Financial Ratings Series

Weiss Ratings & Grey House Publishing

Financial Literacy: Planning for the Future

Protect Yourself from Identity Theft & Other Scams

2022/23

GREY HOUSE PUBLISHING

Financial Literacy: Planning for the Future

Protect Yourself from Identity Theft & Other Scams

Financial Literacy: Planning for the Future

Protect Yourself from Identity Theft & Other Scams

2022/23 Edition

GREY HOUSE PUBLISHING

FINANCIAL RATINGS SERIES

Weiss Ratings & Grey House Publishing

https://greyhouse.weissratings.com

Grey House Publishing
4919 Route 22, PO Box 56
Amenia, NY 12501-0056
(800) 562-2139

Weiss Ratings
11780 US Highway 1, Suite 201
Palm Beach Gardens, FL 33408
(561) 627-3300

Published by Grey House Publishing, Inc., located at 4919 Route 22, Amenia, NY 12501; telephone 518-789-8700. Grey House Publishing neither guarantees the accuracy of the data contained herein nor assumes any responsibility for errors, omissions or discrepancies. Grey House Publishing accepts no payment for listing; inclusion in the publication of any organization, agency, institution, publication, service or individual does not imply endorsement of the publisher.

Grey House Publishing

2022/23 Edition
ISBN: 978-1-64265-891-0

Table of Contents

Welcome!

Grey House Publishing and Weiss Ratings are proud to announce the fourth edition of *Financial Literacy: Planning for the Future*. Each volume in this series provides readers with easy-to-understand guidance on how to manage their finances. This eight-volume set assists readers who are ready for one—or more—of many important next steps in their financial planning—starting a family, buying a home, weighing insurance options, protecting themselves from identify theft, planning for college and so much more. *Financial Literacy: Planning for the Future* takes readers further towards their financial goals.

Written in easy-to-understand language, these guides take the guesswork out of financial planning. Each guide is devoted to a specific topic relevant to making big decisions with significant financial impact. Combined, these eight guides provide readers with helpful information on how to best manage their money and plan for their future and their family's future. Readers will find helpful guidance on:

- Financial Planning for **Living Together, Getting Married & Starting a Family**
- **Buying a Home**
- **Insurance Strategies** & **Estate Planning**
- Making the Right **Health Care Coverage** Choices
- Protect Yourself from **Identify Theft & Other Scams**
- **Starting a Career** & **Career Advancement**
- **Saving for Your Child's Education**
- **Retirement Planning Strategies** & the Importance of Starting Early

Filled with valuable information alongside helpful worksheets and planners, these volumes are designed to point you in the right direction toward a solid financial future, and give you helpful guidance along the way.

Planning for the Future: Protect Yourself from Identity Theft & Other Scams

Introduction

You might think that identity theft is strictly an internet-era phenomenon, but the term actually entered the English language as early as 1964. By the mid-twentieth century, people in developed nations had sizable "paper trails" of financial, medical, and government records, and the crime of identity theft began to emerge.

Today, with the spread of electronic business and the internet, it has become easier and more convenient than ever to take care of the details of life, electronically, more often than not, at any time and on the fly. But there is a corresponding greater risk, too, that someone might intercept our personal details for harmful ends.

The law defines identity theft as falsely using someone else's personal information, including their name, date of birth, Social Security number, credit card numbers, ATM code, electronic signature, and passwords which protect financial information like electronic banking or e-payment sites.

According to the Federal Trade Commission, 2.8 million fraud reports were received in 2021, totaling $5.8 billion in losses. That represents an increase of more than 70 percent over 2020. Nearly half of those losses were due to imposter scams

As fraudsters become more sophisticated, it's important to be aware of the types of security threats that you might come across. *Forbes Magazine*[1] writes that these are some of the biggest cyber security risks that people might face in 2022:

- Data breaches and ransomware attacks rose at a record rate in 2021. As more of our daily lives happen online, these types of attacks will continue to increase.

- "Internet of Things" devices (internet-connected cars and smart home appliances, for instance) are particularly vulnerable and easy to hack. It's predicted that there will be

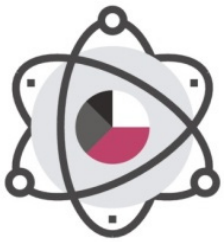
[1] https://www.forbes.com/sites/bernardmarr/2022/03/18/the-biggest-cyber-security-risks-in-2022/?sh=6e1d97117d7b

more than 27 billion of these devices in homes and businesses by 2025, and as the number of devices continues to grow, so does the risk of attack.

As more and more people are working remotely, that increases cybersecurity risks. Many remote employees use their personal computer to connect to their work environment. They might connect from an unsecured network at a local coffee shop, and other users of their personal computer could download ransomware without knowing it. There are several new security measures that companies and employees should think about to keep their home and work networks safe.

Scammers are now hiding malware in video game cheat codes and illegal movie downloads, so younger internet users are at increased risk of downloading malware to their home network.

This guide is meant to educate you about different kinds of identity theft and other common scams and to help you understand strategies to protect yourself and your family. It will provide you with tips about how to secure your personal, financial, and electronic data, and give you an overview of how to conduct business—personal and professional—more safely in the 21st century.



Types of Identity Theft

The first step in protecting yourself against identity theft is knowing where and how you could be vulnerable. Identity theft can be divided into several categories.

- **Financial identity theft** is by far the most common category. In this type, the thief uses stolen credentials to access a person's monetary assets. This can be something as straightforward as a stolen ATM card, for example. A more elaborate scheme is one in which a thief takes out loans under the stolen identity.

  Many identity thieves are seeking a borrowed identity. For example, a person might use a stolen name, Social Security number, and date of birth in order to get a job or open a bank account. This kind of activity can go on for years undetected, especially when the thief wishes to keep a low profile. Even though in some cases this causes no negative effects, it can leave a person (whose information was stolen) legally or financially liable.

Types of financial identity theft can include:

- **Employment or tax fraud** is where a thief uses someone else's Social Security number to get a job or file an income tax return.
- **Credit card fraud** where a thief uses someone else's credit card or credit card number for fraudulent purposes.
- **Phone or utilities fraud** is when a thief uses someone else's information to open a fraudulent phone or utilities account.
- **Bank fraud** is when a thief uses someone else's information to open a fraudulent bank account or to take over someone else's bank account.
- **Loan or lease fraud** is when a thief uses someone else's information to get an auto loan, a mortgage, or a lease.
- **Government benefits fraud** is when a thief uses someone else's information to steal their Social Security benefits or other government benefits.

- **Child identity theft** is a variation of a borrowed identity scheme where a criminal obtains a child's name and Social Security number for purposes of fraudulently getting a job, opening a bank account, or even obtaining a driver's license. This kind of identity theft can go on for years undetected, as parents have no reason to monitor activity of a minor's Social Security number. Studies have shown this is surprisingly common, and a growing problem.
- **Medical identity theft** is when a criminal uses a stolen identity to receive medical treatments or prescription drugs. This is closely related to insurance theft, where a criminal with your insurance information seeks insurance payouts in your name. In addition to the financial and legal risks, these forms of identity theft can jeopardize a person's medical history. It can fill the person's medical records with inaccurate information which makes it harder for doctors to deliver accurate care.

- **Social engineering**, broadly, is manipulating others to gain information or bypass security. For example, a person might show up at an office claiming to be a delivery or repair person, hoping to talk their way into a non-public area. This can overlap with identity theft when someone uses borrowed credentials — a borrowed name, or even a swiped employee ID — to gain access. Phishing is an important identity theft technique to guard against, discussed on page 18.

- **Real estate fraud** is when a criminal uses a person's identifying details to alter property ownership records. These changes can lie dormant for years and be extremely difficult to prove after the fact. There have even been cases where people have been evicted from their own homes as a result of these schemes.

- **Elder identity theft** is notoriously difficult to combat. Millions of senior citizens are the victims of identity theft each year, and are a growing target for thieves, for several reasons. First, many seniors have accumulated considerable amounts of funds and assets over their working lives for their retirements. Second, many elderly persons are unfamiliar or uninterested in the complexities of modern technology that make identity theft possible. Third, some senior citizens suffer from dementia and other cognitive declines that make them especially vulnerable.

Data Breaches

Unfortunately, it is becoming more and more common to hear about corporate data breaches that affect the personal information of millions of customers. Whether by hackers or ineffective security measures, these data breaches reveal that your personal information is not as secure as you might think.

Based on the number of people affected, the ten largest corporate data breaches[2] are:

1. **CAM4** (2020): 10.88 billion users affected

2. **Yahoo** (2017): 3 billion customers affected

[2]https://www.upguard.com/blog/biggest-data-breaches

3. **Aadhaar** (2018): 1.1 billion users affected
4. **First American Financial Corp** (2019): 885 million customers affected
5. **Verification.io** (2019): 763 million users affected
6. **LinkedIn** (2021): 700 million users affected
7. **Facebook** (2019): 533 million users affected
8. **Yahoo!** (2014): 500 million accounts affected
9. **Starwood (Marriott)** (2018): 500 million customers affected
10. **Friend Finder Networks** (2016): 412 million customers affected

Data breaches of any sort can leave your personal information vulnerable to attack so it's important to do what you can to protect yourself.

Securing Your Social Security Number

Your nine-digit Social Security number (SSN) is one of the most important pieces of information associated with your identity as an American citizen.

With only your name and SSN, someone can impersonate your identity for purposes of getting a job. A clever and determined thief can use that information to access your banking information or even alter property and home ownership records in your name. Unlike a credit card number, your Social Security number follows you around for your entire life, and a compromised Social Security number can be difficult or impossible to replace.

★ An easy thing you can do to protect your Social Security number is to keep the actual Social Security card someplace safe, like a locked box of records at home. Don't carry your Social Security card in your wallet!

Also be careful where you give out your number. There are only a few cases where you are required to give out your Social Security number. These include:

- Applying for a job;
- Opening a bank account;

- Filing your taxes;
- Applying for a Student Loan;
- State government paperwork like child support, Medicaid, and Unemployment Compensation; and
- Federal government paperwork like savings bonds and workers' compensation.

You do not have to give out your social security to private businesses to access their services. This includes doctors as well as utilities like the power company and your internet provider.

Sometimes, a business will ask for your Social Security number as a personal identifier for their records. In this case, you can offer your driver's license number, passport number, student ID number, etc. instead.

Scammers might say they are calling to collect a bill or are calling from your utility company and they'll ask you for your Social Security number. You should never give out your SSN to anyone who seems suspicious, and never give your SSN to someone who calls you on the phone, sends you a text, or contacts you by email.

If you're not sure, ask the person the following questions:

- Why do you need my Social Security number and how will it be used?
- What happens if I refuse to give you my number for safety reasons?
- What law requires me to give out my Social Security number?

If a person can't easily answer these questions, or you're suspicious about their answers, don't give them your number!

How to Check Your Social Security Number for Fraudulent Activity

The Social Security Administration has an online system called "My Social Security." You can access it at https://www.ssa.gov/site/signin/en/.

After creating an account to verify your identity, you will be able to track all activity on your SSN!

Securing Your Home Computer

It's possible to do an amazing amount of personal business online these days — banking, bill-paying, remote work, job interviews, and even college courses can be conducted entirely online.

Of course, with all this power, there comes the responsibility to protect your data. It only takes a single vulnerability for someone to steal your data and potentially your whole identity.

Buying a computer from a reputable name brand manufacturer is recommended. Acer, Apple, Asus, Dell, HP, and Lenovo are all established brands. If you buy a computer from a smaller off-brand manufacturer, there is always a risk it could come pre-installed with spyware.

This is also important if you are ever buying a replacement keyboard for your computer. In late 2017, it was discovered that an off-brand keyboard manufacturer in China had built a special "key logger" chip inside the keyboard, which would secretly transmit all text typed (all your logins!) to a remote server on the internet.

If you need a replacement keyboard, stick to one from a major manufacturer: Logitech, Microsoft, and Razer are all safe, popular manufacturers of aftermarket keyboards. Of course, the computer manufacturers mentioned here are safe sources, too.

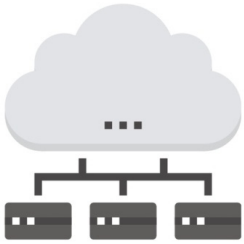
As for wireless keyboards, it is safest to just not use them! There is no guarantee of encryption over the transmitted keyboard signal, and even wireless keyboards from major manufacturers can easily be spied on. These keyboards are popular with home theater PCs, and they might be okay if you are just trying to look up movies on Netflix, but if there is any chance you might be using the

Top 5 Suppliers of Desktops, Notebooks & Workstations Worldwide

- Lenovo
- HP
- Dell
- Apple
- Acer

Source: https://www.canalys.com/newsroom/global-pc-market-Q4-2021

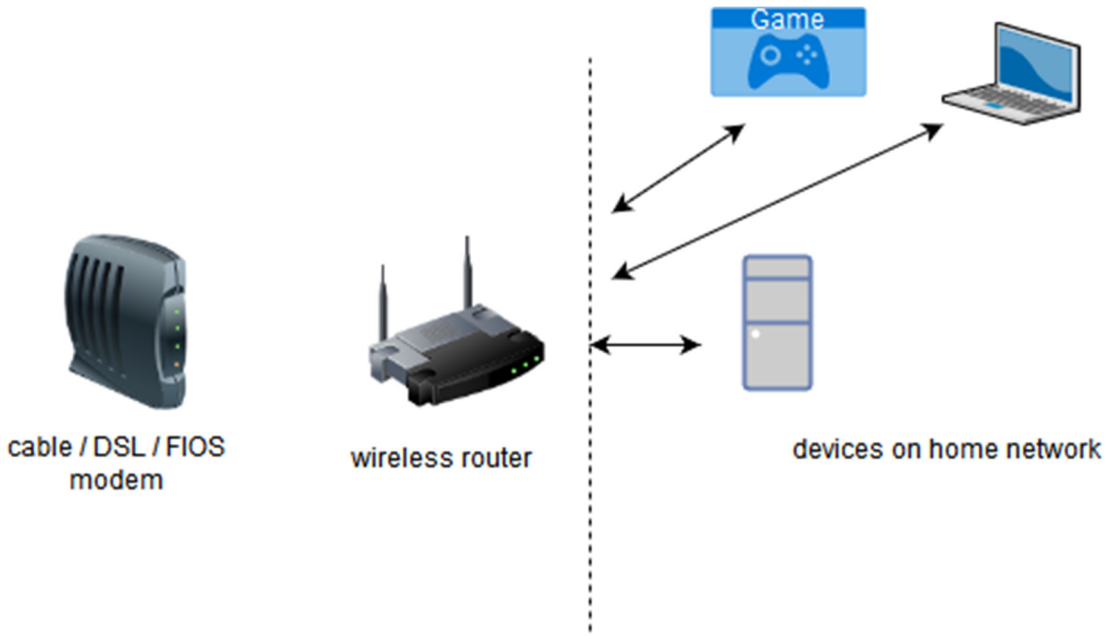
keyboard to login to a sensitive personal account like your email, then you shouldn't take the risk.



Home Network Safety

Your internet service provider (ISP) connects you with the internet by way of a device generically known as a modem (modulator - demodulator). This device bridges your home network with a cable, DSL, fiber-optic, or satellite connection to the internet. Your internet provider might also provide you with a second box called a wireless router (it has one or two small antennas on it). It is also possible that the modem and wireless router functions might be combined into a single box.

In either case, this router device directs all traffic between the internet and the individual devices on your home network (laptops, desktop PCs or home theater PCs, game consoles, tablets, etc.) This allows the router to see any unencrypted device on your home network. If you share photos between an iPad and TV, it goes through the router. If you bring home documents from the office and copy them from a laptop to a home computer, those documents have to travel wirelessly (or via a network cable) through the router. File transfers on a home network are



usually not encrypted, and this means those documents can potentially be seen by your internet provider. It also means anyone at the internet provider's end can connect to your home network as if they had your wi-fi password. This lets a malicious user get "in the front gate" of your home network, making it much easier to attack individual systems.

An inexpensive way to protect the privacy of the traffic on your home network is to connect a second router, which typically costs $50-$100. This lets you isolate all of your home traffic onto the second router you personally control, without exposing it to the internet provider (and potentially malicious hackers).

An internet search for "how to connect a second home router" will provide plenty of information. You might want a technically-inclined friend's help, but it probably won't be necessary. They aren't difficult to set up, and it should only take a few minutes. Some people choose to add a second internal "guest" router, for example, to allow visiting guests to use wi-fi without exposing the private home network. This can make sense in a group house situation where you might not personally know everyone who will be using your wi-fi.

Deregulating Net Neutrality

After the FCC's Restoring Internet Freedom Order and transparency rule amendments became effective June 11, 2018, there is no longer a thorough guarantee of privacy for data that travel across a router owned by an Internet service provider. For example, Verizon's FIOS agreement states (in section 11.4):

"We also will access and record information about your computer and Equipment's profile and settings and the installation of software we provide. You agree to permit us and our applicable third party supplier to access your computer and Equipment and to monitor, adjust and record such data, profiles and settings for the purpose of providing the Service."

Other Internet providers have similar language in their service agreements. It's not *necessarily* intrusive, but think of a comparison. Suppose the electric company changed their policy to say that they now have the right to peek into your window to check if your lights are working. You would probably want a way to close the curtains!

Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) is a private encrypted "tunnel" to the internet, usable on a home or public network.

A VPN is typically a subscription-based service — ExpressVPN (expressvpn.com), NordVPN (nordvpn.com), and Surfshark (surfshark.com) are three popular providers — that typically cost a few dollars a month. When you use the VPN, all of your internet traffic, including the addresses and contents of sites you visit, is hidden and encrypted from outsiders.

If you ever use public wi-fi networks to do business, like those at coffee shops, hotels, and airports, or if you use those public networks to do remote work, it is highly recommended to make the investment in a VPN subscription.

There should be little expectation of privacy when using public wi-fi networks, which can be thought of as bunch of strangers sharing the same home network. It can be easy for a nosy stranger with a little technical knowledge to snoop on your browsing. Crowded airport and hotel lounges can be enticing for identity thieves, with potentially dozens of targets at any time.

A VPN is also a good thing to consider if you spend time doing business on public computers, such as in internet cafes, libraries, or university computer labs. These computers will frequently "reset" themselves between users, clearing out personal data from the user session, but there is no guarantee of privacy.

Do be aware that some private networks (especially those in the workplace) might not want you running VPN software; be sure to check with your employer's network manager before running a VPN on a work computer.

Make sure to research a VPN app before subscribing. Some VPN apps are free because they share your information with other companies or sell advertising on the app. Search for the VPN app with the words "review," "scam," or "complaint" to see what other users have said about the company. Look at the reviews online or in the app store to see how other customers rate the app.

Protect Your Personal Information and Data

Secure Your Devices. Keep your security software, internet browser, and operating system up to date. Criminals look for weak points to exploit before the software companies can fix them. But updating your software regularly — as soon as possible when a newer version comes out — helps make sure you have critical patches and protections against security threats. Don't ignore reminders to make updates. Be sure to update your security software, operating system software, internet browsers and apps.

Secure Your Accounts. Once your computer, tablet, and phone are secure, next take steps to protect your accounts — particularly those with personal information, like your bank, email, and social media accounts.

Create and use strong passwords. That means at least 12 characters. Making a password longer is generally the easiest way to increase its strength. Consider using a passphrase of random words so that your password is more memorable, but avoid using common words or phrases.

Use multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. These additional credentials could be a passcode you get via an authentication app or a security key or a scan of your fingerprint, your retina, or your face. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

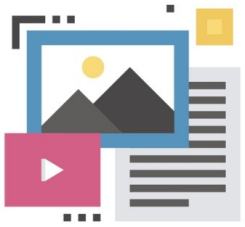
Choose security questions only you know the answer to. Many security questions ask for answers to information available in public records or online. So, when you can, avoid questions like your zip code, mother's maiden name, and birth place. And avoid using questions with a limited number of responses that attackers can easily guess — like the color of your first car.

Back up your data to protect it. Backing up your data means making an extra copy of all your files. That way, if something happens — say a virus, your device crashes, or you're hacked — you still have your files. It's important to do it once a week so you don't lose important data, like your photos, documents, and files. If you do need to restore a backup, it will only be as current as the last time you backed up. You can back up your files in the cloud or you can save your files to an external storage device.

Protect Your Home Network. One important way to protect your information is to protect your network at home. Think of your router as the connecting point between your devices and the internet. If malware gets onto any of your connected devices, it can spread to the other devices connected to your network. Your devices, accounts, and whole network are only as secure as your router.

Protect Yourself While on Wi-Fi. You can control how secure your home network is — but you can't do the same for public Wi-Fi. It's always best to assume it's not secure. The easiest solution? Save your online shopping, banking, and other personal transactions for when you're on your home network. Or use your mobile data, as that data is typically encrypted. If you do use public Wi-Fi, read more about protecting your personal information while you're online in public.

Source: https://consumer.ftc.gov/articles/protect-your-personal-information-data



The Internet of Things

In the mid-2010s, an exciting array of internet-connected "smart devices" for the home began to proliferate. internet-connected webcams paved the way for "smart" refrigerators, thermostats, baby monitors, coffee makers, and lightbulbs. Digital "home assistants" use voice recognition to allow users to look up online information or adjust appliances in the home.

Called the Internet of Things (IoT), these physical devices are connected to the internet and can be controlled wirelessly. Some of the most popular IoT devices today are:

- Voice Activated Home Assistants
- Smart Door Locks, Video Doorbells & Security Systems
- Smart Televisions & Smart Speakers
- Smart Baby Monitors
- Smart Bluetooth Trackers
- Smart Bike Locks & Trackers
- Smart Thermostats
- Smart Electric Outlets
- Smart Lightbulbs & Lighting Systems
- Smart Pet Feeders
- Smart Kitchen Appliances & Countertop Displays
- Robot Vacuums
- Smart Smoke Detectors, Air Quality Monitors & Air Purifiers
- Smart Health Trackers & Emergency Response Systems
- Smart Home Gym Equipment

These devices are getting more and more popular, and that means if you have smart devices in your home, they need to be part of your data security plan, otherwise they can be an easy target for hackers.

The controller circuits built into these devices can be inexpensive with little expectation of security. All computer hardware can have vulnerabilities that appear over time, but a bug that appears in a laptop or internet connected gaming console can be fixed with a software patch. With a simple smart device like an internet connected thermostat, there's no way to apply a patch, and the vulnerability can remain undetected for years, allowing an intruder to use the compromised device to snoop around a user's home network.

Even with devices from major manufacturers, dangerous security glitches have happened. In late 2017, there was a flaw with a number of Google Home Mini AI speakers, where the devices were accidentally broadcasting all overheard audio (not just specific command phrases) to servers at Google. If a hacker were able to gain control of one of these devices, they would have a way to constantly listen in on your conversations.

Does this mean "smart" devices should be avoided entirely? Not necessarily, but they should be approached with caution. Maybe you're comfortable having an internet-connected camera watching your driveway, but not monitoring your baby's room. An AI speaker might be handy in a basement workshop where your hands are rarely free, but it might be too big of a risk to keep in the family room. Remember that every little personal detail can be potentially useful to a would-be identity thief. Before purchasing a smart device, talk to someone educated about computer security.

How to Protect Your Internet Connected Devices

If you have internet-connected devices at home, the Federal Trade Commission[3] recommends these steps to protect your home network.

Start With Your Router

1. **Change the default settings.** The key to privacy in the Internet-of-Things (IoT) world is your router. All of your connected devices likely connect to the internet through your router. Start by changing defaults — the settings every router comes with — to something unique. You'll need to change the default administrative username, password, and network name. Don't use login names or passwords with your name, your address, or your router brand.

2. **Enable encryption.** You can enable encryption by going to your "administrative settings," then to your "wireless security settings."

[3] https://consumer.ftc.gov/articles/securing-your-internet-connected-devices-home

3. **Check for updates.** Remember to keep checking for hardware and software updates.

Protect Each Device

Once your router is secure, search for each device connected to your router. To make sure you know which devices are connected, go to your router's web interface and look for "connected devices," "wireless clients," or "DHCP clients."

Here are steps to take to protect each device connected to your router:

1. **Change the default username and password.** Never reuse passwords. Hackers sometimes use stolen usernames and passwords from data breaches to hack your other accounts.

2. **Use two-factor authentication.** If a device offers two-factor authentication (a password plus something else, like a code sent to your phone or a thumbprint scan), use it.

3. **Don't just click "next" when you set up your IoT device.** Don't skip this important step for later — set up the security features on your device from the start. Take advantage of your device's security features, like enabling encryption or setting up a passcode lockout ("three strikes, and you're out") to add another layer of protection to your device.

4. **Update your device regularly.** Check for updates to the firmware. You may need to do this on the manufacturer's website. Also, if your device is accessible through an app on your phone, use the most up-to-date version of the app.

5. **Disable or disconnect what you don't use.** Disable features you won't use. If you won't use remote management, it's best to disable it. Also, disconnect from the network older devices you no longer use. Their security may be out of date, creating a weak point on your network.

Password Security

There are just a few keystrokes between you and your private information. Choosing strong passwords for your online accounts is one of the easiest yet most important steps you can take to secure your internet information.

Take a look at the chart on the next page. It would take a hacker less than a second to crack a six character password containing numbers only, lowercase letters only or upper and

lower case letters. It would take a hacker 7 quadrillion years to crack an 18 character password made up of symbols, numbers, upper and lowercase letters.

Many sites require you to choose a password of a minimum length (usually seven to ten characters) and a mixture of lower & upper case letters, numeric digits (0-9), and special characters like "#$%_-=" and so forth. Using more special characters, and making it as long as possible, make the password stronger and harder to guess.

Someone who knows you, or knows information about you could try to guess your password. It's important to avoid any passwords which include your name, the names of any family members or pets, anything that an intruder might be able to guess at by knowing you as a person.

It's also possible that the intruder might be a remote hacker who has a whole list of encrypted passwords they are trying to break, using an automated "dictionary attack" that tests passwords against variations of common English words ("Apple123",

How Long Would it Take a Hacker to Guess Your Password?

Number of Characters	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Symbols, Numbers, Upper & Lowercase Letters
4	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 second	5 seconds
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
10	Instantly	58 minutes	1 month	7 months	5 years
12	25 seconds	3 weeks	300 years	2,000 years	34,000 years
14	41 minutes	51 years	800,000 years	9 million years	200 million years
16	2 days	34,000 years	2 billion years	37 billion years	1 trillion years
18	9 months	23 million years	6 trillion years	100 trillion years	7 quadrillion years

Estimates from https://www.security.org/how-secure-is-my-password/

"0rang3"). Anything that's too close to a regular word, even with some characters substituted, is easy for a computer to guess.

The most secure passwords come from an automated password generator. On the web, https://strongpasswordgenerator.com or https://passwordsgenerator.net are sites which will make a strong password composed of a random mix of letters, numbers, and special characters (u;6,Atn[pDuxq,D'). Most people can't remember a string of random characters like that, which means either writing them down or using a password manager app. Both of these options are discussed in Storing Your Passwords, in the next section.

Sometimes it's not possible or convenient to use a randomized password, especially if it's something that needs to be typed on a phone or tablet with a touch input, which cannot enter special characters as easily as a full desktop keyboard. In this case, a good alternative is to combine two unrelated words into one password, like stovetopdentist or elevatorshoulder, then add a number or a special character. It turns out that there are so many words in English that even a dictionary attack will have a very hard time decrypting this kind of password.

Be Creative

Think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

Source: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

Storing Your Passwords

Most people today have several important passwords they need to remember. Anytime a password connects to a system with personal information — your email, your social media accounts, your work accounts — it's important to have a separate password for that system, not shared anyplace else.

Unless you have a remarkable memory, you will probably have to store your passwords somewhere outside of your own head. There are two approaches to this, writing down the passwords or using a password manager.

Writing down passwords sounds dangerous, but only if someone finds them. If they're written in a book that's kept in a safe location at home, the danger is minimal.

If it's too inconvenient to type in long passwords all the time, or you don't trust having them written down, you can also use a password manager.

A password manager will automatically generate strong passwords for the websites you visit and store them in a file, which is itself protected by a master password.

Best Password Managers for 2022

- Bitwarden
- LastPass
- 1Password
- Dashlane
- Keeper
- KeePassXC

Source: https://www.cnet.com/tech/services-and-software/best-password-manager/

This way, the user only needs to remember a single login. The disadvantage to a password manager is that your entire "key ring" is in a single place (on a single device). Either backups must be kept of the master file, or else the user risks losing all their passwords if they lose their phone. Also, if a hacker ever gained access to the master file, it could be disastrous.

Answering Security Questions

In addition to setting a password, many systems require you to choose and answer one or more security questions to confirm your identity, in case you forget your password, or as an additional identity check over the telephone.

Common security questions are: "What is your mother's maiden name?" "Where did you go to elementary school?" "What is your favorite sports team?" and so forth. These questions are supposed to be easy for the user to remember, but difficult for a stranger to guess.

Unfortunately, most of this information is easy to figure out for a determined criminal. In fact, most security experts have been advising website managers to stop using

security questions all together because they're so easy to guess.

Instead, if the website has multi-factor authentication, experts recommend that method to recover a lost password, it's much more secure than security questions.

Don't Overshare on Social Networking Sites

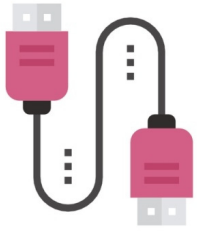
If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information.

Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Source: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

If you absolutely have to set up security questions and you have the opportunity to choose your own questions, pick questions that only you know the answer to. Make sure it's not a question that can be answered looking through your social media too. You might use questions like, "Where was your first kiss?" "Where did you meet your spouse?" "What was your oldest child's favorite toy?"

Another strategy is to invent a scheme of fake answers to your security questions. Maybe your elementary school is "Narnia Clown College" and your favorite sports team is "Duke Ellington Quintet." Just make sure you can remember the answers!



Phishing

Phishing (a play on words from "fishing") is a broad group of malicious techniques where a criminal attempts to expose a person's details by way of deceptive emails.

Phishing attacks first gained popularity in the early days of the public internet, in the mid to late 1990s, by way of so-called "419 scams" (named after the criminal code which prohibited them). The scammer

would contact people by email, pretending to be the caretaker of a vast amount of wealth, and seek the would-be victim's help in transferring the money into a U.S. bank account. This could play out over a long series of email conversations to gain a person's trust before finally tricking them into giving out enough personal information (especially bank account details) to allow the scammer to steal their assets.

Phishing techniques have only grown more sophisticated in the years since. Phishers often use "bots" on social media to try to trick a person into exposing personal information. If you are a fan of social media sites like Facebook and Instagram, be mindful of how much of your life you expose and who you share it with.

Personally targeted "spear phishing" attacks are a recent trend. Here, a criminal will gather personal information about a target and use it to construct a believable fake email or phone call. A criminal might learn the details of a target's family and claim to have been in a car accident with "your brother Jim in Wyoming," and insist a money transfer is urgently needed for medical reasons or to prevent legal problems. These schemes can be frightening and effective to someone who doesn't know they are out there.

Identity thieves will also use forged copies of websites in order to trick users into handing over their credentials. Would you click on a link like http://goog1e.com or http://paypals.net? The risk of phishing is one reason using multi-factor authentication is so important.

Vishing

Voice phishing, or vishing for short, is just like phishing but over the telephone or VOIP (voice over the internet) instead of email.

You might get an email that says your bank or credit card has detected fraud on your account and you need to call their customer service team right away. So, you hurry up and call the number. But, the email was sent by a scammer, and the person answering the phone when you call is a scammer too. They might know some personal information about you, like your address, which they found online. Some of these vishing fraudsters sound like a real customer service rep, so it can be easy to fall into their trap, especially if you are stressed thinking that your account has been hacked. They might try to get you tell them more personal information, like your social security number or your bank account number. They might try to get you to

send them money or gift card activation codes.

Some fraudsters will call your home number or your cell phone, saying they are with the tech support team of a company you do business with. Like the first example, they say that someone has broken into your account, made a very large purchase using your information, and you need to fix it right away. They use that technique to scare you, and get you to take action quickly, so you don't have time to think about whether this call sounds legitimate or not. They might ask you to confirm your email address and your password, thus giving them access to your account. They might say that they need to access your computer to fix the problem, all the while installing malware on your computer while they have access.

If you get an email or a phone call about fraudulent activity on your account, take some extra steps before hurrying to the phone. Look at the sender of the email you received. Is it sent from the right email address and domain? Does it look a little strange? Is it a company that you don't do business with, or haven't done business with in a while? Would this company normally contact you by email? If any of these things look odd or abnormal, don't call the number in the email. Instead, look up the telephone number for the company online and call that number. That way, you're sure you're calling the right business and not a fraudster.

The same thing goes when you're answering the phone. If the person sounds a little strange, or if that company doesn't normally call you for issues like this, take a moment to pause and think, "Does this sound right?" You can always hang up the phone and call the company directly, using the number that you researched online or from your account statement, to make sure that you are talking to a legitimate business.

Be aware that fraud can happen on the phone too, and with VOIP calls over the internet, it's easier than ever for callers to hide their identity, spoof the number that they're calling from, and evade detection.

Smishing

Smishing is another type of phishing attack, this type of attack is sent over SMS or text message.

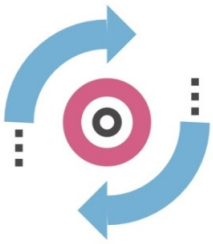
Here's an example of a smishing scam. You receive a text message from your bank. They say that your account has been hacked and you need to click a link or call a number to fix the problem. If you click on the link, it could download malware to

your smartphone. If you call the number, the scammer could try to get access to your personal information. They can even sell your personal information to other fraudsters, making you even more vulnerable to future attacks.

Smishing attempts are becoming more and more common. Most people are aware that emails can contain fraudulent information, but they don't often think of text messages being used by fraudsters. From a thief's point of view, that makes smishing attacks particularly effective.

The Federal Communications Commission[4] has put together this guidance on how to avoid being a victim of a smishing attempt:

- Never click links, reply to text messages or call numbers you don't recognize.
- Do not respond, even if the message requests that you "text STOP" to end messages.
- Delete all suspicious texts.
- Make sure your smart device OS and security apps are updated to the latest version.
- Consider installing anti-malware software on your device for added security.
- Validate any suspicious texts. If you get a text purportedly from a company or government agency, check your bill for contact information or search the company or agency's official website. Call or email them separately to confirm whether you received a legitimate text. A simple web search can thwart a scammer.
- **Bottom line**: Stop before you engage and avoid the urge to respond.



Multi-Factor Authentication

An important idea in computer security is "multi-factor authentication." The idea is that accessing a system requires multiple things:

- **Something you know**, like a PIN or a password;
- **Something you have**, like an ATM card or a special code sent to your smartphone; or
- **Something you are**, like your fingerprint or voice recognition.

[4] https://www.fcc.gov/avoid-temptation-smishing-scams

An ATM bank card is the most common form of multi-factor authentication. To use an ATM banking machine, you need a physical card with a magnetic stripe (something you have), and you also need a private numeric PIN passcode (something you know). This provides an extra layer of security because the card is useless without the PIN and vice-versa.

Multi-factor authentication provides extra security on the internet. One way this works is that if you log into an account from an unfamiliar computer (say, an internet cafe, a work computer, or a university computer lab), the server will send an SMS text message to your phone with a short numeric code that must be entered (in addition to the normal password) to proceed. Someone who found your password would not be able to use it on their own computer without access to your phone. This also serves to alert you if someone unfamiliar tries to use your account.

Some other multi-factor authentication methods require you to install a special authenticator app on your phone, or even a separate keychain-sized device with an LCD screen that displays a code which changes every few seconds.

Some cellphones and laptops can be unlocked with your fingerprint after your initial login with a strong PIN or password.

In all cases, the basic idea is the same; you can log in with one or more of these things: something you know; something you have; or something you are .

★ Find out how to turn on multi-factor authentication on your most important accounts, and use it! Google, Apple, Microsoft, and Yahoo all have a way to turn on the extra step of verification.

The web pages in the list below give information for how to activate multi-factor authentication for major account types. If you do any online banking or use e-payment systems, find out what means of user authentication they provide beyond a simple user / password login.

Sites to Activate Two-Step Verification

- Apple ID

support.apple.com/en-us/HT204915

- Google account

safety.google/authentication/

- Microsoft account

support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-

account-c7910146-672f-01e9-50a0-
93b4585e7eb4

- Yahoo! Account

help.yahoo.com/kb/SLN5013.html

Credit Monitoring Services

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also might be offered by your bank or credit union, credit card provider. employer's benefits program, or insurance company.

Credit Monitoring Services

Credit monitoring services scan activity that shows up on your credit reports. They might monitor activity at one, two, or all three of the major credit bureaus — Equifax, Experian, and TransUnion.

Credit monitoring services will usually alert you when

- a company checks your credit history
- a new loan or credit card account appears on your credit reports
- a creditor or debt collector says your payment is late
- public records show that you filed for bankruptcy
- someone files a lawsuit against you
- your credit limit changes
- your personal information, like your name, address, or phone number, changes

Credit monitoring services will not alert you when

- someone withdraws money from your bank account
- someone uses your Social Security number to file a tax return and collect your refund

If you're considering using a credit monitoring service, here are some questions you can ask them:

- How often do you check credit reports for changes?
- Which of the three credit bureaus do you monitor?
- Is there a limit to how often I can review my credit reports?
- Will I be charged each time I review my credit reports?
- Are other services included, like access to my credit score?

Source: https://consumer.ftc.gov/articles/what-know-about-identity-theft

Identity Monitoring Services

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also might be offered by your bank or credit union, credit card provider. employer's benefits program, or insurance company.

Identity Monitoring Services

Companies that offer identity monitoring services check databases that collect different types of information to see if they contain new or inaccurate information about you. Those could be a sign that someone is using your personal information. These services can detect uses of your personal information that won't show up on your credit report.

Identity monitoring services may tell you when your information shows up in

- a change of address request
- court or arrest records
- orders for new utility, cable, or wireless services
- an application for a payday loan
- a request to cash a check
- on social media
- on websites that identity thieves use to trade stolen information

Most identity monitoring services will not alert you if someone uses your information to

- file a tax return and collect your refund
- get Medicare benefits
- get Medicaid benefits
- get welfare benefits
- claim Social Security benefits
- claim unemployment benefits

Source: https://consumer.ftc.gov/articles/what-know-about-identity-theft

Identity Recovery Services

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also might be offered by your bank or credit union, credit card provider. employer's benefits program, or insurance company.

Identity Recovery Services

Companies that sell credit and identity monitoring services also may offer identity recovery services to help you fix any damage caused by identity theft. These services may be included or cost extra. Some of the services they offer may be things you can do on your own for little or no cost.

Identity recovery services typically give you access to counselors or case managers who will help you recover your identity. They may

- help you write letters to creditors and debt collectors
- place a freeze on your credit report to prevent an identity thief from opening new accounts in your name
- guide you through documents you have to review

Some services will represent you in dealing with creditors or other institutions if you formally grant them authority to act on your behalf.

Source: https://consumer.ftc.gov/articles/what-know-about-identity-theft

Identity Theft Insurance

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also might be offered by your bank or credit union, credit card provider. employer's benefits program, or insurance company.

Identity Theft Insurance

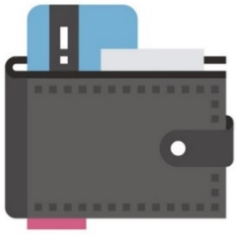
Companies that sell monitoring services also may offer identity theft insurance. These services may be included or cost extra.

Identity theft insurance may cover

- out-of-pocket expenses directly associated with reclaiming your identity, like
  - the cost of copying documents
  - postage costs for sending documents
  - costs for getting documents notarized
- wages you lost
- legal fees you paid

Identity theft insurance generally won't reimburse you for money stolen or financial loss resulting from the theft. Most policies won't pay if your loss is covered by your homeowner's or renter's insurance. If you're considering getting identity theft insurance, ask about the deductible and find out what's covered and what isn't.

Source: https://consumer.ftc.gov/articles/what-know-about-identity-theft



What to do if Your Personal Information is Lost or Exposed?

The Federal Trade Commission offers step-by-step guidance on what to do if your information has been lost or may have been stolen.

You can access this information at https://www.identitytheft.gov/#/Info-Lost-or-Stolen. The steps suggested by the Federal Trade Commission are also outlined below.

Did you recently get a notice that says your personal information was exposed in a data breach? Did you lose your wallet? Or learn that an online account was hacked?

Depending on what information was lost, there are steps you can take to help protect yourself from identity theft.

What Information was Lost or Exposed?

Social Security number

- If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
    - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.
    - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social

Security number to get a tax refund or a job. Respond right away to letters from the IRS.

- Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.

- Continue to check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year.

Online login or password

- Log in to that account and change your password. If possible, also change your username.

    - If you can't log in, contact the company. Ask them how you can recover or shut down the account.

- If you use the same password anywhere else, change that, too.

- Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Debit or credit card number

- Contact your bank or credit card company to cancel your card and request a new one.

- Review your transactions regularly. Make sure no one misused your card.

    - If you find fraudulent charges, call the fraud department and get them removed.

- If you have automatic payments set up, update them with your new card number.

- Check your credit report at annualcreditreport.com.

Bank account information

- Contact your bank to close the account and open a new one.

- Review your transactions regularly to make sure no one misused your account.

    - If you find fraudulent charges or withdrawals, call the fraud department and get them removed.

- If you have automatic payments set up, update them with your new bank account information.

- Check your credit report at annualcreditreport.com.

Driver's license information

- Contact your nearest motor vehicles branch to report a lost or stolen driver's license. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a duplicate.

- Check your credit report at annualcreditreport.com.

Children's personal information

- Request a credit freeze for your child — if this service is available in your state. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions for each credit bureau:

  Equifax: https://www.equifax.com/personal/education/identity-theft/freezing-your-childs-credit-report-faq/

  Experian: http://www.experian.com/help

  TransUnion: http://www.transunion.com/credit-help

- Generally, children won't have credit reports — unless someone is using their information for fraud. To find out if your child has a credit report, ask each credit bureau to check its records. Each bureau has specific instructions for these requests:

  Equifax: https://www.ai.equifax.com/CreditInvestigation/home/MinorChild.html

  Experian: https://www.experian.com/fraudalert Click on "Minor child instructions" under "Additional resources"

  TransUnion: https://www.transunion.com/personal-credit/credit-disputes/fraud-victim-resources/child-identity-theft-inquiry-form.page

- If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove fraudulent accounts.

More information about Child Identity theft can be found on the FTC's

website at
http://www.consumer.ftc.gov/articles/0040-child-identity-theft

What to Do In Case of Identity Theft

We've looked at what kinds of information are of high value to identity thieves: birthdates, Social Security numbers, and any personal facts which might be used to deceive a target for purposes of phishing. We've talked briefly about electronic data security and protecting your online activities.

But what do you do if you think the worst has happened and you are concerned that you have been the victim of identity theft?

The Federal Trade Commission has an online tool at:
https://www.identitytheft.gov/#/Steps
which will help direct you based on the specific form of suspected identity fraud.

This is an easy first step to get started. You can create a personal recovery plan online. The Federal Trade Commission's suggested steps for recovery are also provided here for easy reference.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- Change logins, passwords and PINS for your accounts.
    - You might have to contact these companies again after you have an FTC Identity Theft Report.

Step 2: Place a fraud alert and get your credit reports.

- Place a free, 90-day fraud alert by contacting one of the three credit bureaus. That company must tell the other two.
    - Experian.com/fraudalert
      1-888-397-3742
    - TransUnion.com/fraud
      1-800-680-7289
    - Equifax.com/CreditReportAssistance
      1-888-766-0008

  - A fraud alert is free. It will make it harder for someone to open new accounts in your name. When you have an alert on your report, a business must verify your identity before it issues new credit in your name. You can renew the fraud alert after 90 days.

  - You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.

- Get your free credit reports from Equifax, Experian, and TransUnion. Go to annualcreditreport.com or call 1-877-322-8228

- Due to the pandemic, you can check your reports every week for free through December 2022 at annualcreditreport.com.

- Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 3: Report identity theft to the FTC.

- Complete the online form at https://www.identitytheft.gov/#/assistant or call 1-877-438-4338. Include as many details as possible.

  - Based on the information you enter, IdentityTheft.gov will create your Identity Theft Report and recovery plan.

  - Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.

- If you create an account online, the site will walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away. Once you leave the page, you won't be able to access or update them.

- You may choose to file a report with your local police department. Go to your local police office with:

  - a copy of your FTC Identity Theft Report

  - a government-issued ID with a photo

- proof of your address (mortgage statement, rental agreement, or utilities bill)
- any other proof you have of the theft (bills, IRS notices, etc.)
- FTC's Memo to Law Enforcement, which can be found here: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0088-ftc-memo-law-enforcement.pdf

- Tell the police someone stole your identity and you need to file a report.
- Ask for a copy of the police report. You may need this to complete other steps.

What To Do Next

The Federal Trade Commission suggests taking these steps to begin to repair the damage caused by identity theft.

Close new accounts opened in your name.

If you have created an FTC Identity Theft Report, call the fraud department of each business where an account was opened.

- Explain that someone stole your identity.
- Ask the business to close the account.
- Ask the business to send you a letter confirming that:
  - the fraudulent account isn't yours;
  - you aren't liable for it; and
  - it was removed from your credit report.
- Keep this letter. Use it if the account appears on your credit report later on.

- The business may require you to send them a copy of your FTC Identity Theft Report or complete a special dispute form. The sample **Identity Theft Dispute Letter to a Company (for a new account)** in the appendix of this volume can help.

- Write down who you contacted and when.

Remove bogus charges from your accounts.

Call the fraud department of each business.

- Explain that someone stole your identity.

- Tell them which charges are fraudulent. Ask the business to remove them.

- Ask the business to send you a letter confirming they removed the fraudulent charges.

- Keep this letter. Use it if this account appears on your credit report later on.

- The business may require you to send them a copy of your FTC Identity Theft Report or complete a special dispute form. Use the **Sample Identity Theft Dispute Letter to a Company (for an existing account)** in the appendix of this volume as an example.

- Write down who you contacted and when.

Correct your credit report.

Write to each of the three credit bureaus, their contact information is below. The sample **Identity Theft Letter to a Credit Bureau** in the appendix of this volume can help.

- Include a copy of your FTC Identity Theft Report and proof of your identity, like your name, address, and Social Security number.

- Explain which information on your report came from identity theft.

- Ask them to block that information.

TransUnion.com
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax.com
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285

Experian.com
P.O. Box 9554
Allen, TX 75013

1-888-397-3742

- If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. Once the information is blocked, it won't show up on your credit report, and companies can't try to collect the debt from you. If you have an FTC Identity Theft Report, credit bureaus must honor your request to block this information.
- If you don't have an FTC Identity Theft Report, you still can dispute incorrect information in your credit file. It can take longer, and there's no guarantee that the credit bureaus will remove the information.
- **Consider adding an extended fraud alert or credit freeze.**
- Extended fraud alerts and credit freezes can help prevent further misuse of your personal information. There are

Extended Fraud Alert	Credit Freeze
Lets you have access to your credit report as long as companies take steps to verify your identity	Stops all access to your credit report unless you lift or remove it
Free to place and remove if someone stole your identity. Guaranteed by federal law.	Cost and availability depend on your state law. There might be a small fee for placing, lifting and removing.
Lasts for 7 years	Lasts until you lift or remove
Set it by contacting each of the three credit bureaus: • Report that someone stole your identity. Request an **extended** fraud alert. • Complete any necessary forms and send a copy of your FTC Identity Theft Report.	Set it by contacting each of the three credit bureaus. • Report that someone stole your identity. • Ask the company to put a freeze on your credit file. • Pay the fee required by state law
For fraud alerts: TransUnion.com 1-800-680-7289 Experian.com 1-888-397-3742 Equifax.com 1-888-766-0008	For credit freezes: TransUnion.com 1-888-909-8872 Experian.com 1-888-397-3742 Equifax.com 1-800-349-9960

important differences. The chart on the previous page can help you decide which might be right for you.

Other Possible Steps

Depending on your situation, the FTC suggests that you might need to take additional steps.

Report a misused Social Security number.

- If your Social Security card was lost or stolen, apply online at http://www.ssa.gov/ssnumber/ for free to get a replacement card.
- Do you think someone else is using your Social Security number for work? Review your Social Security work history by creating an account at socialsecurity.gov/myaccount. If you find errors, contact your local Social Security Administration office.

Stop debt collectors from trying to collect debts you don't owe.

- Write to the debt collector within 30 days of getting the collection letter. A sample letter to **Stop Debt Collectors from Trying to Collect Debts You Don't Owe** is included in the Appendix in this volume.
    - Tell the debt collector someone stole your identity, and you don't owe the debt.
    - Send copies of your Identity Theft Report and any other documents that detail the theft.
- Contact the business where the fraudulent account was opened.
    - Explain that this is not your debt.
    - Tell them to stop reporting this debt to the credit bureaus.
    - Ask for information about the debt, and how it happened. The business must give you details if you ask. A sample letter for **Getting Business Records Relating to Identity Theft** is included in the Appendix in this volume.
- For example, if someone opened a credit card in your name, ask for a copy of the

application and the applicant's signature.

- If you haven't already, ask the credit bureaus to block information about this debt from your credit report.
    - The advice in Disputing Errors on Credit Reports can help you block fraudulent information from your credit reports.
- Write down who you contacted and when. Keep copies of any letters you send.

Replace government-issued IDs.

- If your Social Security card was lost or stolen, apply online at http://www.ssa.gov/ssnumber/ for free to get a replacement card.
- If your Driver's license was lost or stolen, contact the nearest DMV branch to report it.
    - The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a replacement license.
- If your Passport was lost or stolen, call the State Department at 1-877-487-2778 or TTY 1-888-874-7793. If you want to replace the passport, you have several options:
    - If you are traveling within two weeks of the loss, make an appointment to apply in person at a Passport Agency or Center.
    - If you are not traveling within two weeks of the loss, submit Form DS-11 https://eforms.state.gov/Forms/ds11.PDF and DS-64 https://eforms.state.gov/Forms/ds64.PDF in person at an authorized Passport Application Acceptance Facility.

Clear your name of criminal charges.

If someone is arrested and uses your name or personal information, contact the law enforcement agency that arrested the thief. You may need to check court records to find out where the thief was arrested.

- File a report about the impersonation.
- Give copies of your fingerprints, photograph, and identifying documents.
- Ask the law enforcement agency to:

  - compare your information to the imposter's
  - change all records from your name to the imposter's name (if you know it)
  - give you a "clearance letter" or "certificate of release" to declare your innocence

- Keep the clearance letter or "certificate of release" with you at all times.
- Write down who you contacted and when.

If a court prosecutes an identity thief using your name, contact the court where the arrest or conviction happened.

- Ask the district attorney for records to help you clear your name in court records.
- Provide proof of your identity.
- Ask the court for a "certificate of clearance" that declares you are innocent.
- Keep the "certificate of clearance" with you at all times.

Contact your state Attorney General.

- Contact information for all state Attorney General's offices are listed in the appendix in this volume.
  - Ask if your state has an "identity theft passport" (a tool you can use to resolve financial issues related to the identity theft) or some other special help for identity theft victims.
  - If you get an identity theft passport, keep it with you at all times.
- Consider hiring a criminal defense lawyer. The American Bar Association can help you find a lawyer. Visit https://www.americanbar.org/groups/legal_services/flh-home/flh-bar-directories-and-lawyer-finders/ for more information.
- Ask the law enforcement agency that arrested the thief which information brokers buy their records.
  - Write to the brokers. Ask them to remove errors from your file.
  - Information brokers buy criminal records and sell

information to employers and debt collectors.

- Write down who you contacted and when. Keep copies of any letters you send.

Additional Steps for Certain Types of Accounts

The Federal Trade Commission has outlined some additional steps for other types of accounts that may have been impacted by identity theft.

Utilities

- If someone used your information to get cable, electric, water, or other similar services, contact the service provider.
    - Tell them someone stole your identity.
    - Ask them to close the account.
- For additional help, contact your state Public Utility Commission and explain the situation.
- Write down who you contacted and when. Keep copies of any letters you send.

Phones

- Contact the National Consumer Telecom and Utilities Exchange and request your NCTUE Data Report. Review it for any accounts you don't recognize.

  www.nctue.com
  1-866-349-5185

- The NCTUE data report is a record of all telecommunication, pay TV and utility accounts reported by exchange members, including information about your account history, unpaid accounts and customer service applications.
- If the service provider doesn't resolve the problem, file a complaint with the Federal Communications Commission at 1-888-225-5322 or TTY 1-888-835-5322.

Government Benefits

- Contact the agency that issued the government benefit and explain that someone stole your identity. You can find local government agencies at https://www.usa.gov/local-governments.
    - For Social Security Benefits, contact the Social Security Administration Office of

the Inspector General at www.socialsecurity.gov/oig or 1-800-269-0271.

- Ask what you need to do to fix the problem.
- If you stopped receiving your benefits because of the identity theft, ask what you need to do to get them reinstated. You may need to appear in person or send something in writing.
- Make a note of who you contacted and when.

Checking accounts

- Do you think someone opened a checking account in your name? Order a free copy of your ChexSystems report, which compiles information about your checking accounts.
- To get your report, contact ChexSystems at 1-800-428-9623. Or visit their website http://consumerdebit.com.
- Then contact every financial institution where a new account was opened. Ask them to close the accounts.
- If someone is writing bad checks against your account, contact your financial institution.
- Ask them to stop payment on stolen checks and close your account.
- Ask them to report the theft to its check verification system. The check verification system will tell businesses to refuse the stolen checks.
- Also, contact any business that took the bad check. Explain that someone stole your identity. Act quickly, before they start collection action against you.
- You also can contact check verification companies. Report that your checks were stolen. Ask them to tell businesses to refuse the stolen checks.

  Telecheck 1-800-710-9898
  Certegy 1-800-437-5120

- If a business rejects your checks, ask the business for an explanation. The business must tell you what information led them to reject your check.
- Write down who you contacted and when. Keep copies of any letters you send.

Student loans

- Contact the school or program that opened the loan.

  - Explain the situation.
  - Ask them to close the loan, and send you a letter that says you aren't responsible for the loan.

- If this is a federal student loan, contact the U.S. Department of Education Office of Inspector General hotline at 1-800-MISUSED (1-800-647-8733) or visit http://www.ed.gov/about/offices/list/oig/hotline.html.

- If these steps don't resolve your situation, contact the U.S. Department of Education Federal Student Aid Ombudsman at 1-877-557-2575 or at https://studentaid.ed.gov/repay-loans/disputes/prepare/contact-ombudsman.

- Write down who you contacted and when. Keep copies of any letters you send.

Apartment or House Rentals

- Ask the landlord who rented the property to the identity thief what tenant history services they use. Contact those companies. Ask for a copy of your tenant history report, and ask what steps you need to take to correct fraudulent information in the report.

- What's a tenant history report? There are several companies that collect and sell information about renters – such as how often a renter was late or if a renter has ever been evicted. If someone leased an apartment in your name, you'll want to correct any errors in your tenant history reports.

- Write down who you contacted and when. Keep copies of any letters you send.

Investment accounts

- Call your broker or account manager, and describe the situation.

- Write down who you contacted and when. Keep copies of any letters you send.

Bankruptcy filed in your name

- Write to the U.S. Trustee in the region where the bankruptcy was filed. Describe the situation and provide proof of your identity. You can find a list of U.S. Trustee offices here: http://www.usdoj.gov/ust

- The U.S. Trustee Program refers cases of suspected bankruptcy fraud to the U.S. Attorneys for possible prosecution. The U.S. Trustee can't give you legal help, so

you may need to hire an attorney.

- Consider hiring an attorney. The American Bar Association or a local legal services provider can help you find a lawyer.
- An attorney can explain to the court that the bankruptcy filing was fraudulent.
- Write down who you contacted and when. Keep copies of any letters you send.

Special Forms of Identity Theft

The Federal Trade Commission also offers specific guidance for additional areas of identity theft.

Tax Identity Theft

- If you get an IRS notice in the mail that says someone used your Social Security number to get a tax refund, follow the instructions provided in the letter.
- Did the notice say you were paid by an employer you don't know? Send a letter to the employer too, explaining that someone stole your identity, and that you don't work for the employer.
- Complete IRS Identity Theft Affidavit (Form 14039), available for download here: https://www.irs.gov/pub/irs-pdf/f14039.pdf. Mail or fax the form according to the instructions.
- File your tax return, and pay any taxes you owe.
- You might have to mail paper tax returns.
- Write down who you contacted and when. Keep copies of any letters you send.
- If these steps don't resolve your situation, contact the IRS for specialized assistance at 1-800-908-4490.
- Place a fraud alert. Contact one of the three credit bureaus. That company must tell the other two.

  TransUnion.com/fraud
  1-800-680-7289

  Experian.com/fraudalert
  1-888-397-3742

  Equifax.com/CreditReportAssistance
  1-888-766-0008

- Get your free credit reports from TransUnion, Experian, and Equifax. Go to annualcreditreport.com or call 1-877-322-8228

- Review your reports. If you find any accounts or charges you don't recognize, follow the steps in **What to Do Next** on page 33 or visit https://www.identitytheft.gov/Steps.

Child Identity Theft

- Did someone use your child's information to commit fraud? Call the company where the fraud occurred.

- Explain that someone stole your child's identity and opened a fraudulent account. Explain that your child is a minor, and cannot enter into legal contracts.

- Ask them to close the fraudulent account and send you a letter confirming that your child isn't liable for the account.

- Send a follow-up letter and include the Minor's Status Declaration, available here: https://www.consumer.ftc.gov/articles/pdf-0095-uniform-minor-status-declaration.pdf, and a copy of your child's birth certificate.

- Make a note of who you contacted and when.

- To find out if your child has a credit report, request a manual search for your child's Social Security number. Each credit bureau has its own process for this:

  Experian: https://www.experian.com/fraud/center.html,click on "Minor child instructions" under "Additional resources"

  TransUnion: https://www.transunion.com/credit-disputes/child-identity-theft-inquiry-form

  Equifax: https://www.ai.equifax.com/CreditInvestigation/home/MinorChild.html

- Why check for a credit report? Generally, children won't have credit reports — unless someone is using their information for fraud.

- If a credit bureau has a credit report for your child, they will send you a copy of the report. To remove fraudulent accounts, follow the instructions provided with the credit report.

- Request a freeze to make it more difficult for someone to use your child's Social Security number to open accounts. To place a freeze, follow the specific instructions for each credit bureau:

  Equifax: https://www.equifax.com/personal/credit-report-services

  Experian: https://www.experian.com/help

  TransUnion: https://www.transunion.com/credit-help

- Did someone file taxes using your child's Social Security number? Complete IRS Identity Theft Affidavit (Form 14039), available here: https://www.irs.gov/pub/irs-pdf/f14039.pdf. Mail or fax the form according to the instructions. If that doesn't resolve the problem, contact the IRS for specialized assistance at 1-800-908-4490.

Medical Identity Theft

- If you suspect that someone used your information to get medical services, get copies of your medical records.

- Contact each doctor, clinic, hospital, pharmacy, laboratory, and health plan where the thief may have used your information. Ask for copies of your medical records.

- Complete the providers' records request forms and pay any fees required to get copies of your records.

- Check your state's health privacy laws. Some state laws make it easier to get copies of your medical records.

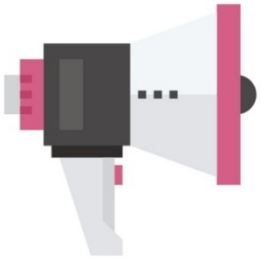
- Federal law gives you the right to know what's in your medical files.

- Did your provider refuse to give you copies of the records to protect the identity thief's privacy rights? You can appeal. Contact the person listed in your provider's Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file.

- If the provider refuses to provide your records within 30

days of your written request, you may complain to the U.S. Department of Health and Human Services Office for Civil Rights. You can contact them online at https://www.hhs.gov/ocr/index.html.

- Review your medical records, and report any errors to your health care provider.
- Write to your health care provider to report mistakes in your medical records.
- Include a copy of the medical record showing the mistake.
- Explain why this is a mistake, and how to correct it.
- Include a copy of your FTC Identity Theft Report, if you have created one.
- Send the letter by certified mail, and ask for a return receipt.
- Your health care provider should respond to your letter within 30 days. Ask the provider to fix the mistake and notify other health care providers who may have the same mistake in their records.
- Notify your health insurer.
- Send your FTC Identity Theft Report to your health insurer's fraud department. Tell them about any errors in your medical records.
- If there are medical billing errors on your credit report, notify all three credit reporting companies by following the steps under **What to Do Next** on page 33.
- Write down who you contacted and when. Keep copies of any letters you send.



Disputing Fraudulent Charges

The Federal Trade Commission provides sample letters to help consumers dispute fraudulent charges if they have been the victim of identity theft. Copies of these sample letters are included in the Appendix in this volume. Sample letters include:

- **Dispute Credit Card Charges**
- **Dispute ATM/Debit Card Transactions**
- **Dispute Letter to a Credit Bureau**

- **Dispute Letter to a Company, for a new account**
- **Dispute Letter to a Company, for an existing account**
- **Identity Theft Letter to a Debt Collector**
- **Request Letter for Getting Business Records Related to Identity Theft**

Fixing the damage to your credit can be a long and tedious process. You'll probably have to dispute every fraudulent transaction not only with the companies involved but with the credit reporting companies, too.

Impact of Identity Theft

Millions of people every year are targets of identity theft, and the impact on victims is often quite serious. Identity theft victims not only have to deal with the financial consequences and considerable amounts of record keeping and follow up to clear their record, but they can also suffer emotionally, with loss of sleep, increased stress levels, the inability to trust others and feelings of powerless or helpfulness[5].

The financial cost is equally high. According to the FTC, 2.8 million fraud reports were collected in 2021, and an estimated $5.8 billion was lost to fraud—an increase of 70% over 2020. In addition to any personal financial losses or legal problems, identity theft can impact your credit score and, from there, it can negatively affect such things as job applications, car insurance rates, and more.

Protect Your Identity by Keeping Personal Information Private

There are many steps you can take to minimize your risk of identity theft. You can do things like shred documents that you don't keep, refuse to give out your phone number or Social Security number when not absolutely necessary, and be aware of your surroundings when using an ATM or a credit card.

The more diligent you are in protecting your personal information, and the personal information of your children or family members, the more

[5] https://www.idtheftcenter.org/aftermath2018/

likely it will be that your information won't fall into the hands of someone who will misuse that information.

Protect Yourself from Other Types of Scams

Identity theft is not the only danger you have to look out for online. Each year, more and more scams are reported to the FTC.

In the next section, you can read about some of the most common scams, and how to protect yourself.

- How to Recognize Spam Text Messages
- Paying Scammers with Gift Cards
- How to Recognize and Avoid Phishing Scams
- Utility Company Scams
- Online Car Sales Scams
- Auto Warranty Scams
- Charities
- Credit Repair Scams
- High School Diploma Scams
- College Degree Scams
- Job Scams
- Nanny and Caregiver Job Scams
- Cryptocurrency Scams
- Foreclosure Rescue Scams
- Refund & Recovery Scams
- Government Imposter Scams
- Fake Check Scams
- Money Transfer Scams
- Deceptive Mortgage Ads
- Romance Scams
- Travel Scams
- Tech Support Scams
- Health Scams
- Health Care Scams
- Telephone Scams

How to Recognize Spam Text Messages

Scammers send fake text messages to trick you into giving them your personal information – things like your password, account number, or Social Security number. If they get that information, they could gain access to your email, bank, or other accounts. Or they could sell your information to other scammers.

The scammers use a variety of ever-changing stories to try to rope you in. They may promise free prizes, gift cards or coupons, offer you a low or no interest credit card, or promise to help you pay off your student loans. Scammers also send fake messages that say they have some information about your account or a transaction. The scammers may say they've noticed some suspicious activity on your account, claim there's a problem with your payment information, send you a fake invoice and tell you to contact them if you didn't authorize the purchase, or send you a fake package delivery notification.

The messages might ask you to give some personal information — like how much money you make, how much you owe, or your bank account, credit card, or Social Security number — to claim your gift or pursue the offer. Or they may tell you to click on a link to learn more about the issue. Some links may take you to a spoofed website that looks real but isn't. If you log in, the scammers can then steal your user name and password. Other messages may install harmful malware on your phone that steals your personal information without you realizing it.

If you get a text message that you weren't expecting and it asks you to give some personal information, don't click on any links. Legitimate companies won't ask for information about your account by text. If you think the message might be real, contact the company using a phone number or website you know is real. Not the information in the text message.

Here's how you can filter unwanted text messages or stop them before they reach you.

- **On your phone:** Your phone may have an option to filter and block messages from unknown senders or spam.
- **Through your wireless provider**: Your wireless provider may have a tool or service that lets you block calls and text messages. Check ctia.org, a website for the wireless industry, to learn about the options from different providers.
- **With a call-blocking app**: Some call-blocking apps also let you block unwanted text messages. Go to ctia.org for a list of call-blocking apps for Android, BlackBerry, Apple, and Windows phones.

You can also search for apps online. Check out the features, user ratings, and expert reviews.

Source: https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

Paying Scammers with Gift Cards

Gift cards are a popular and convenient way to give someone a gift. They're also a popular way for scammers to steal money from you. That's because gift cards are like cash: if you buy a gift card and someone uses it, you probably cannot get your money back. Gift cards are for gifts, not payments. Anyone who demands payment by gift card is always a scammer. Many different kinds of imposters ask you to pay with gift cards. Someone might call you and claim to be from the IRS, collecting back taxes or fines. The caller might say he's from tech support, asking for money to fix your computer. The caller might even say she's a family member with an emergency and needs money right now.

But they all have in common an urgent need for you to send money right away. Imposters will sometimes ask you to wire money to them but, increasingly, they tell you to go put money on a gift card. Here's what happens: the caller will often tell you to go buy a popular gift card, frequently, iTunes, Google Play, or Amazon. The caller will tell you to get the card at a particular store near you – often Walmart, Target, Walgreens, or CVS. They may even have you buy several cards at several stores. Sometimes, the caller will stay on the phone with you while you go to the store. Once you buy the card, the caller then will demand the gift card number and PIN on the back of the card. Those numbers let them immediately get the money you loaded onto the card. And once they've done that, the scammers and your money are gone, usually without a trace.

Other kinds of scammers, some of them also imposters, who might demand payment by gift card include:

- sellers on online auction sites who ask for gift cards to "buy" big items like cars, motorcycles, boats, RVs, tractors and electronics
- someone posing as a service member to get your sympathy, saying he has to sell something quickly before deployment and needs you to pay by gift card

These are all scams. In fact, if anyone tells you to pay by gift card, or by wiring money – for any reason – that's a sure sign of a scam. Every time.

If you paid a scammer with a gift card, tell the company that issued the card right away. When you contact the company, tell them the gift card was used in a scam. Ask them if money is still on the card, and if they can refund your money. If you act quickly enough, the company might be able to get your money back. Be aware that some companies will not return any money even if the gift card hasn't been used. Remember to keep the gift card itself, and keep the gift card receipt. Also, tell the store where you bought the gift card as soon as possible.

Source: https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

Four Steps to Protect Yourself From Phishing

1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

(continued on next page)

How to Recognize and Avoid Phishing Scams (con't)

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

    - Something you have — like a passcode you get via text message or an authentication app.

    - Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What to Do If You Suspect a Phishing Attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: Do I have an account with the company or know the person that contacted me?

If the answer is "No," it could be a phishing scam. Go back and review the tips in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message and then delete it.

If the answer is "Yes," contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

Source: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Utility Company Scams

A call from your gas, electric, or water company threatening to immediately turn off your service is probably a scam. Here's what you need to know.

How Utility Scams Work

Someone calls claiming to be from your gas, water, or electric company. They say your service will be cut off if you don't pay them immediately. This is a scam. Real utility companies don't do this. But these scammers want to scare you into paying, before you have time to confirm what they're telling you.

The caller goes on, telling you to pay by wiring money through a company like Western Union or MoneyGram, giving the caller the numbers of a reloadable card or gift card, or paying them with cryptocurrency. Scammers tell you to pay this way because it's hard to track that money, and almost impossible to get it back.

How To Avoid Utility Scams

Hang up and call the utility company yourself. Call the company using the number on your bill or the utility company's website even if the person who contacted you left a call-back number. Often times, those call-back numbers are fake. If the message came by text, don't respond and do the same. If your bill says you owe anything, pay it as you normally would, not as the caller says.

Never wire money or pay with a reloadable card, gift card, or cryptocurrency to anyone who demands it. Only scammers will require one of those kinds of payment. Your utility company won't ask you to pay that way. Once you send the money, you probably won't get it back.

If you're actually behind on your utility bills, visit https://www.consumer.ftc.gov/articles/getting-utility-services-why-your-credit-matters to learn more about your options.

What To Do If You Paid a Scammer

- Scammers often ask you to pay in ways that make it tough to get your money back. No matter how you paid a scammer, the sooner you act, the better. Learn more about how to get your money back at https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed#Paid.

Source: https://consumer.ftc.gov/articles/scammers-pretend-be-your-utility-company

Online Car Sales Scams

You can buy practically anything online, including used cars. But before you shell out any hard-earned cash, here's a warning about scammers trying to sell cars they don't have or own.

Here's how the scam works: Criminals post ads on online auction and sales websites, like eBay Motors, for inexpensive used cars (that they don't really own). They offer to chat online, share photos, and answer questions. They may even tell you the sale will go through a well-known retailer's buyer protection program. Recently, sellers have been sending fake invoices that appear to come from eBay Motors and demanding payment in eBay gift cards. If you call the number on the invoice, the scammer pretends to work for eBay Motors. Trusting buyers have lost hundreds of thousands of dollars over the past year alone.

So how can you tell if an online car sale is fake?

- **You find bad reviews online**. Check out the seller by searching online for the person's name, phone number and email address, plus words like "review," "complaint" or "scam."

- **Sellers try to rush the sale**. Resist the pressure. Scammers use high-pressure sales tactics to get you to buy without thinking things through.

- **They can't or won't meet in person or let you inspect the car**. Scammers might have an excuse, like a job transfer, military deployment, or divorce, for why you can't see them or the car. But experts agree that you should have an independent mechanic inspect a used car before you buy it.

- **They want you to pay with gift cards or by wire transfer**. If anyone tells you to pay that way, it's a scam. Every time.

- **The sellers demand more money after the sale** for "shipping" or "transportation" costs.

- The **Vehicle Identification Number (VIN) doesn't match the VIN for the car you're interested in**. A vehicle history report can help you spot such discrepancies.

Source: https://www.consumer.ftc.gov/blog/2019/06/put-brakes-phony-online-car-sales

Auto Warranty Scams

Be skeptical of mail and phone calls warning that the warranty on your car is about to expire. The companies behind the letters and calls may give the impression they represent your car dealer or manufacturer. With phrases like Motor Vehicle Notification, Final Warranty Notice or Notice of Interruption, they are trying to make the offer seem urgent — and to get you to call a toll-free number for more information. Investigate before you buy.

More than likely, these pitches are from unrelated businesses that want to sell you extended warranties — more accurately known as service contracts — that often sell for hundreds or thousands of dollars. If you respond to a call from a business pitching so-called extended warranties, you're likely to hear high-pressure sales tactics, as well as demands for personal financial information and a down payment, before you get any details about the service contract. And if you buy a service contract, you may find that the company behind it won't be in business long enough to fulfill its commitments.

If you get mail or phone calls about renewing your vehicle warranty, don't take the information at face value. Your vehicle's warranty may be far from expiring — or it may have expired already. If you have a question about your warranty, check your owner's manual, call the dealer who sold you the car, or contact the vehicle manufacturer.

Be alert to fast talkers. Telemarketers pitching auto warranties often use high-pressure tactics to hide their true motive. Take your time. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.

Never give out personal financial or other sensitive information like your bank account, credit card or Social Security numbers – even your driver's license number or Vehicle Identification Number (VIN) – unless you know who you're dealing with. Scam artists often ask for this information during an unsolicited sales pitch, and then use it to commit other frauds against you.

Be skeptical of any unsolicited sales calls and recorded messages. If your phone number is on the National Do Not Call Registry: You shouldn't get live or recorded sales pitches unless you have specifically agreed to accept such calls, bought something from the company within the last 18 months, or asked the company for information within the last three months.

Source: https://www.consumer.ftc.gov/articles/0054-auto-service-contracts-and-warranties

Charities

How to avoid donating to a sham charity:

- Don't let anyone rush you into making a donation. That's something scammers do.
- Don't feel pressured to donate. Scammers will say anything to get you to give them money. They may say you already pledged to make the donation, or that you donated to them last year. They may even send you a mailer that says you already pledged. Don't let that pressure you into paying what could be a scammer.
- Don't trust your caller ID. Technology makes it easy for scammers to have caller ID say the call comes from anywhere, including your local area code, or from a particular name. In reality, the caller could be anywhere in the world. If you want your donation to help your local community, ask questions about where your donation will be used and how much of your donation will be spent there.
- Check out the name of the charity, especially if it sounds like a well-known organization. Some scammers use names that sound a lot like other charities to trick you.
- Watch out for solicitations that give lots of vague and sentimental claims, but give you no specifics about how your donation will be used.
- If someone is guaranteeing you sweepstakes winnings in exchange for a contribution, that's a scam.

Source: https://www.consumer.ftc.gov/articles/0074-giving-charity

Credit Repair Scams

You'll know you're encountering credit repair fraud if a company:

- insists you pay them before they do any work on your behalf
- tells you not to contact the credit reporting companies directly
- tells you to dispute information in your credit report — even if you know it's accurate
- tells you to give false information on your applications for credit or a loan
- doesn't explain your legal rights when they tell you what they can do for you

Ads That Promise a "New Credit Identity"

Companies promising a "new credit identity" say they can help you hide bad credit history or bankruptcy for a fee. If you pay them, these companies will provide you with a nine-digit number that looks like a Social Security number. They may call it a CPN — a credit profile number or a credit privacy number. Or, they may direct you to apply for an EIN — an Employer Identification Number — from the Internal Revenue Service (IRS). EIN's are legitimate numbers, typically used by businesses to report financial information to the IRS and Social Security Administration — but an EIN is not a substitute for your Social Security number.

The credit repair companies may tell you to apply for credit using the CPN or EIN, rather than your own Social Security number. And they may lie and tell you that this process is legal. But it's a scam. These companies may be selling stolen Social Security numbers, often those taken from children. By using a stolen number as your own, the con artists will have involved you in identity theft.

If you follow a credit repair company's advice and commit fraud, you might find yourself in legal trouble. It's a federal crime to: lie on a credit or loan application, misrepresent your Social Security number, or obtain an EIN from the IRS under false pretenses. The bottom line is that if you use the number they sell you, you could face fines or time in prison.

Source: https://www.consumer.ftc.gov/articles/0225-credit-repair-scams

High School Diploma Scams

Here are some signs you've come across a High School Diploma scam:

You can get the diploma from home, ASAP

No classes? No in-person test? All online? That's a scam. Legitimate programs with classes for credit mean you'll invest weeks or months of time. And real high school equivalency tests are offered at specific days and times, not on-demand. Most people don't pass without really studying.

You have to pay for a diploma

No legitimate high school equivalency program lets you take a test or classes for free, then charges you for the diploma. You might pay for classes or testing, but you shouldn't have to pay for the diploma itself.

They claim to be affiliated with the federal government

The federal government doesn't offer programs for earning high school diplomas. Legitimate tests or programs are approved by your state.

Source: https://www.consumer.ftc.gov/articles/0539-high-school-diploma-scams

College Degree Scams

Though many online schools and distant learning programs are legitimate, there are some organizations that peddle bogus degrees.

A "diploma mill" is a company that offers "degrees" for a flat fee in a short amount of time and requires little to no course work. Degrees awarded through diploma mills are not legitimate, and can cost you more than just your money.

If you're getting a degree without doing any work, chances are you're dealing with a diploma mill. Legitimate colleges or universities — including online schools — require substantial course work and interaction with professors.

"Get a Degree for Your Experience!"

Diploma mills grant degrees for "work or life experience" alone. Accredited colleges may give a few credits for specific experience relevant to a degree program, but not an entire degree.

Flat Fee

Many diploma mills charge on a per-degree basis. Legitimate colleges charge by the credit, course, or semester — not a flat fee for an entire degree.

No Waiting

Though there are schools that offer accelerated degrees in-person or online, earning a degree still takes some time. If an ad promises that you can earn a degree in a few days, weeks, or even months, it's probably a diploma mill.

Pushy Advertising Tactics

Some diploma mills push themselves through aggressive sales tactics. Legitimate institutions, including distance learning programs, won't advertise through spam or pop-ups. They won't use high-pressure telemarketing calls, either.

Source: https://www.consumer.ftc.gov/articles/0206-college-degree-scams

Job Scams

Scammers advertise jobs the same way legitimate employers do — online (in ads, on job sites, and social media), in newspapers, and sometimes on TV and radio. They promise you a job, but what they want is your money and your personal information.

Work-from-home job scams

Many people would like to work from home and generate income. Scammers know this, so they place ads, often online, claiming that they have jobs where you can make thousands of dollars a month working from home with little time and effort. Sometimes the scammers try to get you interested by saying that you can be your own boss, start your own business, or set your own schedule.

But instead of making money, you end up paying for starter kits, "training," or certifications that are useless. You might also find that your credit card is charged without your permission, or you get caught up in a fake check scam. If someone offers you a job and they claim that you can make a lot of money in a short period of time and with little work, that's a scam.

How to Avoid a Job Scam

Before you accept a job offer, and certainly before you pay for one, take these steps to protect yourself from job scams:

Do an online search. Look up the name of the company or the person who's hiring you, plus the words "scam," "review," or "complaint." You might find out they've scammed other people.

Talk to someone you trust. Describe the offer to them. What do they think? This also helps give you vital time to think about the offer.

Don't pay for the promise of a job. Legitimate employers, including the federal government, will never ask you to pay to get a job. Anyone who does is a scammer.

Never bank on a "cleared" check. No legitimate potential employer will ever send you a check and then tell you to send on part of the money, or buy gift cards with it. That's a fake check scam. The check will bounce, and the bank will want you to repay the amount of the fake check.

Source: https://consumer.ftc.gov/articles/job-scams

Nanny and Caregiver Job Scams

If you're looking for a job as a nanny or caregiver, you might have searched online or used particular websites that provide employment matching services. Searching online or using employment matching websites can be useful for finding jobs, but scammers can also post fake job ads designed to trick you into sending money or sharing personal information.

Here are a few things to watch out for:

Be suspicious if you're offered a job and hired without an interview in person or over the phone. Scammers might say they're out of town or too busy, or come up with other excuses for not talking to you on the phone or meeting you in person.

If you get a check before you even start working, it could be a fake check scam. The person hiring you might say it's your first paycheck, or that it's to buy supplies or for expenses related to caring for their loved one. But later they'll tell you to send part of the money to someone else, or return it to them. They'll come up with excuses, like they overpaid you, they need the money to pay for unexpected medical bills, or some other emergency. The check is fake, and by the time the bank realizes it, the scammer has your money, and the bank will want you to repay the money you withdrew.

Here's what to do if you get a job offer:

Check out potential employers before giving them any sensitive information. Search online for their name, email address, phone number, and even the text of the message they sent. You might find that others have had bad experiences and been scammed by the same people, or in a similar way.

Don't send money to your potential boss. Your employer should pay you, not the other way around. Don't believe any story about why your employer sent you a check for more than you expected to be paid, and why you need to send some of that money back. And if your new employer asks you to send them money through a gift card or wire transfer, don't do it. It's a scam and that's not a real job.

Get as many details in writing as you can. Ask the potential employer to send you details of the job duties, the pay, and the hours. If they refuse, that could be a sign of a problem.

Source: https://consumer.ftc.gov/articles/nanny-caregiver-job-scams

Cryptocurrency Scams

Scammers are always finding new ways to steal your money using cryptocurrency. One sure sign of a scam is anyone who says you have to pay by cryptocurrency. In fact, anyone who tells you to pay by wire transfer, gift card, or cryptocurrency is a scammer. Of course, if you pay, there's almost no way to get that money back. Which is what the scammers are counting on.

Here are some cryptocurrency scams to watch out for.

Investment and business opportunity scams

- Some companies promise that you can earn lots of money in a short time and achieve financial freedom.
- Some scammers tell you to pay in cryptocurrency for the right to recruit others into a program. If you do, they say, you'll get recruitment rewards paid in cryptocurrency. The more cryptocurrency you pay, the more money they promise you'll make. But these are all fake promises, and false guarantees.
- Some scammers start with unsolicited offers from supposed "investment managers." These scammers say they can help you grow your money if you give them the cryptocurrency you've bought. But once you log in to the "investment account" they opened, you'll find that you can't withdraw your money unless you pay fees.
- Some scammers send unsolicited job offers to help recruit cryptocurrency investors, sell cryptocurrency, mine cryptocurrency, or help with converting cash to bitcoin.
- Some scammers list scam jobs on job websites. They'll promise you a job (for a fee), but end up taking your money or personal information.

Look for claims like these to help you spot the companies and people to avoid:

- Scammers guarantee that you'll make money. If they promise you'll make a profit, that's a scam. Even if there's a celebrity endorsement or testimonials. (Those are easily faked.)
- Scammers promise big payouts with guaranteed returns. Nobody can guarantee a set return, say, double your money. Much less in a short time.
- Scammers promise free money. They'll promise it in cash or cryptocurrency, but free money promises are always fake.
- Scammers make big claims without details or explanations. Smart business people want to understand how their investment works, and where their money is going. And good investment advisors want to share that information.

Before you invest, check it out. Research online for the name of the company and the cryptocurrency name, plus words like "review," "scam," or "complaint." See what others are saying. And read more about other common investment scams.

Source: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams

Foreclosure Rescue Scams

Scammers are targeting people having trouble paying their mortgages. If you are in danger of foreclosure, AVOID any individual or company that:

Requires a fee in advance

Don't pay any business, organization, or person who promises to prevent foreclosure or guarantees you a new mortgage. So-called "foreclosure rescue companies" claim they can help save your home, but they can't really do that. They're just out to make a fast buck. Some may ask for hefty fees in advance – and then, once you pay, stop returning your calls. Others may string you along before disclosing their charges. Cut off all dealings if someone insists on a fee in advance.

Promises to find mistakes in your loan documents that will force your lender to cancel or modify your loan

Cancelling your loan won't allow you to stay in your home, and in most cases, lenders are not required to modify your loan to make it more affordable simply because of mistakes in your loan documents.

Guarantees to stop a foreclosure

Don't do business with anyone who offers an "easy out" of foreclosure. These kinds of claims are the tell-tale signs of a foreclosure rip-off: "We can stop your foreclosure!" "97% success rate!" "Guaranteed to save your home!"

Advises you to stop paying your mortgage company or stop talking to your mortgage company

Some scammers offer to handle financial arrangements for you, and then pocket your payment instead of sending it to your mortgage company. Send your mortgage payments ONLY to your mortgage company. Scammers may advise you not to communicate with your mortgage company. That's a bad idea because you may not find out until it's too late that the scammer has done nothing for you, that your mortgage company was willing to modify your loan, or even that foreclosure is just days away!

Source: https://www.consumer.ftc.gov/articles/0193-facing-foreclosure

Refund & Recovery Scams

Many consumers might not know that they have been scammed by a bogus prize promotion, phony charity drive, fraudulent business opportunity or other scam. But if you have unknowingly paid money to such a scam, chances are your name is on a "sucker list." That list may include your address, phone numbers, and other information, like how much money you've spent responding to phony offers. Dishonest promoters buy and sell "sucker lists" on the theory that people who have been deceived once have a high likelihood of being scammed again.

These scammers lie when they promise that, for a fee or a donation to a specific charity, they will recover the money you lost, or the prize or product you never received. They use a variety of lies to add credibility to their pitch: some claim to represent companies or government agencies; some say they're holding money for you; and others offer to file necessary complaint paperwork with government agencies on your behalf. Still others claim they can get your name at the top of a list for victim reimbursement.

Here are some tips to help you avoid losing money to a recovery scam:

Don't give money or your bank or credit card account number to anyone who calls offering to recover money, merchandise, or prizes you never received if the caller says you have to pay a fee in advance. Under the Telemarketing Sales Rule, it's against the law for someone to request or receive payment from you until seven business days after you have the money or other item in hand.

If someone claims to represent a government agency that will recover your lost money, merchandise, or prizes for a fee or a donation to a charity, report them immediately to the FTC. National, state, and local consumer protection agencies and nonprofit organizations do not charge for their services.

Before you use any company to recover either money or a prize, ask what specific services the company provides and the cost of each service. Check out the company with local government law enforcement and consumer agencies; ask whether other people have registered complaints about the business. You also can enter the company name into an online search engine to look for complaints.

Source: https://www.consumer.ftc.gov/articles/0102-refund-and-recovery-scams

Government Imposter Scams

Scammers sometimes pretend to be government officials to get you to send them money. They might promise lottery winnings if you pay "taxes" or other fees, or they might threaten you with arrest or a lawsuit if you don't pay a supposed debt. Regardless of their tactics, their goal is the same: to get you to send them money.

Don't do it. Federal government agencies and federal employees don't ask people to send money for prizes or unpaid loans. Nor are they permitted to ask you to wire money or add money to a prepaid debit card to pay for anything.

Don't wire money. Scammers often pressure people into wiring money, or strongly suggest that people put money on a prepaid debit card and send it to them. Why? It's like sending cash: once it's gone, you can't trace it or get it back. Never deposit a "winnings" check and wire money back, either. The check is a fake, no matter how good it looks, and you will owe the bank any money you withdraw.

Don't pay for a prize. If you enter and win a legitimate sweepstakes, you don't have to pay insurance, taxes, or shipping charges to collect your prize. If you have to pay, it's not a prize. And companies, including Lloyd's of London, don't insure delivery of sweepstakes winnings. If you didn't enter a sweepstakes or lottery, then you can't have won.

Don't give the caller your financial or other personal information. Never give out or confirm financial or other sensitive information, including your bank account, credit card, or Social Security number, unless you know who you're dealing with. Scam artists, like fake debt collectors, can use your information to commit identity theft — charging your existing credit cards, opening new credit card, checking, or savings accounts, writing fraudulent checks, or taking out loans in your name. If you get a call about a debt that may be legitimate — but you think the collector may not be — contact the company you owe money to about the calls.

Don't trust a name or number. Con artists use official-sounding names to make you trust them. It's illegal for any promoter to lie about an affiliation with — or an endorsement by — a government agency or any other well-known organization. No matter how convincing their story — or their stationery — they're lying. No legitimate government official will ask you to send money to collect a prize.

Source: https://www.consumer.ftc.gov/articles/0048-government-imposter-scams

Fake Check Scams

Someone sends you a check with instructions to deposit it and wire some or all the money back. The check is fake, but it may look legitimate and may fool bank tellers. You may get cash before the bank finds out the check is fake. It can take weeks to uncover a fake check. You are responsible for the checks you deposit, so if a check turns out to be fraudulent, you will owe the bank any money you withdrew. Here are some versions of the fake check scam:

Lotteries and Sweepstakes. You just won a foreign lottery! The letter says so, and a cashier's check is included. All you have to do is deposit the check and wire money to pay for taxes and fees. Don't do it. The check is probably fake and you will lose any money you send.

Overpayment Scams. Someone responds to your posting or ad, and offers to use a cashier's check, personal check or corporate check to pay for the item you're selling. At the last minute, the "buyer" (or his "agent") finds a reason to write the check for more than the purchase price. He asks you to deposit the check and wire back the difference. Don't do it. The check is probably fake. It might fool a bank teller at first, but eventually the check will bounce and you'll owe money to the bank.

Mystery Shopper Scams. You are hired to be a mystery shopper and evaluate the customer service of a company. You're given a check to deposit in your personal bank account. You're told to withdraw cash and wire the money using a certain money transfer service. Often, the instructions say to send the money to a person in Canada or another country outside the U.S. Don't do it. The check is probably fake and so is the "mystery shopping" job.

Don't wire money to a person who:

- you never met
- says they are your relative, and they're having a crisis — but they don't want you to tell anyone
- says a money transfer is the only form of payment they accept
- asks you to deposit a check and send some of the money back

Source: https://www.consumer.ftc.gov/articles/0090-using-money-transfer-services

Money Transfer Scams

Family Emergency Scams. You get a call out of the blue from someone who claims to be a member of your family and needs cash for an emergency — to fix a car, get out of jail or leave a foreign country. He begs you to wire money right away and to keep the request confidential. Before you send money, talk with your family. If you feel that you cannot ignore the request, try to verify the caller's identity by asking personal questions a stranger can't answer. And keep trying to reach your family to check out the story.

Apartment Rental Scams. Some scammers copy legitimate rental or real estate listings, change the contact information, and place the altered ads on other sites. Others make up listings for places that aren't for rent or don't exist, and try to get your attention by offering below-market rent. If you respond to the ads, the scammers ask you to wire an application fee, security deposit or the first month's rent. It's never a good idea to send money to someone you haven't met for an apartment you haven't seen. If you can't meet in person, see the apartment, or sign a lease before you pay, keep looking.

Advance Fee Loans. You may be tempted by ads and websites that guarantee loans or credit cards regardless of your credit history. But often, when you apply for the loan or credit card, you find out you must pay a fee in advance. If you have to wire money for the promise of a loan or credit card, you're probably dealing with a scam artist.

Buying Online. If you are buying something online and the seller says you must use a money transfer to pay, it's a sign you won't get the item or a refund. Tell the seller you want to use a credit card, an escrow service or another way to pay. If the seller won't accept, find another seller.

Paying a Telemarketer. It's illegal for a telemarketer to ask you to pay with a cash-to-cash money transfer, like those from MoneyGram and Western Union. If a telemarketer asks you to use one of these payment methods, he's breaking the law.

Don't wire money to a person who:

- you never met
- says they are your relative, and they're having a crisis — but they don't want you to tell anyone
- says a money transfer is the only form of payment they accept
- asks you to deposit a check and send some of the money back

Source: https://www.consumer.ftc.gov/articles/0090-using-money-transfer-services

Deceptive Mortgage Ads

If you're looking for a mortgage to buy a home or refinance an existing loan, you may see or hear ads with offers of low rates or payments. The Federal Trade Commission, the nation's consumer protection agency, says that when you're shopping for a home loan, it's important to understand all the terms and conditions of a proposed loan. Start with what is in the ad itself. Read what's between the lines as well as what's in front of your eyes.

What The Ads Say. To help you recognize an offer that may be less than complete, the FTC wants you to know the buzz words that should trigger follow-up questions, as well as information to insist on after you've read an ad.

A Low "Fixed" Rate. Ads that tout a "fixed" rate may not tell you how long it will be "fixed." The rate may be fixed for an introductory period only, and that can be as short as 30 days. When you shop for a mortgage, you need to know when and how your rate, and payments, can change.

Very Low Rates. Are the ads talking about a "payment" rate or the interest rate? This important detail may be buried in the fine print, if it's there at all. The interest rate is the rate used to calculate the amount of interest you will owe the lender each month. The payment rate is the rate used to calculate the amount of the payment you are obligated to make each month. Some offers advertise a low payment rate without telling you that it applies only during an introductory period. What's more, if the payment rate is less than the interest rate, you won't be covering the interest due. This is called "negative amortization." It means that your loan balance is actually increasing because you're not paying all the interest that comes due, and the lender is adding the unpaid interest to the balance you owe.

Very Low Payment Amounts. Ads quoting a very low payment amount probably aren't telling the whole story. For example, the offer might be for an Interest Only (I/O) loan, where you pay only the amount of interest accrued each month. While the low payment amount may be tempting, eventually, you will have to pay off the principal. Your payment may go up after an introductory period, so that you would be paying down some of the principal – or you may end up owing a "balloon" payment, a lump sum usually due at the end of a loan. You must come up with the money when a balloon payment is due. If you can't, you may need another loan, which, in turn, means new closing costs, and potentially points and fees. And if housing prices are falling, you might not be able to refinance to lower your payments.*(continued on next page)*

Deceptive Mortgage Ads (continued)

Teaser Rates. *Mortgage rates near 30-year lows!*
Rates as low as 1%! You are paying too much!
Who doesn't want to reduce their mortgage payments?
Loan amount $300,000 - pay only $900 per month!

Ads with "teaser" short term rates or payments like these don't often disclose that a rate or payment is for a very short introductory period. If you don't nail down the details in advance about your rates and payments for every month of the life of your loan, expect payment shock when the rate and payment increase dramatically.

Official Lookalikes. *Important Notice From Your Mortgage Company.*
Open Immediately — Important Financial Information Enclosed.
Please do not discard — account information enclosed.

Appearances can be deceiving. Mailers that have information about your mortgage and your lender may not be from your lender at all, but rather from another company that wants your business. Companies can legally get your information from public records. Before you respond to any offer, review it carefully to make sure you know who you're dealing with.

You are eligible to take part in an exclusive government loan program. We can negotiate your existing adjustable rate mortgage to a new low fixed rate mortgage. You must contact us immediately regarding this notice.

Some businesses use pictures of the Statue of Liberty or other government symbols or names to make you think their offer is from a government agency or program. If you're concerned about a mailing you've received, contact the government agency mentioned in the letter. If it's a legitimate agency — and not one that just sounds like a government agency — you'll find the phone number in the Blue Pages of your telephone directory.

Source: https://www.consumer.ftc.gov/articles/0087-deceptive-mortgage-ads

Romance Scams

Romance scams reached a record $304 million in losses reported to the FTC in 2020. That's up about 50% from 2019.

Romance scammers create fake profiles on dating sites and apps, or contact their targets through popular social media sites like Instagram, Facebook, or Twitter. The scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money. They'll often say they're living or traveling outside of the United States: working on an oil rig; in the military; or a doctor with an international organization.

We've heard about romance scammers asking their targets for money to:

- pay for a plane ticket or other travel expenses
- pay for surgery or other medical expenses
- pay customs fees to retrieve something
- pay off gambling debts
- pay for a visa or other official travel documents

Scammers ask you to pay by wiring money, with reload cards, or with gift cards because they can get cash quickly and remain anonymous. They also know the transactions are almost impossible to reverse.

Never send money or gifts to a sweetheart you haven't met in person.

If you suspect a romance scam:

- Stop communicating with the person immediately.
- Talk to someone you trust, and pay attention if your friends or family say they're concerned about your new love interest.
- Do a search for the type of job the person has to see if other people have heard similar stories. For example, you could do a search for "oil rig scammer" or "US Army scammer." You can also browse the comments on our blog posts about romance scams to hear other people's stories:
- Do a reverse image search of the person' profile picture to see if it's associated with another name or with details that don't match up – those are signs of a scam.

Source: https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams

Travel Scams

Scammers may call or use mail, texts, faxes or ads promising free or low-cost vacations. In reality, those vacation offers may end up charging poorly disclosed fees or may be fake, plain and simple. Here are some tell-tell signs that a travel offer or prize might be a scam:

You "won a free vacation" — but you have to pay some fees first. A legitimate company won't ask you to pay for a prize. Any company trying to sell you on a "free" vacation will probably want something from you — taxes and fees, attendance at mandatory timeshare presentations, even pressure to buy "extras" or "add-ons" for the vacation, etc. Find out what your costs are before you agree to anything.

The prize company wants your credit card number. Especially if they say it's to "verify" your identity or your prize, don't give it to them.

They cold-call, cold-text, or email you out of the blue. Before you do business with any company you don't know, call the Attorney General and local consumer protection agencies in the company's home state to check on complaints; then, search online by entering the company name and the word "complaints" or "scam" and read what other people are saying.

They don't — or can't — give you specifics. They promise a stay at a "five-star" resort or a cruise on a "luxury" ship. The more vague the promises, the less likely they'll be true. Ask for specifics, and get them in writing. Check out the resort's address; look for photos of the ship.

You're pressured to sign up for a travel club for great deals on future vacations. The pressure to sign up or miss out is a signal to walk away. Travel clubs often have high membership fees and limited choice of destinations or travel dates.

You get a robocall about it. Robocalls from companies trying to sell you something are almost always illegal if you haven't given the company written permission to call you. That's true even if you haven't signed up for the national Do Not Call Registry.

Source: https://www.consumer.ftc.gov/articles/0046-travel-tips

Tech Support Scams

Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need, to fix a problem that doesn't exist. They often ask you to pay by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a money transfer app because they know those types of payments can be hard to reverse.

Tech support scammers use many different tactics to trick people. Spotting these tactics will help you avoid falling for the scam.

Phone Calls: Tech support scammers may call and pretend to be a computer technician from a well-known company. They say they've found a problem with your computer. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. Then they try to make you pay to fix a problem that doesn't exist. Listen to an FTC undercover call with a tech support scammer. If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.

Pop-up Warnings: Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

Online Ads and Listings in Search Results Pages: Tech support scammers try to get their websites to show up in online search results for tech support. Or they might run their own ads online. The scammers are hoping you'll call the phone number to get help.

If you think there may be a problem with your computer, update your computer's security software and run a scan. If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer technical support in person.

If a tech support scammer contacts you, report it to the Federal Trade Commission. When you report a scam, the FTC can use the information to build cases against scammers. Are you skeptical that reporting scams will make a difference? Tech support scams are common. In 2017, the FTC received more than 150,000 reports about these scams from people like you. Add your voice. Report tech support scams to the FTC.

Source: https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

Health Scams

People spend billions of dollars a year on products and treatments in the hope of improving their health and fitness. But a lot of that money goes to companies that make fake claims about those products and treatments, cheating people out of their money, their time — even their health. If you're thinking about buying a health product or service, here are some things to keep in mind to get the best outcomes for you and your family.

If you're thinking about buying a health product or service to treat an illness or ailment, here are some steps to take to get the best outcomes for yourself and your loved ones.

- Do your research. Search for the name of the treatment or product online, plus the words "review," "complaint," or "scam."
- Ask your doctor first. If you're curious about a treatment, talk to your doctor or health care provider about it. Here are some questions to ask.
- Does this product or treatment actually work?
- What's the scientific evidence?
- Are you familiar with this brand?
- Can you tell me about the ingredients in this product?
- How will it interact with other supplements or drugs I take?
- What are the side effects?
- If it's safe to take, what's the right amount?

Know that unproven products and treatments are dangerous. Taking unproven products might mean that you stop or delay taking proven medical treatments ordered by your health care provider. Unproven products might cause bad interactions with your treatments. They also might delay you making other important changes to help your condition — say in your diet or lifestyle.

Don't let any company take advantage of your hope. Be skeptical about any treatment or product that makes guarantees or promises about your health, and check with your doctor or health care provider.

"Natural" doesn't mean either safe or effective. In fact, "natural" can mean both harmful and ineffective. And some "natural" products might interfere with proven treatments recommended by your doctor.

Federal law says sellers that peddle cures must have scientific proof to back up their claims. Ads must be truthful — not misleading. But whenever you see or hear an ad, know that no government agency approves those ads before they go public.

Source: https://consumer.ftc.gov/articles/common-health-scams

Health Care Scams

Charging you for help getting new insurance

Someone contacts you, offering to help you navigate the Health Insurance Marketplace for a fee – or saying that you need a new insurance card now or you'll have to pay a penalty. Regardless of the set-up, their goal is to get your bank account or credit card number. **Don't give your information.** The people who offer legitimate help with the Health Insurance Marketplace, sometimes called Navigators or Assisters, are not allowed to charge you. In fact, you can't pay them. What's more, you don't need to buy a special insurance card, or pay any penalties for not buying one, either.

Medicare cards

Someone gets in touch, saying you need a new Medicare card. They tell you that you'll lose Medicare coverage if you don't pay a fee for a new card or give them your Social Security number and bank account or credit card number. **Not true.** Don't give your personal or financial information to anyone who contacts you. When in doubt, call 1-800-MEDICARE, before you give anyone your money or information.

Medical discount scams

Someone contacts you, offering discounts on health services and products. They might say the discount plan will save you money and that it meets the minimum coverage required under "Obamacare" so you won't have to pay a penalty or look at other plans. **Medical discount plans are not health insurance.** Sometimes, medical discount plans illegally pretend to be insurance. Ask specific questions and don't pay until you read the terms. Your state insurance commissioner's office can tell you if a health plan is insurance. Most medical discount plans are a membership in a "club" that claims to offer reduced prices from certain doctors, certain pharmacies, and on some procedures. Some medical discount plans provide legitimate discounts, but others are scams that don't deliver on the medical services promised. Others are attempts to get your personal or financial information, so the scammer can use it to commit identity fraud.

Source: https://www.consumer.ftc.gov/articles/0394-suspect-health-care-scam

Telephone Scams

Every year, thousands of people lose money to telephone scams — from a few dollars to their life savings. Scammers will say anything to cheat people out of money. Some seem very friendly — calling you by your first name, making small talk, and asking about your family. They may claim to work for a company you trust, or they may send mail or place ads to convince you to call them.

If you get a call from someone you don't know who is trying to sell you something you hadn't planned to buy, say "No thanks." And, if they pressure you about giving up personal information — like your credit card or Social Security number — it's likely a scam. Hang up and report it to the Federal Trade Commission.

Often, scammers who operate by phone don't want to give you time to think about their pitch; they just want you to say "yes." But some are so cunning that, even if you ask for more information, they seem happy to comply. They may direct you to a website or otherwise send information featuring "satisfied customers." These customers, known as shills, are likely as fake as their praise for the company.

Here are a few red flags to help you spot telemarketing scams. If you hear a line that sounds like this, say "no, thank you," hang up, and file a complaint with the FTC:

> *You've been specially selected (for this offer).You'll get a free bonus if you buy our product. You've won one of five valuable prizes. You've won big money in a foreign lottery. This investment is low risk and provides a higher return than you can get anywhere else. You have to make up your mind right away. You trust me, right? You don't need to check our company with anyone. We'll just put the shipping and handling charges on your credit card.*

Scammers use exaggerated — or even fake — prizes, products or services as bait. Some may call you, but others will use mail, texts, or ads to get you to call them for more details. Here are a few examples of "offers" you might get:

- **Travel Packages.** "Free" or "low cost" vacations can end up cost-ing a bundle in hidden costs. Some of these vacations never take place, even after you've paid.
- **Credit and loans.** Advance fee loans, payday loans, credit card protection, and offers to lower your credit card interest rates are very popular schemes, especially during a down economy.
- **Charitable causes.** Urgent requests for recent disaster relief efforts are especially common on the phone.

Telephone Scams (continued)

- **Sham or exaggerated business and investment opportunities.** Promoters of these have made millions of dollars. Scammers rely on the fact that business and investing can be complicated and that most people don't research the investment.
- **High-stakes foreign lotteries.** These pitches are against the law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. What's more, you may never see a ticket.
- **Extended car warranties.** Scammers find out what kind of car you drive, and when you bought it so they can urge you to buy overpriced — or worthless — plans.
- **"Free" trial offers.** Some companies use free trials to sign you up for products — sometimes lots of products — which can cost you lots of money because they bill you every month until you cancel.

Everyone's a potential target. Fraud isn't limited to race, ethnic back-ground, gender, age, education, or income. That said, some scams seem to concentrate in certain groups. For example, older people may be targeted because the caller assumes they may live alone, have a nest egg, or may be more polite toward strangers.

When you get a call from a telemarketer, ask yourself:

- **Who's calling… and why?** The law says telemarketers must tell you it's a sales call, the name of the seller and what they're selling before they make their pitch. If you don't hear this information, say "no thanks," and get off the phone.
- **What's the hurry?** Fast talkers who use high pressure tactics could be hiding something. Take your time. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.
- **If it's free, why are they asking me to pay?** Question fees you need to pay to redeem a prize or gift. Free is free. If you have to pay, it's a purchase — not a prize or a gift.
- **Why am I "confirming" my account information — or giving it out?** Some callers have your billing information before they call you. They're trying to get you to say "okay" so they can claim you approved a charge.
- **What time is it?** The law allows telemarketers to call only between 8 am and 9 pm. A seller calling earlier or later is ignoring the law.
- **Do I want more calls like this one?** If you don't want a business to call you again, say so and register your phone number on the National Do Not Call Registry. If they call back, they're breaking the law.

Telephone Scams (continued)

Some Additional Guidelines

- Resist pressure to make a decision immediately.
- Keep your credit card, checking account, or Social Security numbers to yourself. Don't tell them to callers you don't know — even if they ask you to "confirm" this information. That's a trick.
- Don't pay for something just because you'll get a "free gift."
- Get all information in writing before you agree to buy.
- Check out a charity before you give. Ask how much of your donation actually goes to the charity. Ask the caller to send you written informa-tion so you can make an informed decision without being pressured, rushed, or guilted into it.
- If the offer is an investment, check with your state securities regulator to see if the offer — and the offeror — are properly registered.
- Don't send cash by messenger, overnight mail, or money transfer. If you use cash or a money transfer — rather than a credit card — you may lose your right to dispute fraudulent charges. The money will be gone.
- Don't agree to any offer for which you have to pay a "registration" or "shipping" fee to get a prize or a gift.
- Research offers with your consumer protection agency or state Attorney General's office before you agree to send money.
- Beware of offers to "help" you recover money you have already lost. Callers that say they are law enforcement officers who will help you get your money back "for a fee" are scammers.

Report any caller who is rude or abusive, even if you already sent them money. They'll want more. Call 1-877-FTC-HELP or visit ftc.gov/complaint.

Join the National Do Not Call List. Register your home and mobile phone numbers with the National Do Not Call Registry. This won't stop all unsolicited calls, but it will stop most. If your number is on the registry and you still get calls, they're probably from scammers ignoring the law. Hang up, and report them at www.donotcall.gov.

Source: https://www.consumer.ftc.gov/articles/0076-phone-scams

Appendices

Helpful Resources

- **Credit Reporting Agencies**

  EquiFax
  http://www.equifax.com
  1-800-525-6285

  Experian
  http://www.experian.com
  1-888-397-3742

  TransUnion
  http://www.transunion.com
  1-800-680-7289

- **Federal Government Agencies**

  Federal Trade Commission
  To report identity theft: http://www.identitytheft.gov
  1-877-438-4338
  1-866-653-4261 (TTY)

  Legal Services Programs
  To locate a legal services provider:
  http://www.lsc.gov/local-programs/program-profiles

  Federal Communications Commission
  For help with telephone service:
  http://www.fcc.gov/cgb
  1-888-225-5322
  1-888-835-5322 (TTY)

  Federal Financial Institutions Examination Council
  To locate the agency that regulates a bank or credit union:
  http://www.ffiec.gov/consumercenter

  U.S. Department of Justice
  To report suspected bankruptcy fraud: http://www.justice.gov/ust/eo/fraud
  Or send email to:USTP.Bankruptcy.Fraud@usdoj.gov

U.S. Postal Inspection Service
To file a complaint:
http://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx
1-877-876-2455

U.S. Securities and Exchange Commission
To report fraud: http://www.sec.gov/complaint/tipscomplaint.shtml
1-800-732-0330

U.S. Department of State
To report a lost or stolen passport: http://www.travel.state.gov/passport
1-877-487-2778
1-888-874-7793 (TDD/TTY)

U.S. Postal Service
To place a hold on mail, go to http://www.usps.com/holdmail
To locate a post office: http://www.usps.com
1-800-275-8777

Social Security Administration
To report fraud: go to http://www.socialsecurity.govand type "Fraud" in the Search box.
1-800-269-0271
1-866-501-2101 (TTY)

IRS
https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
1-800-908-4490

Attorney General Contacts by State

State	Phone	Website
Alabama	(334) 242-7300	http://www.ago.state.al.us/
Alaska	(907) 269-5602	http://www.law.state.ak.us/index.html
Arizona	(602) 542-4266	http://www.azag.gov/
Arkansas	(800) 482-8982	http://www.ag.arkansas.gov/
California	(916) 445-9555	http://ag.ca.gov/
Colorado	(720) 508-6000	http://www.coloradoattorneygeneral.gov/
Connecticut	(860) 808-5318	http://www.ct.gov/ag/
Delaware	(302) 577-8400	http://attorneygeneral.delaware.gov/
District of Columbia	(202) 727-3400	http://oag.dc.gov/
Florida	(850) 414-3300	http://myfloridalegal.com/
Georgia	(404) 656-3300	http://law.ga.gov/
Hawaii	(808) 586-1500	http://ag.hawaii.gov/
Idaho	(208) 334-2400	http://www.ag.idaho.gov/
Illinois	(312) 814-3000	http://illinoisattorneygeneral.gov/
Indiana	(317) 232-6201	http://www.in.gov/attorneygeneral/
Iowa	(515) 281-5164	http://www.iowaattorneygeneral.gov
Kansas	(785) 296-2215	https://www.ag.ks.gov/
Kentucky	(502) 696-5300	http://ag.ky.gov/
Louisiana	(225) 326-6000	http://www.ag.state.la.us/
Maine	(207) 626-8800	http://www.maine.gov/ag/
Maryland	(410) 576-6300	http://www.marylandattorneygeneral.gov/
Massachusetts	(617) 727-2200	http://www.mass.gov/ago/
Michigan	(517) 373-1110	http://www.michigan.gov/ag
Minnesota	(800) 657-3787	http://www.ag.state.mn.us/
Mississippi	(601) 359-3680	http://www.ago.state.ms.us/
Missouri	(573) 751-3321	http://ago.mo.gov/

Attorney General Contacts by State

State	Phone	Website
Montana	(406) 444-2026	https://doj.mt.gov/
Nebraska	(402) 471-2682	http://www.ago.ne.gov/
Nevada	(775) 684-1100	http://ag.nv.gov/
New Hampshire	(603) 271-3658	https://www.doj.nh.gov/index.htm
New Jersey	(609) 292-8740	http://nj.gov/oag
New Mexico	(505) 490-4060	https://www.nmag.gov/
New York	(518) 474-7330	http://www.ag.ny.gov/
North Carolina	(919) 716-6400	http://www.ncdoj.gov/
North Dakota	(701) 328-2210	http://www.ag.state.nd.us
Ohio	(614) 466-4320	http://www.ohioattorneygeneral.gov/
Oklahoma	(405) 521-3921	http://www.oag.state.ok.us/
Oregon	(503) 378-6002	http://www.doj.state.or.us/
Pennsylvania	(717) 787-3391	https://www.attorneygeneral.gov/
Rhode Island	(401) 274-4400	http://www.riag.ri.gov/
South Carolina	(803) 734-3970	http://www.scag.gov/
South Dakota	(605) 773-3215	http://atg.sd.gov/
Tennessee	(615) 741-3491	http://www.tn.gov/attorneygeneral
Texas	(512) 463-2100	https://www.texasattorneygeneral.gov/
Utah	(801) 538-9600	http://attorneygeneral.utah.gov/
Vermont	(802) 828-3173	http://www.atg.state.vt.us/
Virginia	(804) 786-2071	http://www.oag.state.va.us/
Washington	(360) 753-6200	http://www.atg.wa.gov
West Virginia	(304) 558-2021	http://www.wvago.gov/
Wisconsin	(608) 266-1221	http://www.doj.state.wi.us
Wyoming	(307) 777-7841	http://attorneygeneral.state.wy.us

Sample: Dispute Credit Card Charges

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Creditor]
[Fraud Department (companies may specify an address to receive fraud dispute letters), or Billing Inquiries Department]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am writing to dispute a fraudulent charge on my account in the amount of $_____. I am a victim of identity theft, and I did not make or authorize this charge. I am requesting that the charge be removed, that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement. This request is made pursuant to the Fair Credit Billing Act's amendments to the Truth in Lending Act, 15 U.S.C. §§ 1666-1666b, 12 C.F.R. § 226.13. See also 12 C.F.R. § 226.12(b).

Enclosed are copies of [use this sentence to describe any enclosed information, such as sales slips, payment records] supporting my position. Please investigate this matter and correct the billing error as soon as possible.

Sincerely,
[Your Name]

Enclosures:

[List what you are enclosing.]

Source: https://www.identitytheft.gov/Sample-Letters/dispute-credit-card-charges

Sample: Dispute ATM/Debit Card Transactions

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Address]
[City, State, Zip Code]

RE: Notice of stolen/lost [or unauthorized use of] ATM/Debit Card Account Number [Your account#]

Dear Sir or Madam:

I am the victim of identity theft. My ATM/Debit card was lost or stolen [or was used for an unauthorized transaction] on [insert date]. I did not authorize any transactions on or after this date, and I did not authorize anyone else to use my ATM/Debit card in any way.

I am notifying you, pursuant to the Electronic Fund Transfer Act, and implementing Regulation E, 15 U.S.C. § 1693 et seq., 12 C.F.R. § 205, of my lost [or stolen] ATM/Debit Card [or unauthorized transaction]. See especially 12 C.F.R. §§ 205.6, 205.11. I request that you investigate any unauthorized transactions involving this card, including but not limited to the following:

[List of unauthorized transactions].

I am attaching a copy of each of the following documents to this letter:

1. A copy of my Identity Theft Report which includes:
   - my FTC Identity Theft Report
   - the police report about the theft of my identity
2. The FTC Notice to Furnishers of Information, which can be found here: https://www.consumer.ftc.gov/articles/pdf-0092-notice-to-furnishers.pdf

Please close the account [if applicable] and restore any funds which have been withdrawn from my account [if applicable]. Please also notify me in writing of the results of your investigation or if you have any questions regarding this notice or my requests. [As applicable] Please send me written confirmation that [any funds have been restored] and [the account has been closed].

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- FTC Notice to Furnishers of Information [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0092-notice-to-furnishers.pdf

Source: https://www.identitytheft.gov/Sample-Letters/dispute-debit-card-transactions

Sample: Dispute Letter to a Credit Bureau

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

(Write to each relevant credit reporting agency, one at a time:)

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069

Experian
P.O. Box 9554
Allen, TX 75013

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft and I write to dispute certain information in my file resulting from the crime. I have circled the items I dispute on the attached copy of the report I received. The items I am disputing do not relate to any transactions that I have made or authorized. Please remove/correct this information at the earliest possible time.

[This/These] item(s) [identify item(s) disputed by name of the source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.] [is/are] [inaccurate or incomplete] because [describe what is inaccurate or incomplete about each item, and why] . As required by section 611 of the Fair Credit Reporting Act, 15 U.S.C. § 1681i, a copy of which is enclosed, I am requesting that the item(s) be removed [or request another specific change] to correct the information.

[If applicable: Enclosed are copies of [describe any enclosed documentation, such as payment records, court documents] supporting my position.] Please reinvestigate [this/these matter(s)] and [delete or correct] the disputed item(s) as soon as possible.

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing]

- Proof of identity: [a copy of my driver's license/other government-issued identification card/other]
- Copy of Credit Report
- Fair Credit Reporting Act Section 611 [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0091-fair-credit-reporting-act-611.pdf

Source: https://www.identitytheft.gov/Sample-Letters/dispute-credit-bureau

Sample: Dispute Letter to a Company for a New Account

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Fraud Department (companies may specify an address to receive fraud dispute letters), or Billing Inquiries Department]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft and I am writing to dispute certain information you have reported about me to the credit reporting agencies (CRAs). I have enclosed a copy of my FTC Identity Theft Report and my credit report showing the items that I dispute. [Consumers should redact information from both reports that is unrelated to the dispute with this company.] Because the information you are reporting is the result of identity theft, and does not reflect my activities, I am requesting that you stop reporting this information to the CRAs pursuant to section 623(a)(1)(B) of the Fair Credit Reporting Act, 15 U.S.C. §1681s-2(a)(1)(B). I ask that you take these steps as soon as possible.

Enclosed are copies of [use this sentence if applicable and describe any additional enclosed documentation] supporting my position. Also enclosed is a copy of the Notice to Furnishers issued by the Federal Trade Commission, which details your responsibilities under the Fair Credit Reporting Act as an information furnisher to CRAs. Please cease reporting this information to the CRAs, investigate [this/these matter(s)], and delete the disputed item(s) as soon as possible.

Please send me a letter documenting the actions you have taken to absolve me of any responsibility for the information I am disputing, which resulted from the identity theft.

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of identity: [a copy of my driver's license/other government-issued identification card/other]
- Credit report with disputed information indicated
- FTC Notice to Furnishers of Information [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0092-notice-to-furnishers.pdf

Source: https://www.identitytheft.gov/Sample-Letters/dispute-new-account

Sample: Dispute Letter to a Company for an Existing Account

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Fraud Department (companies may specify an address to receive fraud dispute letters), or Billing Inquiries Department]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am writing to dispute [a] fraudulent charge(s) on my account in the amount(s) of $_____, and posted on [dates]. I am a victim of identity theft, and I did not make [this/these] charge(s). I request that you remove the fraudulent charge(s) and any related finance charge and other charges from my account, send me an updated and accurate statement, and close the account (if applicable). I also request that you cease reporting the inaccurate information to all of the nationwide credit reporting agencies (CRAs) to which you provided it.

Enclosed is a copy of my Identity Theft Report supporting my position, and a copy of my credit report showing the fraudulent items related to your company that are the result of identity theft. [Consumers should redact information that is unrelated to the dispute with this company.] Also enclosed is a copy of the Notice to Furnishers issued by the Federal Trade Commission, which details your responsibilities under the Fair Credit Reporting Act as an information furnisher to CRAs. The Notice also specifies your responsibilities when you receive notice from a CRA, under section 605B of the Fair Credit Reporting Act, that information you provided to the CRA may be the result of identity theft. Those responsibilities include ceasing to provide the inaccurate information to any CRAs, and ensuring that you do not attempt to sell or transfer the fraudulent debts to another party for collection.

Please investigate this matter and send me a written explanation of your findings and actions.

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of identity: [a copy of my driver's license/other government-issued identification card/other]
- Credit report with disputed information indicated
- FTC Notice to Furnishers of Information [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0092-notice-to-furnishers.pdf

Source: https://www.identitytheft.gov/Sample-Letters/dispute-new-account

Sample: Identity Theft Letter to a Debt Collector

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Credit Collection Company]
[Company Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

I am a victim of identity theft. An identity thief used my personal information without my permission to open an account and make purchases with [name of business where account was opened]. This debt is not mine. I have enclosed proof of my identity and a copy of my FTC Identity Theft Report.

In accordance with the Fair Debt Collection Practices Act, I am asking you to stop collection proceedings against me and stop communicating with me about this debt, except as the Fair Credit Reporting Act allows. I also ask that you notify [the business where the account was opened] and tell them the debt is the result of identity theft.

[Provide details about what happened. Include the dates and amounts of fraudulent transactions.]

I have enclosed a copy of the Federal Trade Commission's Notice to Furnishers of Information. It explains your responsibilities under the Fair Credit Reporting Act (FCRA). The FCRA requires that debt collectors give an identity theft victim documents related to an account if the victim asks. Please send me copies of all records relating to the account, including:

- Account applications made on paper, online, or by telephone
- Account statements or invoices
- Records of payment or charge slips
- Delivery addresses associated with the account
- Records of phone numbers used to activate or access the account
- Signatures on applications and accounts
- Investigators report

Please send me a letter explaining what you have done to:

- Inform [business where the account was opened] that the debt is the result of identity theft
- Stop collection proceedings against me
- Stop reporting information about the debt to credit reporting companies
- Provide me with the records I request

Thank you for your cooperation.

Sincerely,
[Your Name]

(continued on the next page)

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of identity: [a copy of my driver's license/other government-issued identification card/other]
- FTC Notice to Furnishers of Information [PDF]FTC Notice to Furnishers of Information [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0092-notice-to-furnishers.pdf

Source: https://www.identitytheft.gov/Sample-Letters/identity-theft-debt-collector

Sample: Request Letter for Getting Business Records Related to Identity Theft

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Address specified by the company for 609(e) requests, or, if none is specified, the address for the Fraud Department or Billing Inquiries Department]
[City, State, Zip Code]

RE: Request for Records Pursuant to Section 609(e) of the Fair Credit Reporting Act

[Description of fraudulent transaction/account]
[Dates of fraudulent transaction or Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft. The thief [made a fraudulent transaction/opened a fraudulent account] in my name with your company. In accordance with section 609(e) of the Fair Credit Reporting Act, 15 U.S.C. § 1681g(e), I am requesting that you provide me copies of business records relating to the fraudulent [transaction/account] identified above. The law directs that you provide these documents at no charge, and without requiring a subpoena, within thirty (30) days of your receipt of this request. I am enclosing a copy of the relevant federal law and the Federal Trade Commission's business education publication on this topic.

Enclosed with this request is the following documentation, as applicable:

- Proof of my identity: A copy of my driver's license, other government-issued identification card, or other proof of my identity; and
- Proof of my claim of identity theft:
- A copy of the police report about my identity theft; and
- A completed and signed FTC Identity Theft Report or alternative affidavit of fact.

Please provide all records relating to the fraudulent [transaction/account], including:

- Application records or screen prints of internet/phone applications
- Statements/invoices
- Payment/charge slips
- Investigator's summary
- Delivery addresses
- All records of phone numbers used to activate or access the account
- Any other documents associated with the account
- Please send these records to me at the above address.

(continued on next page)

[If applicable: In addition, I authorize the law enforcement officer who is investigating my case to submit this request on my behalf and/or receive copies of these records from you. The law enforcement officer's name, address and telephone number is: [insert officer name, address and telephone]. Please also send copies of all records to this officer.]

If you have any questions concerning this request, please contact me at the above address or at [your telephone number].

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing]

- Identity Theft Report
- Proof of identity: [a copy of my driver's license/other government-issued identification card/other]
- Fair Credit Reporting Act Section 611 [PDF] which can be found here: https://www.consumer.ftc.gov/articles/pdf-0091-fair-credit-reporting-act-611.pdf
- A copy of Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft which can be found here: https://www.ftc.gov/tips-advice/business-center/guidance/businesses-must-provide-victims-law-enforcement-transaction

Source: https://www.identitytheft.gov/Sample-Letters/request-records-related-identity-theft

Glossary

Borrowed identity: A variation on identity theft. A friend might borrow your identity if he or she uses your key card to access the building where you live. Or, an undocumented worker or a person wanting to remain anonymous might use a stolen name, Social Security number, and date of birth in order to apply for a job or to open a bank account.

Child identity theft: A variation of a borrowed identity scheme in which a criminal obtains a child's name and Social Security number in order to get a job, open a bank account, or even obtain a driver's license.

Financial identity theft: The most common category of identity theft. In this type, the thief uses stolen credentials to access a person's monetary assets.

Identity Theft:. Falsely using someone else's personal information, including their name, date of birth, Social Security number, credit card numbers, ATM code, electronic signature, and passwords which protect financial information like electronic banking or e-payment sites.

Insurance theft: A form of identity theft in which a criminal uses your insurance information in order to obtain insurance payouts illegally.

Internet service provider (ISP): A company that connects you to the internet by way of a device generically known as a modem.

Key Logger: Software that logs everything that you type. Used by malicious agents to obtain sensitive

information, like your secure passwords for email or bank accounts.

Medical identity theft: A form of identity theft in which a criminal uses a stolen identity in order to receive medical treatments or prescription drugs.

Modem: The device that connects your home network (via a cable, DSL, fiber-optic, or satellite connection) to the internet. Short for modulator - demodulator. Your wireless router usually connects to the modem.

Net neutrality: Net neutrality is the principle that all online content should be treated the same by the companies that deliver it, namely internet service providers. Net neutrality rules that were approved by the FCC in 2015 were repealed in 2017.

Password Manager: An application that stores your passwords for you.

Phishing: A play on the word "fishing." A broad group of malicious techniques where a criminal attempts to discover a person's details by way of deceptive electronic communication, usually an email or a chat message.

Social engineering: A form of identity theft in which a criminal misrepresents themselves socially in order to gain information or to bypass a means of security. For example, a person might show up at an office claiming to be a delivery or repair person, hoping to talk their way into a non-public area.

Real estate fraud: A form of identity theft in which a criminal uses a person's identifying details to alter property ownership records.

Virtual Private Network (VPN): A VPN allows you to join a network virtually, i.e. a VPN is connected through software not hardware. It also allows private communication, i.e. the data is transmitted with encryption.

Wireless Router: A device that usually connects to your modem. It directs all traffic between the internet and the various devices on your home network like your laptops, desktop PCs or home theater PCs, game consoles, tablets, etc.

https://greyhouse.weissratings.com

The Weiss Financial Ratings Series, published by Weiss Ratings and Grey House Publishing, offers libraries, schools, universities and the business community a wide range of investing, banking, and insurance and financial literacy tools. Visit www.greyhouse.com or https://greyhouse.weissratings.com for more information about the titles and online tools below.

- Weiss Ratings Consumer Guides
- Weiss Ratings Financial Literacy Basics
- Weiss Ratings Financial Literacy: Planning for the Future
- Weiss Ratings Financial Literacy: How to Become an Investor
- Weiss Ratings Guide to Banks
- Weiss Ratings Guide to Credit Unions
- Weiss Ratings Guide to Health Insurers
- Weiss Ratings Guide to Life & Annuity Insurers
- Weiss Ratings Guide to Property & Casualty Insurers
- Weiss Ratings Investment Research Guide to Bond & Money Market Mutual Funds
- Weiss Ratings Investment Research Guide to Exchange-Traded Funds
- Weiss Ratings Investment Research Guide to Stock Mutual Funds
- Weiss Ratings Investment Research Guide to Stocks
- Weiss Ratings Medicare Supplement Insurance Buyers Guide
- Weiss Financial Ratings Series Online – **https://greyhouse.weissratings.com**

Box Set: 978-1-64265-891-0

Grey House Publishing

4919 Route 22, Amenia, NY 12501
518-789-8700 800-562-2139 FAX 845-373-6360
www.greyhouse.com e-mail: books@greyhouse.com