud, one of the most powerful things one can do to prevent victimization is to reframe how you view incoming sales solicitations. Instead of viewing robocalls as possible opportunities to save money or to avoid losing money, we recommend increasing your level of skepticism about ALL such contacts. Here are some additional tips to consider.

GUILTY UNTIL PROVEN INNOCENT

In today's aggressive marketplace, there is so much fraud coming at us that it requires a skeptical view of all offers one might receive.

QUESTION ALL UNSOLICITED MESSAGES

Anytime you receive a phone call, a text, an email or a social media message out of the blue that you did not initiate, assume it's a scam.

AVOID INTERACTIONS THAT TRIGGER YOUR EMOTIONS

Research has shown that when we are in a heightened emotional state, something the scammers call "under the ether" - we are more susceptible to losing money to fraud. Avoid making financial decisions when you are in such an emotional state.

ASK MORE QUESTIONS THAT YOU ANSWER

Scammers HATE fraud targets who ask a lot of questions, mainly because they don't have good answers to tough questions. If the offer is legitimate, the person will willingly answer all your questions. Scammers on the other hand, usually just hang up.

SELF-IDENTIFY AS A FRAUD FIGHTER

Research has shown that individuals who think of themselves as fighting fraud are themselves less likely to be scammed. Consider volunteering for your local police department or attorney general's office to fight fraud. Or join AARP's "Digital Fraud" team (see Resources page.)

HARDEN THE TARGET

In the age of AI, where it is increasingly difficult to tell if someone is who they say they are, sheltering ourselves from the incoming fire has never been more important. "Harden the Target" means taking measures that make it difficult if not impossible for scammers to reach you with their malicious pitches. The following are suggestions that will help you reduce the number of fraud attacks you are exposed to on a daily basis and better monitor your financial accounts with the help of new fraud prevention technologies.

ANTI-VIRUS SOFTWARE

Most computer operating systems have anti-virus software to detect and prevent malware from getting into your computer. It is important to keep such software current. Consider going into your settings and turning on the “auto update” function to make sure your software is up to date.

CALL BLOCKING

Call blocking software can reduce the number of unwanted robocalls you receive by over 90 percent. Consider a call blocking app from companies like Nomorobo.com.

FREEZE YOUR CREDIT

Federal law allows all consumers to "freeze" their credit for free with all three of the major credit bureaus - Transunion, Experian and Equifax - so that identity thieves cannot use your personal information to open fake accounts in your name. When you want to open a new account, you can “thaw” credit temporarily.

You must request a freeze with each bureau separately.

- www.equifax.com/personal/credit-report-services/credit-freeze/
- www.experian.com/help/credit-freeze/
- www.transunion.com/credit-freeze

GO PAPERLESS/LOCKING MAILBOX

Stolen mail is still a big source of identity theft. Make sure you have a locking mailbox. Also, consider going "paperless" so sensitive financial information is no longer sent through the mail but is available via online access to your bank or other financial institutions.

ONLINE BANKING/MONITORING

Most banks provide a free monitoring service that allows you to set up automatic alerts that will email or text you when one of your accounts, including credit cards, is accessed. To take advantage of this service, you need to set up online banking. It is vital to monitor your accounts on a daily or weekly basis.

PASSWORD MANAGER

It is important to use a unique password for each and every internet account. If you have difficulty remembering passwords, consider a password manager app like Dashlane.com, OnePass.com or Lastpass.com.

SHRED IMPORTANT FINANCIAL DOCUMENTS

To protect your identity, it's important to shred financial documents that may contain account information or other personal identifying information that could be used by ID thieves to steal your identity. Consider getting a home shredder or look online for financial institutions that periodically offer to shred your financial documents for free.

TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication adds an additional layer of protection against hackers infiltrating your online accounts. It requires you to have a log in and password, but also a phone number or email to verify your identity. Use this for sensitive accounts like banking, 401k/pension, and credit card accounts.

US POSTAL SERVICE/INFORMED DELIVERY

This is an email notification service that the post office offers for free. You sign up and every morning before your mail is delivered, USPS sends you an email showing you scans of the mail that will be delivered that day. This allows you to know if anything is missing.

WEBSITE PRIVATE SETTINGS

Thinking about social media accounts like Facebook, Instagram, Linkedin and X (former Twitter), go to your privacy settings and limit access to only those whom you authorize. If you don't, scammers can look up your personal information and use it to spoof your identity and exploit it for their advantage.

VIRTUAL PRIVATE NETWORK (VPN)

A VPN creates a secure, encrypted "tunnel" for your internet traffic, hiding your online activity, identity, and location by routing it through a remote server. Numerous companies offer VPNs for a monthly fee such as Nord, Proton and Norton VPN.

ROBOCALL SCAMS TARGETING OLDER PERSONS

TECH SUPPORT SCAMS

Tech support scams prey almost exclusively on older consumers, many of whom lack confidence when it comes to their computers. Like most scams, tech support operations use robocalls, but they also send email, computer popups and texts to hook victims. Regardless of the channel, the approach is always the same: get the fraud target worried about the status of their computer so they can sell you unnecessary repairs, or worse, remote access into your computer to hack into your accounts. Here is an example.

THE PITCH:

Hi This is Tony calling you from Cal Tech. This is about your computer. You may have a dangerous virus.
I can help you fix this.

FRAUD FIGHTER PRO TIP:

Any time you receive a message, whether it's a robocall, a popup on your computer or a text message, telling you there might be a virus on your computer, do not respond directly, don’t click on a link or press "1" to talk to someone or reply to an email. Instead, ask a trusted friend who might be more familiar with computers if they could come look at it.

Another alternative is to take it to a store front like the Geek Squad at Best Buy or a local repair shop. Under no circumstances should you ever allow a stranger who called you to remote access into your computer. That is simply asking for trouble.

SOCIAL SECURITY ROBOCALL SCAM

Robocall scammers are criminals who have no credibility whatsoever. They hide behind entities that do have credibility like the Social Security Administration, Medicare, the FBI, the US Customs and Border Patrol. Here is an example.

THE PITCH:

This call is from the Social Security Administration. Your social security number is going to be suspended in the next 24 hours for committing some suspicious and fraudulent activities in the state of Texas. Call me back as soon as possible.

FRAUD FIGHTER PRO TIP:

Americans across the country receive calls like this every day. Scammers claim hackers have stolen their Social Security cards or fake US Customs agents call and claim the fraud target's name was on a box seized by drug agents. These scare tactics are increasing as the world seems to be more on edge and people are more anxious. Remember that being in a heightened emotional state plays to the the scammer's advantage because it makes us less able to think rationally about what we are being told. If you receive a call like this, hang up and contact the Social Security Administration 1 (800) 772-1213 and ask them if there is an issue. The worst thing you can do is stay on the line with these people.

GRANDPARENTS ROBOCALL SCAM

The grandparent scam is another swindle that has many different entry points. We have heard reports of scammers roaming Facebook looking for older persons who have not changed their privacy settings so only family and friends can see their postings. Consequently, complete strangers with ill intentions can see postings of one's children and grandchildren, their names, ages, activities, so it makes it easy work to call and pose as one of them. Other scammers will simply make thousands of phone calls hoping they reach an older person and can convince them they are a grandchild in trouble. Here is an example.

THE PITCH:

Hi Grampa. Its your grandson. I'm in trouble. I got into a car accident last night and hit a pregnant lady. I'm in jail and need you to bail me out. Can you help me?

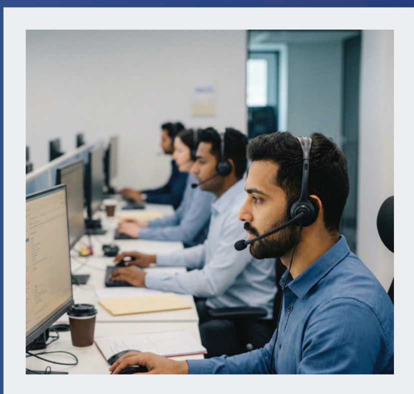
FRAUD FIGHTER PRO TIP:

One way to verify if the person calling is really your granddaughter or grandson is to ask them a question only they know the answer to such as "What was the name of your first pet?" Another way to verify who is calling is to tell them to hang up and they will call back the grandson (or the grandson's parent) on his cell phone. Ultimately, these scammers are hoping the fraud target will not stop to question the caller and simply act by wiring money for bail. Don't take the bait!

MEDICARE CARD ROBOCALL SCAM

The single largest percentage of all robocalls flowing into America's phone lines are related to Medicare. Most of them are trying to sell Medicare Gap or Medicare Advantage supplement insurance. But there are several Medicare robocalls that are straight up scams. The Medicare Card replacement scam is one of them. Here is an example.

THE PITCH:



This is Jack from The US Medical Department. Our records show that your paper red white and blue Medicare card has been deactivated for security reasons. I'd like to send you a replacement. Can I have your Medicare number?

FRAUD FIGHTER PRO TIP:

These types of calls are all scams - period. Investigators who have fielded these calls have played along with the scammer. Some even ask what will happen if they don't give them their Medicare number. The scammers' answer? You will not be able to use your card, and Medicare will no longer pay any of your medical bills. Talk about a threat of loss! Of course, none of it is true and the scammer simply hopes to collect your personal identifying information so they can either use it to steal your identity or to place a false claim with Medicare using your account credentials. If you receive such a call, hang up. If you are concerned about the status of your Medicare account, contact Medicare directly at **1 (800) Medicare (633-4227).**

ONLINE PURCHASE ROBOCALL SCAM

Job one for scammers is to gain the fraud target's trust. What better way to do that than to pose as Amazon or Microsoft or your phone company. Here is an example of a very common business impostor scam.

THE PITCH:

> *This is Amazon Security. You have been charged $1,279.99 on your default card saved on Amazon.com. If you have not made this transaction, someone may have hacked into your account. To talk to customer care, press 1.*

FRAUD FIGHTER PRO TIP:

This example has the scammer posing as Amazon and trying to instill fear into the mind of the fraud target that someone has gotten into their account. Often, they will claim you need to remove all your money from the bank to avoid hackers stealing it. They steer victims to the nearest Bitcoin ATM and have them deposit the money and convert it to Bitcoin so the hacker can't steal it. Instead, they steal it from your Bitcoin account. The best thing to do is to delete these types of messages and do not talk to the person on the other end of the line. If you are concerned about your account, independently log onto your Amazon account or call your bank using the number on one of your statements to make sure there are no issues.

ROMANCE SCAMS

Romance scammers prey on individuals who are lonely and seek companionship from others. They use various communications platforms to lure unsuspecting victims. It can be a phone call, a text, a dating app or a social media invitation. Typically, the message is from a very attractive man or woman. Here is an example of a message found on Facebook that was a scammer seeking victims.

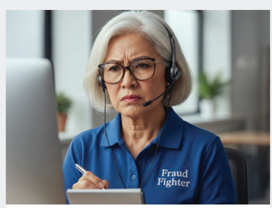
THE PITCH:

> *I saw your profile on Facebook and I'd like to meet you.*

FRAUD FIGHTER PRO TIP:

In this example, the scammer hopes the fraud target responds and is willing to engage. She pretends to fall in love with the target by showering him (or her) with praise and love, a tactic known as "love bombing". Once the scammer succeeds in winning the heart and mind of the fraud target, they will either 1) claim they need to borrow money because their business is experiencing trouble or 2) they will invite them to invest in Bitcoin so they can make a lot of money in a short amount of time.

The scammer may be willing to engage with a fraud target for months before they ask for money. Older persons reported losing $329 million dollars to romance scams in 2025. Beware of individuals who reach out to you unsolicited and immediately claim you are the one they have been looking for their whole life. It's nothing more than a time-tested ruse to steal your money.



SWEEPSTAKES ROBOCALL SCAM

The fake sweepstakes prize scams have been around for many years in various forms, but unfortunately, they still persist today. And research has shown that while anyone of any age can lose money to a scam, older persons are more likely to lose money to a prize scam than younger people. Here is an example.

THE PITCH:

On behalf of Publisher's Clearinghouse, you have been selected as the winner of our grand prize: a cash award of $5,500,000, a 2026 Mercedes Benz and $7,000 for life. Congratulations!!

FRAUD FIGHTER PRO TIP:

Scammers have been pretending to be Publisher's Clearinghouse to perpetuate their scams for decades, but that's not the only company or agency scammers use. They have also been known to pose as Reader's Digest, the Federal Trade Commission, the FBI, and even AARP. Any time you receive a call proclaiming that you won millions of dollars, hang up immediately.

UTILITY ROBOCALL SCAM

The scammer poses as someone from your utility company - either phone, gas, electric or cable TV - and offers to provide a discount and/or give you an upgrade on your router so your TV will work better. This may involve giving them the password to your WIFI or other personal identifying information. Here is an example:

THE PITCH:

This is David and I'm calling from your TV services. We are running a senior citizen promotion and offering a 40-50% discount off your TV bill monthly. You paid your bill on time every month and are a senior so you are eligible. Can I start the process?

FRAUD FIGHTER PRO TIP:

The calls flooding into American homes offer the promise of saving money, but the reality is they are attempts to get you to spend money or to steal your identity under the guise of saving money. We have seen scammers posing as representatives from Spectrum, AT&T, Xfinity, PG&E and many more. If you receive a call from a utility company saying that because you are a senior citizen or because you pay your bill on time every month, you are entitled to a 30-50% discount, don't believe it. It's a scam. There are also many robocallers trying to sell solar panels by claiming it can reduce your electric bill by hundreds of dollars each year. It is best to avoid engaging with these callers. If you are interested in exploring the use of solar panels, it is best to contact your utility company directly and ask if they recommend any vendors who provide such products.

RESOURCES

Here are some resources for Fraud Fighters:

AARP FRAUD WATCH NETWORK

The AARP Fraud Watch Network Helpline has trained volunteer fraud experts who can answer any questions you have about fraud. For more fraud resources, go to

AARP.org/fraudwatchnetwork

Call 1877-908-3360.

CHECK OUT A CHARITY

Visit to find out if a charity is registered before giving.

Charity Navigator.org

FRAUD PREVENTION STRATEGIES, LLC

is a Seattle-Based Consulting Firm, directed by former Attorney General fraud investigator and AARP State Director Doug Shadel. They offer public speaking and expert witness testimony. For more information, contact:

Doug@fraudpreventionstrategies.com.

NATIONAL DO NOT CALL REGISTRY

You can sign up for the Do Not Call List to reduce the number of spam and scam attacks you receive. It is administered by the Federal Trade Commission and once you are on the list, legitimate telemarketers must refrain from calling you. Go to

https://www.donotcall.gov

to sign up or **Call 1-888-382-1222.**

NOMOROBO.COM APP

The Nomorobo call blocking app will virtually eliminate unwanted spam and scam robocallers. Go to

www.nomorobo.com

to download the app today.

STOP SPAM MAIL

To decide what types of mail you do and don't want from marketers, register at the Association of National Advertisers' (ANA) website

DMAchoice.org

and choose what catalogs, magazine offers, and other mail you want to get. DMAchoice will stop most, but not all, promotional mail. You'll have to pay a **$6 processing fee,** and your registration will last for **10 years.**

YOUR ATTORNEY GENERAL'S OFFICE

To file a complaint against a scammer, look up your nearest AG office by logging on to

https://www.naag.org/find-my-ag/.

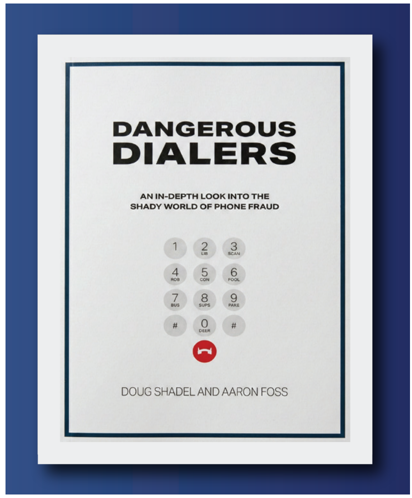
YOUR FEDERAL TRADE COMMISSION OFFICE

To file a complaint with the Federal Trade Commission, log onto

https://reportfraud.ftc.gov/.

NEW BOOK FOR FRAUD FIGHTERS

DANGEROUS DIALERS



If you have enjoyed the examples in this booklet, the new book **Dangerous Dialers** is a must-read. Drawing on interviews with informants, cyber police, former convicted scammers, and millions of undercover audio recordings, fraud experts **Doug Shadel and Aaron Foss**, teach you everything about phone scams and offer a set of tools for anyone wishing to arm themselves against these attacks. Inside you'll find:

REAL LIFE EXAMPLES

of how AI and other technologies are used to spoof calls and deceive victims.

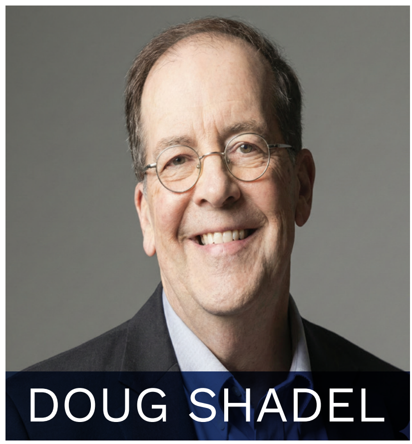
UNDERCOVER RECORDINGS

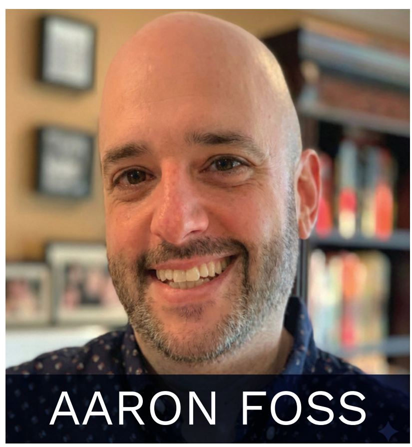
of investigators posing as victims to expose scammers.

THE "HALL OF SHAME

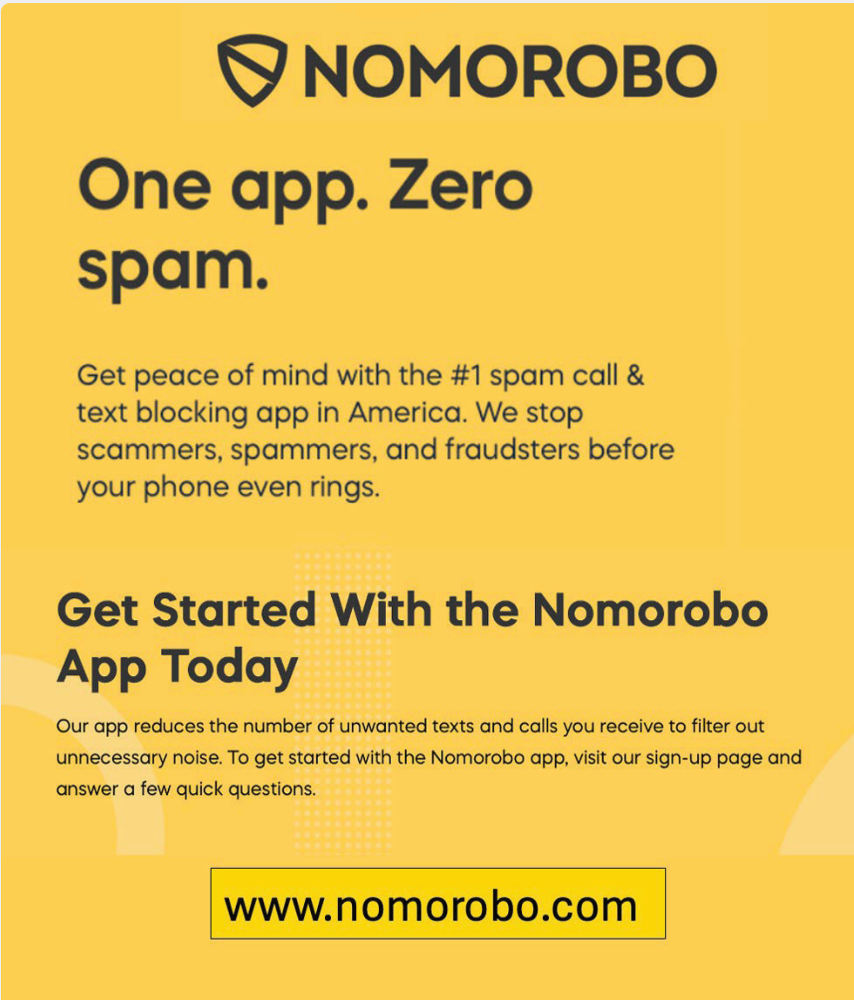
collection of 150 of the most common (and dangerous) scam recordings.

Join the ranks of thousands of fraud fighters nationwide who are not just protecting themselves from these scams but are also watching out for and reporting them to authorities. Available at **Amazon.com or your favorite bookstore.**





THE ULTIMATE TOOL TO BLOCK UNWANTED ROBOCALLS



YOUR FRAUD FIGHTER GUIDE

Consumer fraud complaints have increased dramatically in recent years, with losses in the billions of dollars. Older consumers have been especially hard-hit, with annual losses as high as $80 billion a year according to the Federal Trade Commission.

This Fraud Fighter Guide provides older persons with a set of tools they can use to defend against this epidemic of malicious attacks and join the ranks of "Fraud Fighter" with thousands of others.

Inside you will learn how to:

- Spot persuasion tactics employed by scammers
- Adopt a "Fraud Fighter" Mindset
- "Harden the Target" to block incoming scam attacks
- Learn how professional Fraud Fighters respond to scam calls.

NOMOROBO

FRAUD PREVENTION STRATEGIES LLC
EST. 2022