

# The Financial Safety Playbook

Carefull is an all-in-one financial safety service that organizes and protects everyday finances for you or a loved one. Its two-way oversight guards against outside threats with 24/7 account, credit and identity monitoring to alert you to unusual activity, signs of fraud, the latest scams and misuse of your personal information – backed by \$1 million in identity theft insurance. And it catches inside risks such as everyday money mistakes, missed bills and redundant services to stop small issues from becoming big problems. Carefull’s comprehensive platform also includes secure digital storage for important documents and passwords, home title monitoring and a trusted contacts system for secure sharing and coordination with trusted family members and advisors.



# 5.4 million reports of fraud reported in 2023

**\$10 billion** reported lost in 2023 to  
scams and fraud

Median loss per person to fraud in  
2023 was **\$500**


When people ages  
70 and older had a  
loss, the median  
amount was **much  
higher.**

**\$480** for adults 20-29

**\$803** for adults 70-79

**\$1,450** for adults 80+

Source: Federal Trade Commission Consumer Sentinel Network



**Thieves and hackers** are finding more and more clever ways to get people to part with their money and personal information. In fact, Americans reported losing \$8.8 billion to fraud and scams in 2022 alone—a 30% increase over 2021, according to the FTC.

**That's why it's so important to be proactive to protect yourself and your loved ones.** The more protections you put in place and the sooner you implement safe money habits, the less likely you will be among the millions who have their money and identities stolen each year through scams, fraud and exploitation.

Fortunately, there are some simple steps you can take to beat the bad guys at their game. Created by Carefull, this Financial Safety Playbook will walk you through those steps.

The Financial Safety Playbook will provide you with ways to protect your accounts and personal information. It will help you develop safe money habits and identify signs of scams and fraud. It will show you what safeguards are needed to keep your finances safe as you age and the threat of elder financial exploitation grows. And it will provide you with tips to repair the damage if you are targeted by scammers.

# Stay Safe from Scams, Fraud and Financial Exploitation in Five Steps

1

## Put Strong Protections in Place

Being proactive can help reduce your risk that your accounts and personal information will be compromised.

2

## Develop Safe Money Habits

Don't inadvertently put your personal information at risk through your own actions.

3

## Know the Red Flags of Scams and Fraud

Be able to identify the signs that someone is trying to take advantage of you.

4

## Identify Your Inner Circle of Support

Pinpoint family and friends you can trust to help protect your finances and put systems in place for them to get involved, if necessary.

5

## Know Where to Turn for Help

Find out how to repair the damage if you are a target of scams, fraud or financial exploitation.

# Step 1:

## Put Strong Protections in Place

You've likely heard that the best defense is a good offense. This rings especially true when it comes to keeping your finances safe from scams and fraud. Take these steps to protect your accounts and personal information from threats and limit the damage if you do become a victim.

**Check each step off this list as you go:**

- Protect your computer** from malware that can steal your data or damage your devices. If your computer didn't come with antivirus software already installed, check with the manufacturer's customer service to find out which antivirus software programs it recommends. And turn on automatic updates to keep your computer's software up to date.
- Protect your smartphone** by running any operating system updates as soon as you get reminders to do so. Only download apps from trusted sources, such as the Apple App and Google Play stores, and keep downloaded apps updated. Most importantly, make sure you create a strong passcode to access your phone so thieves won't be able to get into it if it is lost or stolen.
- Set up online access to all of your financial and service accounts** (utilities, Internet, phone, etc.) if you haven't already. Having online access allows you to check your accounts whenever you want rather than waiting for a monthly statement to make sure everything is OK.
- Sign up for credit monitoring** to be alerted when there are changes to your credit report or credit score. This can help you spot fraudulent activity and respond to it quickly. Credit monitoring is included as part of the Carefull service.
- Use strong passwords** that are at least 12 characters long and include a variety of random upper- and lowercase letters, numbers and symbols. Create different passwords for every account so thieves can't access all of your accounts if they get one of your passwords. To make it easier to create multiple unique passwords and securely store them, use an online password manager such as the one offered through Carefull's digital Vault feature.
- Use multi-factor authentication** in addition to strong passwords. This will require you to use another verification factor such as a text message with a code you'll need to enter in addition to your username and password. Never provide these authentication codes to any unsolicited callers, even if they claim to be with your financial institution, because this is a way that thieves can take over your account.
- Install a spam blocker on your mobile phone** to cut down on the number of spam calls you receive. Most phone providers offer spam call blocking applications. Members of Carefull's financial safety service can take advantage of Carefull's spam blocking assistance, which can help them install their provider's preferred spam call blocking application.

**Use account monitoring** to receive alerts whenever transactions are made on your financial accounts. Your financial institutions might offer the option to be notified when there is certain activity in your accounts. However, you could use a more comprehensive service such as Carefull to monitor your bank, credit card and investment accounts 24/7 and alert you to a broad range of unusual transactions, signs of fraud and money mistakes, such as late payments.

**Sign up for credit monitoring** to be alerted when there are changes to your credit report or credit score. This can help you spot fraudulent activity and respond to it quickly. Credit monitoring is included as part of the Carefull service.

**Sign up for identity monitoring** to detect whether your personal information is being misused or sold illegally on the dark web. This protection is included with the Carefull service, as well as up to \$1 million in identity theft insurance.

**Freeze your credit reports** to prevent new loans and credit accounts from being open in your name. It does so by blocking access to your credit report, which lenders need to see before extending credit. It's free, takes only a few minutes and won't impact your credit score. Plus, you can lift the freeze if you need to apply for credit. Contact all three credit bureaus to place a freeze on your credit reports:

- Equifax: <https://www.equifax.com/personal/credit-report-services/credit-freeze/> or 1-888-766-0008
- Experian: <https://www.experian.com/freeze/center.html> or 1-888-397-3742
- TransUnion: <https://www.transunion.com/credit-freeze> or 1-800-680-7289



### **Why You Need a mySocialSecurity Account**

A my Social Security account is a free online account offered by the Social Security Administration that allows you to manage your benefits and much more. It also is a smart way to protect your personal information and benefits from thieves. If criminals do get your Social Security number and other personal information, they may be able to set up a my Social Security account in your name if you haven't done so already to access your benefits. To create a my Social Security account, visit [SSA.gov/myaccount/](https://SSA.gov/myaccount/).

# Step 2:

## Develop Safe Money Habits



### Keep financial documents secure

Get into the habit of shredding all account statements and documents with your personal information before tossing them in the trash. Store important financial and legal documents in a safe place such as a home safe or filing cabinet with a lock. You also could scan and upload important documents to a digital vault, such as the one that is included with the Carefull service.



### Secure your Social Security number

Don't carry your Social Security card with you because thieves can use it to steal your identity. Also, never provide your Social Security number if you get an unsolicited phone call, email or text message asking for it. This is a tactic scammers use to get your personal information. Government agencies typically communicate by mail, and your financial institutions won't call out of the blue asking for your personal information.



### Avoid links in emails and texts from strangers

Never click on a link in an email or text message from an unknown sender. It could contain a virus or send you to a fake website where you'll be prompted to enter personal or account information.

Also, be wary of messages that claim to be from financial institutions, retailers and organizations that might be familiar to you that prompt you to click on links to provide personal or account information. Hover your mouse over the link to see if the url it's directing you to is associated with the business or organization that supposedly sent the email. To be on the safe side, though, reach out directly to the organization by looking up its phone number or website online (rather than using a number or web address in the email).



### Don't use public Wi-Fi

Free Wi-Fi at the coffee shop or any other public place is tempting, but there's no guarantee that it's secure. You're better off using your mobile data to access the Internet when you're not at home, especially if you plan on logging into financial accounts. If you want to use your computer to work in a public space, use your mobile phone as a hotspot to connect to the Internet rather than a public Wi-Fi connection, which hackers can tap into.



## Set up automatic bill payments

Setting up automatic payments for as many bills as possible can help protect you from a scam known as check washing, which has been on the rise lately. Thieves have been stealing checks out of mailboxes and using chemicals to remove the ink so they can change the recipients or amounts on the checks. Setting up automatic bill payments through your service providers or bank eliminates the need to put checks in the mail.

For any checks you must mail, deposit them in a U.S. Postal Service blue collection box inside a post office just before pickup time. Never leave mail in your mailbox overnight. If you will be out of town and can't collect your mail, visit [USPS.com](https://www.usps.com) to place a hold on your mail.



## Shop safely online

Check the website address of online retailers for a padlock symbol and “https” to ensure that the site is secure. Also, keep an eye out for web addresses that look legitimate but have the name of the retailer misspelled, which is a sign that the site is fake.

When shopping online, don't opt on retailers' sites to save your information for next time. Although it makes shopping more convenient for you, it also makes it easier for hackers to get your payment information.



## Avoid deals that are too good to be true

If you see a price advertised on a social media site, in an online ad, or in an email or text message that looks too good to be true, it probably is. The link you see might take you to a fake website, where your account information will be stolen. Before clicking, do a search online for the offer and add the words “complaint” or “reviews” to detect whether it's a scam. Better yet, shop only at the sites of retailers you know.



## Let calls go to voicemail

One of the most common ways scammers contact people is through phone calls. To stay safe, don't answer any calls that you get from anyone who isn't a family member or friend. Instead, let calls go to voicemail. Then, listen to the message and decide if you want to respond.

This strategy works better than relying on caller ID because scammers can make it appear that they're calling from a local number or even a known company or agency. If you don't answer, scammers typically will hang up before the call goes to voicemail. If they do leave a message, don't call the number they leave. Look up the number of the company or organization that supposedly is calling to find out if it was trying to contact you.





### **Be careful what you share online**

Sure, it's nice to get birthday wishes from friends on social media sites. But by publishing your birthday along with your maiden name or other personal information, you're giving away too much information to thieves who might be able to use it to answer your online account security questions. So think twice before sharing, avoid online quizzes that ask for a lot of personal information and consider making your social media profile private so only friends and family can see what you share.



### **Be wary**

A little suspicion can go a long way toward keeping your finances safe. If a situation is raising any red flags for you, don't rush into a decision (that's what scammers want you to do). It's OK to say "No" and hang up or walk away. Or, reach out to someone you trust—a family member, friend, bank representative or financial professional—to get a second opinion before taking action.



### **Think twice before sharing passwords**











It's a good idea to let your spouse, partner or another trusted family member know where your account passwords are stored in case something happens to you and those accounts need to be accessed. However, you shouldn't reveal your passwords to anyone else—no matter who they claim to be. Your financial institutions, service providers or government agencies won't call out of the blue asking for your account login credentials or other personal information.

And don't ever share your passwords with someone you haven't met in person, especially not a love interest you've met online who might actually be trying to scam you. The bottom line is that it's up to you to keep your passwords safe.



# Step 3:

## Know the Red Flags of Scams and Fraud

-  **Sense of urgency:**  
Scammers play on people's emotions by telling them that they need to act immediately to avoid a negative outcome or to claim a special offer or prize.
-  **Threats:**  
Scammers might threaten to arrest you, freeze your account, suspend government benefits or deport you unless you do as they ask.
-  **Request for a specific payment type:**  
Scammers ask for a specific form of payment that allows them to remain anonymous and makes it hard for victims to get their money back, such as wire transfers, gift cards, prepaid cards, cryptocurrency, Zelle and money transfer apps.
-  **Calls, emails or texts from government agencies:**  
Government agencies such as the IRS and Social Security Administration initiate contact by mail. If you get a call or message from someone claiming to be with a government agency, it's a scam.
-  **Unsolicited calls asking for personal information:**  
Financial institutions, service providers and government agencies won't call, email or send text messages out of the blue to request that you provide your personal or account information.
-  **Limited-time offers and high-pressure sales tactics:**  
Emails, text messages and phone calls from people offering a chance to get a special deal or to get in on a money-making opportunity for a limited time only are scams.
-  **Offers of investments with high returns and no risk:**  
A pitch for an investment that offers high returns with no risk is a scam. All investments have some level of risk.
-  **Emergency calls from grandkids:**  
A call from someone claiming to be your grandchild in desperate need of cash could be a scam. Telltale signs include a plea to wire money, buy gift cards and provide the card numbers, or send cash through a payment app such as Zelle.
-  **Online romance that results in a request for money:**  
If you meet someone online who makes excuses to meet in person then asks for money, it's likely a scam.
-  **Free lunches:**  
Offers to attend free lunch or free dinner investment seminars are sales pitches that are meant to get you to purchase high-fee, unsuitable or even fraudulent investments. Don't go.



## Step 4:

# Identify Your Inner Circle of Support

Protecting your finances doesn't have to be solely your responsibility—nor should it be. There should be people in your inner circle you can talk to about financial decisions you make or get a second opinion from when a situation seems suspicious. You also need someone who can be your financial advocate so that your finances can continue to be protected if something happens to you.

Your inner circle might include your spouse or partner, your children or other family members, and financial and legal professionals. It's important to identify people you trust, let them know what roles you expect them to play in your financial life and share details about your finances with them. You also need to put legal protections in place to give those you trust the right to get involved with your finances if necessary.

**Put legal protections in place.** Meet with an attorney to draft powers of attorney documents. A financial power of attorney document lets you name someone you trust to make financial decisions for you if you can't. A health care power of attorney document allows you to name someone to make medical decisions for you if you can't.

Drafting these documents while you still are relatively young, healthy and mentally competent allows you to decide who will be in charge of your finances and health care if something happens to you. If you wait and start to experience cognitive decline, you might be talked into giving these powers to someone you wouldn't normally trust.

**Name a trusted contact on your financial accounts.** This is a person your financial institutions can contact if there is suspicious activity on your accounts and they can't reach you. Think of your trusted contact as your emergency contact for financial matters. That person is there to help, not to act on your behalf.

Any financial firms that are required to ask for trusted contacts, such as brokerage firms, likely have reached out to you to provide contact information for someone you trust. If you haven't complied with the request, check your account online to see if you can add a contact or reach out directly to the financial firm. If you have accounts with financial institutions that haven't asked for a trusted contact, ask if you can provide one.

# The Importance of Family Money Talks

Sharing details about your finances with your adult children or other trusted family members is a way to ensure that they have the information they need to protect your finances if something happens to you. That doesn't mean that you have to share every detail. It's up to you to decide what sort of information you are comfortable providing. At the least, share what sort of estate planning documents (will, financial and healthcare powers of attorney, advance directive) you have, contact information for any financial professionals you work with, and locations of important financial documents and lockbox keys.

However, the more details you're willing to share, the better able your trusted family members will be able to protect your finances if emergencies arise. Discuss what your sources of income are, whether you have savings, and what financial obligations and liabilities you have. Also, tell your adult children or other family members what your plans are for advanced age, discuss what roles they might have to play, create a plan for incapacity and establish accountability.

It's important to talk before there is a crisis so that you can stay in control of the conversation. Having these conversations sooner rather than later and putting a plan in place also can help prevent people you don't trust from trying to fill support roles and take advantage of you as you age.

**Get a second set of eyes on your finances.** Letting family members see what's going on in your bank account might feel like you're giving up your autonomy. However, having a second set of eyes on your finances can offer a lot of protection as you age. Again, it's important to identify family members you trust and to give a certain level of access before you experience any sort of cognitive decline so that safety net already exists before problems arise.

The Carefull service makes it safe and easy to give family members view-only access to your financial accounts. Carefull

provides account, credit and identity monitoring and will alert you if it spots something unusual. You can add family members or friends as Trusted Contacts so that they can see your linked accounts (but not make transactions) and get alerts.

Putting legal protections in place, having family money talks, developing a safety net and getting a second set of eyes on your finances can help reduce your risk of being financially exploited as you age. Don't wait to take these steps.

# Step 5:

## Know Where to Turn for Help

Remember, **it's not your fault if you were targeted by a scammer or thief.** What's important is that you act quickly to report the crime and limit the damage.

### If you made any sort of payment to a scammer

Contact the financial institution or company (your bank, credit card company, gift card issuer, etc.) through which you made the payment. It might be possible to cancel or reverse the payment, but there is no guarantee that you will get your money back if you authorized the payment. (You're not liable for fraudulent charges—see below.)

### If you gave a scammer your account login credentials

Immediately create a new username and password for the account.

### If you gave a scammer remote access to your computer

Disconnect it from the Internet immediately and shut it down. Contact your computer manufacturer's tech support for help in identifying whether spyware has been installed on your computer.

### If you gave a scammer your Social Security number

Place a security freeze on your credit reports at all three credit bureaus (Experian, Equifax and TransUnion), to prevent thieves from opening new lines of credit in your name.

File a report about the scam with local law enforcement and the Federal Trade Commission by phone at 1-877-438-4338 or online at [IdentityTheft.gov](https://www.identitytheft.gov). Carefull members can get support from a Care Agent through Carefull's Scam Check feature.

## If you are a victim of fraud or identity theft

**Contact the company, financial institution or government agency where the fraud occurred** to let it know that your identity has been stolen and that there has been fraudulent activity on your account.

- If you discover an unauthorized account that has been opened in your name, report it to the fraud department at the company where the account was opened and close the account.
- If you discover a fraudulent charge, contact your debit card or credit card issuer immediately by calling the customer service number on your card or by finding the number on the company's website if your card was stolen. The Fair Credit Billing Act limits your liability for fraudulent credit charges to \$50. Your liability for fraudulent debit card charges is limited to \$50 if you report the fraud within two business days and \$500 if you report it within 60 days. You could be responsible for the full amount if you notify the bank more than 60 days after receiving an account statement that shows the unauthorized charges.
- Cancel your debit or credit card if the card or card number was stolen and request a new one. Also, change your account password in case it has been compromised. Follow up your call with a letter to your card issuer.

**Place a security freeze on your credit reports with all three of the credit bureaus** to prevent thieves from opening new accounts in your name. Get free copies of your credit reports from [AnnualCreditReport.com](https://www.annualcreditreport.com) to check for unauthorized accounts or transactions.

**Contact your local law enforcement to report the crime.** Also, file a report with the Federal Trade Commission's [IdentityTheft.gov](https://www.identitytheft.gov) site to receive a recovery plan and FTC Identity Theft Report, which you can file with business to prove your identity was stolen and with the three credit bureaus to have any fraudulent accounts removed from your credit reports.

## If you are a victim of elder financial abuse

**Contact Adult Protective Services** if someone you know is mishandling or misusing your finances or the finances of someone you love. APS are social service programs that help older adults and adults with disabilities if they are being abused, neglected or exploited. You can find your local APS through [Napsa-now.org](https://www.napsa-now.org). Contact your financial institutions to alert them to any fraudulent activity in the account to find out if you can get your money back.

**Contact local law enforcement** to report the theft of your assets. Call 911 if there is an urgent threat of harm.

**Contact your local district attorney's office** to take legal action against the person who is exploiting you.

**Reach out to a trusted family member, friend or attorney** if you need assistance contacting authorities and your financial institutions. Do not confront the person responsible for the exploitation yourself.

You can stay up-to-date on the latest scams that are circulating through Carefull. Carefull publishes Scam Alerts on its Take Care online publication and keeps its members informed through weekly summary emails and a monthly email newsletter.

Carefull also provides Scam Check and Hack Recovery to support its members who are targeted by scammers and hackers. The Carefull service includes up to \$1 million in identity theft insurance to help victims recover lost funds and legal fees. And our Care Agents are available to answer your questions and provide assistance for scam, fraud and exploitation issues.

Visit [getcarefull.com](https://getcarefull.com) to learn more.