A PLAIN-ENGLISH PRACTICAL GUIDE

Scams and Identity Theft

How to Protect Yourself and Recover



How to Protect Yourself and Recover

Andrew Dominguez

Trinfinity Enterprises

Scams and Identity Theft

How to Protect Yourself and Recover

Andrew Dominguez

Trinfinity Enterprises

Scams and Identity Theft: How to Protect Yourself and Recover

Copyright 2026 by Andrew Dominguez.

Free to download. All rights reserved.

No part of this book may be reproduced, distributed, or transmitted in any form or by any means without written permission from the publisher, except for brief quotations in reviews. You are welcome to download this book and read it for free at trinfinityenterprises.com.

Independently published. First edition, 2026.

Trinfinity Enterprises, Dayton, Nevada.

Questions and corrections: andrew@trinfinityenterprises.com

Please read before you use this book. This book is for general information and education only. It is not legal, medical, financial, tax, or other professional advice, and reading it does not create a professional relationship of any kind. Laws, rules, prices, and research change, and every situation is different. Before you act on anything in this book, check it against current sources and talk with a lawyer, doctor, licensed professional, or other qualified expert as your situation calls for. I worked hard to get the facts right, but I can't promise that every detail is complete, correct, or current. You use this information at your own risk. To the fullest extent the law allows, Andrew Dominguez, Trinfinity Enterprises, and Andrew Dominguez's heirs, estate, successors, and assigns accept no responsibility or liability for any loss, injury, or damage of any kind that comes from using or relying on this book.

Legal notice. I am not a lawyer. This book explains laws, court cases, and government processes in plain words for general learning. It is not legal advice and does not create an attorney-client relationship. Laws change, courts read them differently, and the rules in Nevada or at the federal level may not match the rules where you live. For any legal question about your own situation, including firearms, self-defense, elections, immigration, property, or criminal matters, talk with a lawyer licensed in your state, and check official government sources for current forms and deadlines.

Money notice. I am not a financial adviser, accountant, tax preparer, or attorney. This book is general information about money. It is not investment, tax, insurance, or financial advice, and it is not a recommendation to buy or sell anything. Tax laws, rates, and limits change every year. Talk with a licensed financial professional, certified public accountant (CPA), or tax attorney before you make decisions about your own money, taxes, retirement, insurance, or debt.

Contents

Before You Begin....1
Chapter 1: The Size of the Problem....3
Chapter 2: The Four Signs of a Scam....5
Chapter 3: Government and Business Imposters....8
Chapter 4: The Family Emergency Scam....11
Chapter 5: Romance Scams....13
Chapter 6: Investment and Cryptocurrency Scams....15
Chapter 7: Prizes, Jobs, Shopping and Rentals....17
Chapter 8: At the Door and in the Mail....19
Chapter 9: Phones, Texts and Email....21
Chapter 10: Protecting Your Identity....23
Chapter 11: Freeze Your Credit....25
Chapter 12: If You Were Scammed: The First 24 Hours....28
Chapter 13: Recovering From Identity Theft....30
Chapter 14: Protecting an Older Parent....32
Chapter 15: Where to Report....34
Scam Warning Signs Checklist....36
My Real Numbers Worksheet....37
Sources....38
About This Book....39

Before You Begin

Almost everyone I know has gotten the call, the text or the email. A voice says your Social Security number has been suspended. A text says a package could not be delivered. A message from a "bank" says someone tried to use your card and you need to verify your account right now. Most of us hang up or delete it. But scammers do not need most of us. They need the one person who is tired, worried or caught off guard on a busy day, and every one of us has days like that.

This book is about how to spot a scam before it costs you, how to protect your identity so a thief cannot use it, and exactly what to do if the worst happens. It covers phone, text, email, mail and in-person scams, and it walks you through the official recovery steps from the Federal Trade Commission (FTC), step by step.

Who This Book Is For

It is for anyone with a phone, a bank account or a mailbox. It is especially for older adults and for the people who look out for them. If you have a parent or grandparent who lives alone, Chapter 13 is written for you.

How to Use This Book

Each chapter covers one kind of scam or one step in protecting yourself. Each ends with a short "Do This Now" box: one thing you can do in about ten minutes to make yourself harder to fool. At the back you will find a one-page warning signs checklist to post by the phone, a worksheet for listing the phone numbers of your bank and card companies, and the official places to report fraud.

The Most Important Rule in This Book If anyone contacts you out of the blue and pressures you to pay, to share a code, or to keep it secret, stop. Hang up, close the message, and contact the company or agency yourself using a number you already know is real. No real bank, agency or family emergency is hurt by a five-minute pause to check.

Where the Facts Come From

The numbers and advice in this book come from official sources such as the Federal Trade Commission, the FBI's Internet Crime Complaint Center, the Social Security Administration, the IRS, the U.S. Department of Justice and the Nevada Attorney General, checked as of November 18, 2026. They are listed at the back of the book. Scams change constantly, so the official websites named in this book are the best place to check for the newest tricks.

No Shame

If you have been scammed, you are not stupid, and you are not alone. Scammers are professionals. They practice their scripts, study their targets, and use fear, love and hope against people. The people who recover best are the ones who report it quickly and ask for help. This book will show you how.

Chapter 1: The Size of the Problem

Scams are not a small problem, and they are getting worse. The Federal Trade Commission collects reports from people who have been targeted. In June 2026 it reported that people said they lost about $16 billion to fraud in 2025, the highest amount on record and about 25 percent more than in 2024.

Those are only the losses people reported. Most people never report a scam, out of embarrassment or because they do not know where to go. The real total is much higher.

Older Adults Are Losing the Most per Person

In its October 2026 report to Congress, the FTC said reported fraud losses among adults 60 and older grew from about $600 million in 2020 to about $3 billion in 2025. Much of that growth came from a small number of people who lost extraordinarily large amounts, often their life savings. Older adults' reported losses to investment scams rose 42 percent in 2025, to more than $1 billion, and many of those scams first reached people on social media. The FTC also estimated that when unreported losses are counted, the total cost of fraud to older adults in 2025 could have been as high as $119.5 billion.

The same report said older adults were more likely than younger adults to report losing money to tech support scams, prize and lottery scams, romance scams, government impersonators and family impersonators. Each of those gets its own chapter in this book.

Imposters Lead the List

The most common kind of fraud reported to the FTC is the imposter scam, where someone pretends to be someone you trust. Nearly one

in three fraud reports in 2025 were about imposters, and people reported losing $3.5 billion to them, nearly three times as much as in 2020. Business imposters, most often fake bank fraud departments, took nearly $1 billion. Government imposters took about $920 million.

Why Scams Work Scammers do not win because people are foolish. They win because they are good at getting past our defenses: they create a crisis, they sound official, they use our love for family, and they rush us so we do not stop to think. Knowing their playbook is the best defense.

How This Book Is Organized

Chapters 2 through 9 cover the most common scams and how to spot them. Chapters 10 and 11 cover protecting your identity and freezing your credit. Chapters 12 through 15 cover what to do if you have been scammed or your identity has been stolen, how to protect an older parent, and where to report fraud.

Do This Now Write the main phone number for your bank and for each credit card company on the worksheet at the back of this book, copying it from the back of your card or a statement. When something seems wrong, that is the number you will call.

Chapter 2: The Four Signs of a Scam

Scams come in hundreds of costumes, but almost all of them follow the same script. Learn the script, and you can spot a new scam even if you have never heard of it before.

The Federal Trade Commission boils it down to four signs. In its own words: “Scammers PRETEND to be from an organization you know.” “Scammers say there’s a PROBLEM or a PRIZE.” “Scammers PRESSURE you to act immediately.” “Scammers tell you to PAY in a specific way.” Here is what each one looks like in real life.

Before the Signs: A Contact You Did Not Expect

Most scams start with a contact you did not ask for: a phone call, a text, an email, a social media message, a pop-up on your computer, or a knock at the door. Real problems with your bank, the government or a family member do sometimes start this way. That is exactly why scammers use it. The answer is not to panic. It is to check, using a number or website you already know is real.

Sign 1: They Pretend to Be Someone You Trust

The caller says they are from Social Security, the IRS, your bank, Amazon, Microsoft, the sheriff’s office, the power company or your grandson. Caller ID can be faked to show any name or number. Emails and texts can copy a company’s logo exactly. A real-looking caller ID or logo proves nothing.

Sign 2: A Problem or a Prize

There is a problem: your account was hacked, your Social Security number was used in a crime, there is a warrant for your arrest, your power will be shut off in an hour, your grandson is in jail. Or there is

a prize: you won a lottery, you qualify for a grant, an investment will double your money. Either way, the goal is the same, to get you emotional so you stop thinking clearly.

Sign 3: Pressure to Act Now

They say you must act now. They tell you not to hang up, not to tell anyone, not even your bank or family. The FTC's advice is simple: "Resist the pressure to act immediately," and "Stop and talk to someone you trust."

Sign 4: A Specific Way to Pay

They tell you to pay in a way that is hard to trace or reverse. The FTC names these: cryptocurrency, a wire transfer through a company like MoneyGram or Western Union, a payment app, or a gift card, where they ask you to read them the numbers on the back. Another version sends you a check, asks you to deposit it and send part of the money back. The check later turns out to be fake, and you owe the bank the full amount.

> **The Payment Rule** No real government agency or bank will demand that you pay by gift card or cryptocurrency, move your money to "protect" it, or hand cash or gold to someone who comes to your door. If anyone asks you to pay that way, it is a scam. Every time.

The Fake Security Alert

One of the costliest scams today combines all four signs. The FTC warns that "some of the costliest impersonation scams start with a fake security alert, often from a bank." You get a text or call saying there is suspicious activity on your account. Then a "fraud investigator" calls, sounds professional, knows some of your information, and says your money is in danger. To "protect" it, you

are told to move it to a “safe account,” withdraw it in cash for a courier, or buy gold. Every dollar goes to the scammer. The FTC says plainly that it “will never threaten you, say you must transfer your money to ‘protect it,’ or tell you to withdraw cash or buy gold and give it to someone.” Neither will your bank.

Do This Now Practice your exit line out loud: “I don’t do business on calls I didn’t make. I’ll call you back at the number on my card.” Then hang up and call the real number.

Chapter 3: Government and Business Imposters

The most common scam in America is someone pretending to be someone you trust. In 2025, people told the Federal Trade Commission they lost nearly $1 billion to business imposters, most often fake bank fraud departments, and about $920 million to government imposters.

Fake Government Agencies

The caller says they are from Social Security, the IRS, Medicare, the FBI, the sheriff's office or the court. The story varies: your Social Security number was used in a crime, you owe back taxes, there is a warrant for your arrest, you missed jury duty, or your benefits will be cut off. The answer is always the same: pay now, in a way that cannot be traced, and do not hang up.

Here is what the real agencies say about how they contact you.

- **Social Security.** "Social Security will never ask for sensitive or personal information through social media, email, or text message." Its scam page lists the payment demands that mark a scam: gift cards, gold or silver, prepaid debit cards, wire transfers, cryptocurrency, or mailing cash. It also warns that "legitimate companies and other agencies cannot transfer your phone call directly to SSA or OIG," so a caller who offers to transfer you to Social Security is a scammer.
- **The IRS.** "We normally contact you the first time by mail delivered by the U.S. Postal Service." The IRS emails or texts only if you signed up for it, and "a social media direct message is never from us." "Unannounced visits are rare." A call, email or text is not from the IRS if it is unexpected, rushes you, threatens

you, asks for personal or financial information, or demands payment now.

- **Law enforcement.** Social Security's inspector general warns that federal law enforcement "will never send photographs of credentials or badges to demand any kind of payment." No real officer collects a fine or bail over the phone.

Fake Banks and Fraud Departments

A text says a large purchase was made on your card: "Reply YES or NO." When you reply, you get a call from the "fraud department." The caller knows your name and maybe part of your card number. They say your account has been hacked and walk you through "protecting" your money: moving it to a new account, reading them a code that was just texted to you, or withdrawing cash for a courier.

The code is the key. When a real company texts you a one-time code, it is to prove that you are the one logging in or making a change. Anyone who asks you to read that code back to them is trying to get into your account.

> **Never Share a Code** A real bank, store or agency will never call you and ask you to read back a security code that was sent to your phone. If someone asks, hang up.

Fake Tech Support

A pop-up on your computer flashes a warning, sometimes with a loud alarm, saying your computer is infected and you must call a number right away. Or someone calls claiming to be from Microsoft, Apple or your internet company. They ask you to let them connect to your computer, then "find" problems and charge you to fix them, or use the access to get into your bank account.

Real tech companies do not call you out of the blue about viruses, and their real warnings do not tell you to call a phone number.

Fake Utility Shutoffs

A caller says your power or water will be shut off within the hour unless you pay right now. Real utilities send written notices before a shutoff. If you get a call like this, hang up and call the number on your bill.

Fake Package and Toll Texts

A text says a package could not be delivered, or you owe an unpaid toll, and gives you a link. The link leads to a fake site that steals your card number. If you are expecting a package, check it on the shipper's real website or app, typed in yourself.

> **Do This Now** Look up your bank's real fraud department number on the back of your card and save it in your phone under a clear name like "BANK - REAL NUMBER." When something seems wrong, call that number yourself.

Chapter 4: The Family Emergency Scam

The phone rings late at night. A young voice says, “Grandma, it’s me. I’m in trouble.” There has been a car accident, or an arrest, or a hospital bill in another country. They need money right now for bail or a lawyer, and they beg you not to tell Mom and Dad. Sometimes a second person comes on the line, a “lawyer” or “police officer,” who explains how to pay.

This is the family emergency scam, often called the grandparent scam. The Federal Trade Commission describes it simply: “Someone calls or contacts you saying they’re a family member or close friend. They say they need money to get out of trouble.” Then it asks the right questions: “Is there really an emergency? Is that really your family or friend calling? It could be a scammer.”

Why It Works

It works because it uses love against you. You hear a loved one in trouble, and every instinct says help first and ask questions later. The scammer counts on that. The plea for secrecy keeps you from making the one phone call that would end the scam.

The Voice May Sound Real

Scammers sometimes find a few seconds of a family member’s voice in a video posted online and use artificial intelligence to copy it. The FTC has warned that “scammers use voice cloning to make their requests for money or information more believable.” So even if the voice sounds exactly right, that does not prove it is your grandson.

How to Stop It

1. Slow down. A real emergency can survive a five-minute check.

2. Hang up and call the person directly at the number you already have for them. If they do not answer, call their parent, spouse or another family member.

3. Ask a question only the real person would know, something that is not on social media.

4. Never send money by gift card, wire, cryptocurrency or cash to a courier because a caller told you to. A real lawyer or jail does not collect bail that way.

5. Ignore the request for secrecy. Telling someone is exactly what the scammer fears.

A Family Code Word Many families agree on a code word or phrase that a family member would use in a real emergency. Pick one that is not posted anywhere online, share it in person, and make sure older relatives know it. If a caller cannot give the code word, hang up and call your family directly.

Do This Now Call or visit the older relatives in your family this week and tell them about this scam. Agree on a code word. That one conversation may save them thousands of dollars.

Chapter 5: Romance Scams

Romance scams are some of the cruelest, because they take money and trust at the same time. The FTC's October 2026 report to Congress listed romance scams among the frauds where older adults were more likely than younger adults to report losing money.

How They Work

It starts with a friendly message on a dating site, social media or even a wrong-number text. The person is attractive, attentive and kind. They write every day. Within weeks they are saying "I love you." But there is always a reason they cannot meet in person or turn on a video call: they work on an oil rig, they are a doctor overseas, they are deployed with the military.

Then comes the first request for money. A plane ticket so they can finally visit. A customs fee. A medical bill. A business problem. Once you send money, the requests grow. Some scammers move on to "investment" pitches, telling you they have made a fortune in cryptocurrency and want to help you do the same.

The FTC sums up the scammer's lies in three lines: "Scammers say they can't meet you in person." "Scammers will ask you for money." "Scammers will tell you how to pay."

Warning Signs

- They profess love quickly.
- They always have a reason they cannot meet or video chat.
- They ask you to move the conversation off the dating site to a private messaging app.
- They ask for money, gift cards or cryptocurrency, or offer to teach you to invest.

- They ask you to keep the relationship secret from family and friends.

What to Do

The FTC's rule is simple: "Never send money or gifts to a sweetheart you haven't met in person." If you think it may be a scam, stop communicating with the person. Talk to a friend or family member you trust; scammers try to isolate you because outsiders see the warning signs clearly. You can also do a reverse image search of the person's profile photo to see whether it appears under other names. If you already paid, contact your bank or the payment company right away, report it at ReportFraud.ftc.gov, and report the profile to the dating site or app.

If It Is Someone You Love If a parent or friend is caught in a romance scam, be gentle. Shame drives people deeper into the scam. Listen first, then share what you know about how these scams work, and offer to help them check.

Chapter 6: Investment and Cryptocurrency Scams

Investment scams cause some of the largest losses of any fraud. The FTC reported that older adults' losses to investment scams jumped 42 percent in 2025 to more than $1 billion, and that people often said the scammers first reached them on social media.

How They Work

An ad, a social media post or a new online friend promises big, safe returns, often in cryptocurrency, gold or foreign currency trading. You are shown a professional-looking website or app where your "account" grows quickly. You may even be allowed to withdraw a small amount at first, to build trust. Then you invest more. When you try to take out your money, there are suddenly fees, taxes or "verification" payments to make, and then the site disappears.

Warning Signs

- Promises of high returns with little or no risk.
- Pressure to invest quickly before the "opportunity" closes.
- Investment advice from someone you met online or through a wrong-number text.
- Being told to pay in cryptocurrency or to send money to a crypto platform the other person picked.
- A request to pay fees or taxes before you can withdraw your own money.

Protect Yourself

Before you invest, check that the person and the firm are registered. The Financial Industry Regulatory Authority's BrokerCheck and the Securities and Exchange Commission's Investor.gov let you look up brokers and advisers. Talk to someone you trust who is not

involved. And remember that no legitimate investment guarantees high returns with no risk.

Do This Now Make a rule for yourself: you will never invest money with anyone you met online, and never send cryptocurrency to anyone who contacted you first.

Chapter 7: Prizes, Jobs, Shopping and Rentals

Some scams start with good news instead of bad.

Prizes, Sweepstakes and Lotteries

You have won a lottery, a sweepstakes or a new car. All you have to do is pay the taxes or a processing fee first. The FTC's 2026 report to Congress listed prize, sweepstakes and lottery scams among those where older adults were more likely to report losses. A real prize never requires you to pay to collect it. If you did not enter, you did not win.

Job Scams

A message offers easy work from home: reshipping packages, "reviewing" products online, or a job with great pay after a short text interview. Then you are asked to pay for training or equipment, or you are sent a check to deposit and asked to send part of it back. The check bounces days later, and you owe the bank. Real employers do not ask you to pay to get a job or to send money back from a paycheck.

Online Shopping

A website or social media ad offers a popular item at a price too good to be true. You pay, and nothing arrives, or what arrives is junk. Before buying from a site you do not know, search the company's name with words like "scam" or "complaint." Paying by credit card gives you the strongest right to dispute a charge if the item never comes.

Rentals and Pets

A rental listing shows a beautiful home at a low price, but the "owner" is out of the country and asks for a deposit before you can see it. A puppy for sale needs a shipping fee, then an insurance fee, then a crate fee. Never pay a deposit for a rental you have not seen in person, and never pay for a pet you have not met.

Do This Now If something you are about to buy or pay for online makes you feel rushed or excited, wait one full day before you pay. Scams rarely survive a night's sleep.

Chapter 8: At the Door and in the Mail

Not every scam comes through a screen. Some knock on the door.

Home Repair Scams

A crew shows up saying they just finished a job down the street and have leftover materials. They can fix your roof or pave your driveway today, for cash, at a great price. The work is poor or never finished, and the crew disappears. In Nevada, contractors are licensed by the Nevada State Contractors Board, and you can check a license before you hire. Get written bids, check the license, and never pay in full up front.

Fake Officials at the Door

Someone in a uniform or with a badge says they are from the gas company, the water department or a government agency and need to come inside or collect a payment. Ask for identification, keep the door closed, and call the company or agency at a number you look up yourself before letting anyone in.

Mail Scams

Mail scams include fake prize notices, fake checks, letters that look like official bills or government notices, and fake charity appeals. Look closely at who the letter is really from. Real government notices come from the agency itself, and you can call the agency at its published number to confirm.

Protect Your Mailbox

Thieves steal checks and bank statements from mailboxes and change the amounts on checks. Pick up your mail promptly, use a locking mailbox if you can, and drop outgoing checks inside the post office rather than leaving them in your box with the flag up.

Do This Now Put a note by your front door: "I never pay for work or let anyone in on the spot. I'll call to check and get back to you."

Chapter 9: Phones, Texts and Email

Most scams reach people through their phone or inbox. A few settings and habits cut down on how many get through.

Calls

- Let calls from numbers you do not know go to voicemail. A real caller will leave a message.
- Use the call-blocking and spam-filtering tools your phone and phone company offer. The FTC recommends blocking unwanted calls.
- Remember that caller ID can be faked. A call that shows your bank's name, or even your own number, can still be a scam.
- Never press a number to "be removed from our list." It tells the scammer your number works.

Texts

- Turn on your phone's filter for texts from unknown senders, as the FTC recommends.
- Do not tap links in texts you did not expect, even if they look like they come from a bank, a shipper, a toll road or a government agency.
- Do not reply, even with "STOP," to a text that looks like a scam. Delete it, and report it if you want to (Chapter 15).

Email

- Look at the actual sender address, not just the name. "Amazon Support" may be writing from a random address.
- Do not open attachments or click links in emails you did not expect. Go to the company's website by typing it yourself.
- Turn on two-step verification for your email account. Your email is the master key to all your other accounts, because that is where password resets go.

Social Media

Keep your profiles private, and be careful what you share. Birthdays, pet names, high schools and family names are common answers to security questions, and they help scammers sound like they know you. Be wary of friend requests from people you are already friends with; it may be a copied account.

> **Do This Now** Turn on spam call blocking and unknown-sender text filtering on your phone today. If you are not sure how, ask your phone company or a family member to help.

Chapter 10: Protecting Your Identity

Identity theft happens when someone uses your personal information, such as your name, Social Security number, bank account or credit card number, to open accounts, get loans, file tax returns, get medical care or commit crimes in your name. You cannot make yourself impossible to rob, but you can make yourself a much harder target.

Guard Your Social Security Number

Your Social Security number is the most valuable piece of information a thief can get. Do not carry your card in your wallet. When a form or an office asks for your number, ask why they need it and how they will protect it. Many do not really need it.

Strong Passwords and Two-Step Verification

Use a different password for each important account, especially email, banking and shopping. A password manager can remember them for you. Turn on two-step verification wherever it is offered, so that a thief who steals your password still cannot get in without the code sent to your phone.

Watch Your Accounts

- Read your bank and credit card statements every month, or turn on alerts that text or email you for every charge.
- Check your credit reports. You can get free reports from all three bureaus at AnnualCreditReport.com, the official site.
- Read the “Explanation of Benefits” statements from Medicare or your health insurer. A bill for care you never got can be a sign of medical identity theft.

Paper and Devices

- Shred papers with account numbers or your Social Security number before throwing them away.
- Keep your computer and phone updated, since updates fix security holes.
- Be careful on public Wi-Fi. Avoid logging in to your bank on a coffee shop network.

Do This Now Turn on two-step verification for your email and your bank today, and freeze your credit (Chapter 11).

Chapter 11: Freeze Your Credit

If you do only one thing after reading this book, freeze your credit. It is free, it takes about fifteen minutes online, and it is one of the strongest protections there is against a thief opening new accounts in your name.

What a Credit Freeze Does

When someone applies for a credit card, a loan or a phone account in your name, the lender almost always checks your credit report with one of the three nationwide credit bureaus: Equifax, Experian and TransUnion. A credit freeze locks that report. While it is in place, lenders cannot see it, so a thief who has your name, birth date and Social Security number still cannot open new credit in your name.

According to the Federal Trade Commission:

- "There's no cost to place or lift a credit freeze."
- A freeze "lasts until you lift it."
- You have to contact all three bureaus, because each keeps its own report.
- You do not need to be a victim of identity theft to freeze your credit. Anyone can.

What a Freeze Does Not Do

A freeze does not stop you from using the credit cards and loans you already have. It does not stop scammers from tricking you into sending money, and it does not protect bank accounts you already own. That is why the rest of this book still matters.

When You Need New Credit

When you apply for a loan, a new card, a mortgage, or sometimes a new phone or apartment, you lift the freeze, for a short time or for one lender, then put it back. Ask the lender which bureau it uses, and you may only need to lift that one. Each bureau gives you a PIN or an online account for this. Keep it with your important papers.

How to Freeze Your Credit

Contact each bureau. The FTC links to these pages:

Bureau	Where to freeze online
Equifax	equifax.com/personal/credit-report-services
Experian	experian.com/help
TransUnion	transunion.com/credit-help

Type the address yourself rather than clicking a link in an email or text, since scammers copy the look of real websites.

Fraud Alerts

A fraud alert is a lighter tool. It does not lock your report. It tells lenders to take extra steps to confirm it is really you before opening an account.

Type	How long it lasts	What you need
Initial fraud alert	One year, and you can renew it	Free. Contact one bureau, and it must tell the other two.
Extended fraud alert	Seven years	An FTC identity theft report or a police report. It also takes you off prescreened marketing lists for five years.
Active duty alert	One year	For service members on active duty.

Many people use both: a freeze to stop new accounts, and an extended fraud alert after an identity theft.

Do This Now Freeze your credit at all three bureaus today. Write your PINs or account logins on a card and store it with your important papers, not in your wallet.

Chapter 12: If You Were Scammed: The First 24 Hours

If you have sent money or shared information with a scammer, act fast. The sooner you move, the better your chance of stopping the money or limiting the damage. Do not let embarrassment slow you down.

Step 1: Stop Contact

Stop talking to the scammer. Do not answer their calls or texts. They will often come back with a new story, sometimes posing as someone who can "recover" your lost money for a fee. That is a second scam.

Step 2: Contact Whoever Moved the Money

How you paid decides who to call first.

If you paid with	Call right away
Credit or debit card	Your card company, at the number on the back of your card. Ask to dispute the charge and get a new card.
Bank transfer or wire	Your bank, and ask it to try to reverse the transfer. For a wire through a company like Western Union or MoneyGram, call that company too.
Gift card	The company that issued the gift card. Tell them it was used in a scam and ask if they can freeze or refund it. Keep the card and the receipt.
Payment app	The app company, and your bank or card linked to the app.
Cryptocurrency	The company you used to send it. Crypto payments usually cannot be reversed, but report it right away.
Cash by mail or courier	The U.S. Postal Inspection Service if mailed, and local police.

Step 3: Secure Your Accounts

If you gave the scammer a password, change it, and change it anywhere else you used the same one. If you let someone connect to your computer, disconnect it from the internet, run your security software, and consider having it checked by a trusted repair shop. If you shared your Social Security number or bank details, go to Chapter 13 and start the identity theft steps.

Step 4: Report It

Report the scam to the FTC at ReportFraud.ftc.gov. Report online crimes to the FBI's Internet Crime Complaint Center. If you are an older adult, the National Elder Fraud Hotline, 833-FRAUD-11 (833-372-8311), can assign a case manager to help you report. Chapter 15 lists where to report.

Step 5: Tell Someone You Trust

Talk to a family member or friend. Scammers often target people again, and you will want someone in your corner. Being scammed is upsetting. It is a crime that happened to you, not a failure on your part.

> **Watch for Recovery Scams** After a loss, you may be contacted by someone who promises to get your money back for a fee, sometimes claiming to be a lawyer or a government agency. Government agencies do not charge to help you recover money. This is another scam.

Chapter 13: Recovering From Identity Theft

If someone has used your information to open accounts, file taxes, get medical care or commit other fraud in your name, there is an official, step-by-step path to recovery. The Federal Trade Commission runs it at IdentityTheft.gov. As the site puts it, "Recovering from identity theft is a process."

At IdentityTheft.gov you can report the theft and get a personal recovery plan, which the site describes as "step-by-step advice that can help you limit the damage, report identity theft, and fix your credit." The basic order is:

1. **Call the companies where the fraud happened.** Tell each bank, card company or business that an account was opened or used without your permission. Ask them to close or freeze the account and change your passwords and PINs.
2. **Place a fraud alert and freeze your credit.** Contact one credit bureau for a free fraud alert, and freeze your credit at all three (Chapter 11).
3. **Report to the FTC at IdentityTheft.gov.** Your FTC Identity Theft Report lets you get an extended fraud alert, which lasts seven years, and helps you prove to businesses that the accounts are not yours.
4. **Change your passwords.** Start with email and banking.
5. **Check your Social Security account.** Social Security recommends signing in to, or creating, your my Social Security account at ssa.gov/myaccount, so you can watch for changes and so a thief cannot create one in your name.

6. **Clean up your credit reports.** Ask each credit bureau to remove fraudulent accounts and inquiries, and keep checking your reports for months afterward.

Keep a Recovery Log

Get a notebook or start a file. Write down every call: the date, the company, the person you spoke with, and what they said. Keep copies of every letter and report. Send important letters by certified mail with a return receipt. Recovery can take weeks or months, and this log will save you time and arguments.

Special Kinds of Identity Theft

- **Tax identity theft.** If the IRS tells you a return was already filed under your number, or you get a notice about income you did not earn, contact the IRS at the number on the notice and follow its instructions.
- **Medical identity theft.** If you see services you did not get on a Medicare or insurance statement, call your insurer and ask for a copy of your medical records so wrong information can be corrected.
- **Benefits fraud.** If someone changes your Social Security direct deposit or applies for benefits in your name, contact the Social Security Administration.
- **Criminal identity theft.** If someone gives your name to police when arrested, contact the police department and the court involved to clear your record.

Do This Now Even if nothing has happened to you, look at IdentityTheft.gov now so you know where it is. It is the place to start if you ever need it.

Chapter 14: Protecting an Older Parent

Older adults lose the most money per person to fraud. The FTC told Congress in October 2026 that reported losses among people 60 and older grew from about $600 million in 2020 to about $3 billion in 2025, and that the median loss reported by people 80 and older was $2,000. Many scams are aimed directly at them: tech support, prizes, romance, government imposters and family emergencies.

If you have a parent or grandparent who lives alone, you can help without taking over their life.

Talk About It, Without Lecturing

Bring up scams as news, not as a warning about them: “I read about a scam where people pretend to be from the bank. Have you ever gotten a call like that?” People who have been targeted often feel embarrassed. Make it clear that anyone can be fooled and that they can always call you, any time, with no judgment.

Set Up Protections Together

- Freeze their credit at all three bureaus (Chapter 11).
- Turn on spam call blocking and text filtering on their phone.
- Set up alerts on their bank account for large withdrawals or transfers. Many banks and investment firms let a customer name a trusted contact the bank can call if it suspects fraud or exploitation.
- Agree on a family code word (Chapter 4).
- Post the one-page warning signs checklist from the back of this book by their phone.

Warning Signs a Parent May Be Caught in a Scam

- New secrecy about money, phone calls or a new online friend.

- Large or unusual withdrawals, wire transfers, or buying gift cards or cryptocurrency.
- Packages, prize notices or “investment” statements they cannot explain.
- Anxiety about a debt, a warrant or a problem with Social Security.
- Someone new who is suddenly very involved in their finances.

Planning Ahead

Talk with your parent, while they are well, about a durable power of attorney for finances and who they would want to help if they ever could not manage their own money. A lawyer can help set this up. It is much easier to plan before there is a crisis.

Do This Now Call your parent this week and go over the four signs of a scam from Chapter 2. Then ask, “Is there anything you’ve been wanting to ask me about?”

Chapter 15: Where to Report

Reporting a scam may not get your money back, but it helps. Reports go into databases that law enforcement uses to find and stop scammers, and they help agencies warn others about new tricks. Some reports, like an FTC identity theft report, also give you documents you need for your own recovery.

What happened	Where to report
Any scam or fraud	Federal Trade Commission: ReportFraud.ftc.gov
Identity theft	Federal Trade Commission: IdentityTheft.gov
Online fraud or cybercrime	FBI Internet Crime Complaint Center: ic3.gov
Social Security imposters or benefit fraud	Social Security Office of the Inspector General: oig.ssa.gov/report
Scams in Nevada	Nevada Attorney General: ag.nv.gov
Mail fraud or stolen mail	U.S. Postal Inspection Service: uspis.gov
You are an older adult and need help reporting	National Elder Fraud Hotline: 833-FRAUD-11 (833-372-8311), Monday through Friday, 10 a.m. to 6 p.m. Eastern (7 a.m. to 3 p.m. Pacific). English, Spanish and other languages.
A crime in progress or a threat of harm	Call 911, or your local sheriff or police

You can also reach the FTC by phone at (877) 382-4357. Press 3 for an interpreter.

Reporting to the Nevada Attorney General

Nevadans can file a consumer complaint with the Nevada Attorney General's Office using the online complaint form on ag.nv.gov, in English or Spanish. The office says only formally filed and signed complaints are processed, and that complaints are reviewed and

processed within 14 to 45 business days. If you do not get an acknowledgment email within 24 hours of filing, the office lists these numbers: (775) 684-1100 or (702) 486-3420.

What to Have Ready

Before you report, gather what you can: dates and times of contact, phone numbers, email addresses, website addresses, usernames, the amount you paid and how, receipts, gift card numbers, transaction numbers and screenshots. Do not delete the messages until you have saved them.

> **Do This Now** Tear out or copy the Where to Report table and keep it with your important papers.

Scam Warning Signs Checklist

Post this by your phone. If you can check any box, stop and check with someone you trust before you do anything.

- ☐ Someone contacted me out of the blue.
- ☐ They say they are from the government, my bank, a company I know, or my family.
- ☐ There is a problem, a threat or a prize.
- ☐ They want me to act right now.
- ☐ They want me to keep it a secret.
- ☐ They want a code that was texted to me, a password or my Social Security number.
- ☐ They want payment by gift card, wire, cryptocurrency, payment app, or cash or gold handed to someone.
- ☐ They want me to move my money to “protect” it.
- ☐ They want to connect to my computer.
- ☐ I have never met this person face to face.

My Real Numbers Worksheet

Copy these numbers from the back of your cards or from your statements, not from a text, email or search ad.

Account	Real phone number
My bank	
Credit card 1	
Credit card 2	
Phone company	
Power company	
Medicare or health insurance	
Family member to call first	
Second family member or friend	

Sources

These are the main sources used for this book. Pages were read on November 18, 2026.

- Federal Trade Commission, “FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025” (press release, June 15, 2026).
- Federal Trade Commission, “FTC Issues Annual Report to Congress on Agency’s Actions to Protect Older Adults” (press release, October 19, 2026).
- Federal Trade Commission, “How To Avoid a Scam” (consumer.ftc.gov, updated August 2026).
- Federal Trade Commission, “Credit Freezes and Fraud Alerts” (consumer.ftc.gov, August 2025).
- Federal Trade Commission, “What To Know About Romance Scams” (consumer.ftc.gov, updated August 2026).
- Federal Trade Commission, family emergency scam articles and consumer alerts, including “Scammers Use Fake Emergencies To Steal Your Money” and “Fighting back against harmful voice cloning” (consumer.ftc.gov).
- Federal Trade Commission, IdentityTheft.gov.
- Social Security Administration, “What Are Social Security-Related Scams?” (ssa.gov/scam, 2026).
- Internal Revenue Service, “How to know it’s the IRS” (irs.gov, updated October 22, 2026).
- U.S. Department of Justice, Office for Victims of Crime, “National Elder Fraud Hotline” (ovc.ojp.gov).
- Nevada Attorney General, “Complaints and Constituent Frequently Asked Questions” (ag.nv.gov).

About This Book

Scams and Identity Theft is part of a set of free plain-language guides from Trinfinity Enterprises. Facts were checked against official sources as of November 18, 2026. This book is general information, not legal or financial advice. If you have lost money, contact your bank and the agencies listed in Chapter 15. If you find something that has changed or needs correcting, please write to andrew@trinfinityenterprises.com.