



**The FTC Hopes You Will Help
Fight Fraud!**

Chances are good that someone sitting near you has been scammed. They may not talk about it, but if the statistics are right, it has happened.

The truth is sharing **WHAT** you know can help protect someone **WHO** you know from a scam. That's why we've created this booklet. To help you:

****Reinforce what you already know****

****Start a conversation****

****Pass it on****

If you suspect a scam, act quickly. Please report it to the Federal Trade Commission. Report fraud online (ftc.gov/complaint) or call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261. The FTC operator will give you the next steps to take.

Your complaints make a difference!

consumer.ftc.gov

Get Help or Information from the Federal Trade Commission,
the nation's consumer protection agency

FTC's Toll Free Fraud Hotline 877-382-4357



IdentityTheft.gov

Recovering from identity theft is easier with a plan.

IdentityTheft.gov can help >

TAKE ACTION: To Receive FTC Scam Alerts Via Email
Go To [FTC.gov/subscribe](https://www.ftc.gov/subscribe).



SCAM ALERTS

what to know and do about scams in the news

Crooks use clever schemes to defraud millions of people every year. They often combine sophisticated technology with age-old tricks to get people to send money or give out personal information. They add new twists to old schemes and pressure people to make important decisions on the spot. One thing that never changes: they follow the headlines — and the money.

Contents

Identity Theft

Someone gets your personal information and runs up bills in your name. They might use your Social Security or Medicare number, your credit card, or your medical insurance — along with your good name.

Charity Fraud

Someone contacts you asking for a donation to their charity. It sounds like a group you've heard of, it seems real, and you want to help.

Imposter Scams

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know — your grandchild, a relative or a friend. Or maybe it's from someone you feel like you know, but you haven't met in person — say, a person you met online who you've been writing to.

Health Care Scams

You see an ad on TV, telling you about a new law that requires you to get a new health care card. Maybe you get a call offering you big discounts on health insurance. Or maybe someone says they're from the government, and she needs your Medicare number to issue you a new card.

Paying Too Much

Everyone pays all kinds of bills. Some are higher than you think they should be. Sometimes, unexpected charges appear on your bill – or sometimes, you might see a fee for a service you don't recall ordering. Are you paying more than you should?

“You've Won” Scams

You get a card, a call, or an email telling you that you won! Maybe it's a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can't wait for you to get your winnings.



FEDERAL TRADE COMMISSION

PROTECTING AMERICA'S CONSUMERS

Imposter Scams Top Complaints Made to FTC in 2018

For the first time, imposter scams topped the list of consumer complaints submitted in 2018 to the Federal Trade Commission's nationwide Consumer Sentinel database, driven in part by a jump in reports about government imposter scams.

Fraudsters operating government imposter scams falsely claim to be from the Internal Revenue Service, Social Security Administration, or another government agency to get people to turn over money or personal information. Government imposter scams made up nearly half of the 535,417 imposter scam reports to the FTC in 2018. Consumers reported losing a total of nearly \$488 million to all types of imposter scams in 2018—more than any other type of fraud—and reported a median loss of \$500.

Many government imposter scam reports involved fraudsters who [falsely claimed to be from the Social Security Administration](#). These scammers typically tell people their Social Security number has been suspended, or that there is some other problem, in an effort to get them to reveal their Social Security number or pay money to “reactivate” it. In reality, Social Security numbers are never suspended and the Social Security Administration will never require you to pay to obtain one.

“If you get a call out of the blue from someone claiming to be from a government agency like the Social Security Administration or IRS asking you for personal information or money, it’s a scam,” said Andrew Smith, Director of the FTC’s Bureau of Consumer Protection. “You should hang up immediately and report it to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).”

Increase in Reports, Fraud Losses

In all, the FTC received nearly three million complaints from consumers in 2018. Consumers reported losing nearly \$1.48 billion to fraud in 2018—38 percent more than the year before. Debt collection complaints dropped to the number two spot after topping the FTC’s list of consumer complaints for the previous three years.

Identity theft was the third most common complaint, and consistently ranks among the top consumer complaints made to the FTC. There was a 24 percent increase last year in identity theft reports that involved credit card fraud on new accounts. At the same time, there was a large drop (38 percent) in reports involving tax identity theft.

As in previous years, wire transfers and credit cards were the first and second most widely reported form of payment for fraud. In 2018, however, a growing number of consumers reported that scammers demanded to be paid with gift and reload cards. The number of consumers who said they paid with a gift or reload card grew from over 28,000 in 2017 to more than 41,000 in 2018, while the total amount paid using a gift or reload card to scammers nearly doubled to \$78 million.

The Consumer Sentinel Network’s secure online database is currently available to more than 2,500 individual users in civil and criminal law enforcement agencies across the country and abroad. Agencies use the data to research cases, identify victims and track possible targets. Although non-governmental organizations may contribute data to the database, only law enforcement agencies can access the database. Law enforcement personnel can join Sentinel at [Register.ConsumerSentinel.gov](https://www.ftc.gov/consumer-sentinel).



Click image to see full visual snapshot



Imposter Scams

Here's how they work:

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you *feel* like you know, but you haven't met in person – say, a person you met online who you've been writing to.

Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do:

- 1. Stop. Check it out – before you wire money to anyone.** Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.
- 2. Pass this information on to a friend.** You may not have gotten one of these calls or emails, but the chances are you know someone who has.





FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Phishing: Don't Take the Bait

Phishing: Don't Take the Bait

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.



The Bait



Scammers use familiar company names or pretend to be someone you know.



They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.

They pressure you to act now — or something bad will happen.

Avoid the Hook



Check it out.

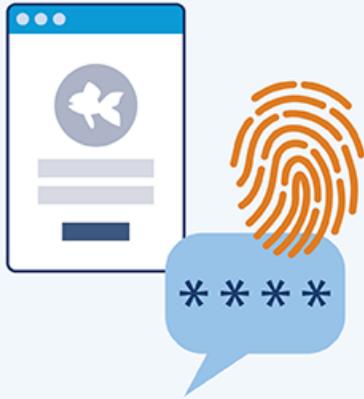
- » Look up the website or phone number for the company or person who's contacting you.
- » Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
- » Tell them about the message you got.

Look for scam tip-offs.

- » You don't have an account with the company.
- » The message is missing your name or uses bad grammar and spelling.
- » The person asks for personal information, including passwords.
- » **But note: some phishing schemes**



are sophisticated and look very real,
so check it out and protect yourself.



Protect yourself.

- » Keep your computer security up to date and back up your data often.
- » Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.
- » Change any compromised passwords right away and don't use them for any other accounts.

Report Phishing

- » Forward phishing emails to spam@uce.gov and reportphishing@apwg.org.
- » Report it to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).



For more information, visit [ftc.gov/phishing](https://www.ftc.gov/phishing)
[aba.com/phishing](https://www.aba.com/phishing)





FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

**Consumer
Protection**

Data Spotlight
FTC reporting back to you

Government imposter scams top the list of reported frauds

Share This Page

Emma Fletcher

Jul 1, 2019

TAGS: [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Imposter](#)

Pretending to be someone people trust is what scammers do. They may claim to be a well-known company or a beloved family member, but data from the FTC's Consumer Sentinel Network suggest that pretending to be the government may be scammers' favorite ruse. Since 2014, the FTC has gotten nearly 1.3 million reports about government imposters. That's far more than any other type of fraud reported in the same timeframe. This spring, monthly reports of government imposter scams reached the highest levels we have on record.¹

The vast majority of people who report this type of scam say it started with a phone call,² and these callers have their mind games down pat. Government impersonators can create a sense of urgent fear, telling you to send money right away or provide your social security number to avoid arrest or some other trouble. Or they can play the good guy, promising to help you get some free benefit like a grant or prize, or even a back brace. Scammers like to make the situation so immediate that you can't stop to check it out.

These scams can be extremely lucrative. Reported losses to government imposter scams add up to more than \$450 million since 2014. Only 6% of people who report government imposters say they lost money.³ But when people do lose money, it's a lot: the median individual reported loss is \$960.⁴ People ages 20 to 59 report losing money to these scams at higher rates than people 60 and over, but median individual reported losses increase with age. People 80 and over report a median loss of \$2,700.⁵

Gift cards are now the payment method of choice for these scammers. Most people who tell us they lost money to a government imposter say they gave the scammer the PIN number on the back of gift cards like Google Play or iTunes cards.⁶ Wire transfers come in a distant second to gift cards as a payment method. But with both methods, the scammer gets quick cash while staying anonymous, and the money is simply gone.

The top government imposters reported so far in 2019 have both familiar and new faces. The FTC reported recently about the dramatic surge in Social Security imposters, but IRS imposters are still hanging on in the top five. Scammers use “bureau” or “administration” in their name to make their government grant offers sound official, and use generic names like “sheriff’s office” to suggest a hefty law enforcement presence. Government imposters will adapt quickly to find new ways to get your money. Lots of government agencies have been impersonated, including the FTC. The scammer’s pitch is even more convincing when they fake the number on your caller ID so it shows the name or phone number of a real government agency. It’s illegal to fake the number on caller ID, but scammers know it helps convince people that the caller really is with the government.

Oh, the stories scammers tell . . .

Phony Social Security Administration – “Your Social Security number has been frozen, but we’ll help you keep your money ‘safe!’”

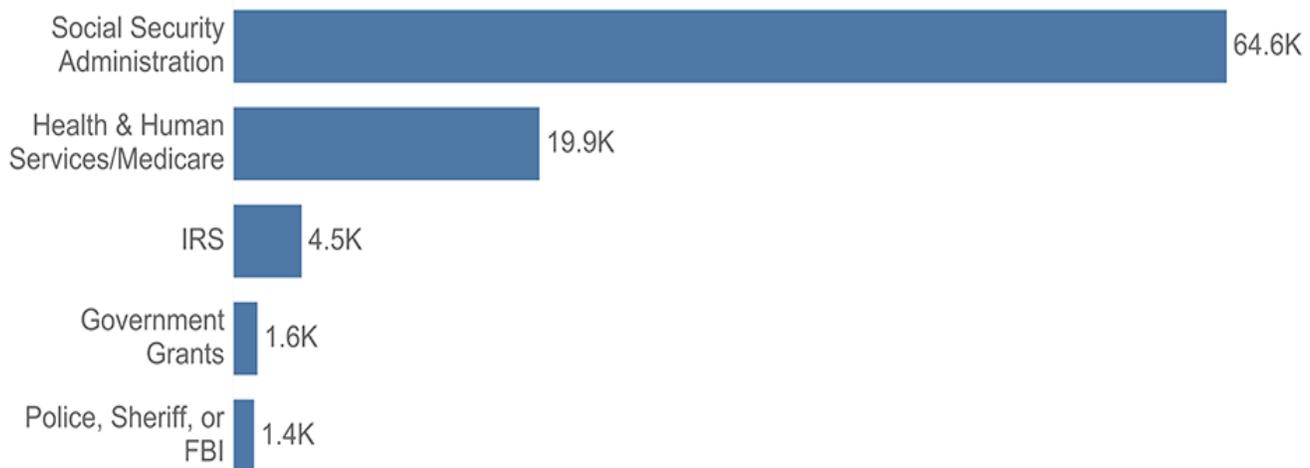
Health & Human Services/Medicare con – “Call now for your free back brace!”

IRS imposter – “There’s a lawsuit against you for unpaid taxes.”

Fake government grant offer – “You’re eligible for a government grant . . . for a fee.”

Bogus police, sheriff, or FBI – “There is a warrant for your arrest for failing to appear in court!”

Top Government Imposters by Number of Reports January - May 2019



So what can you do to protect yourself against imposters when their stories keep changing?

Be suspicious of any call from a government agency asking for money or information. Government agencies don’t call you with threats, or promises of – or demands for – money. Scammers do.

Don’t trust caller ID – it can be faked. Even if it might look like a real call, don’t trust it.

Never pay with a gift card or wire transfer. If someone tells you to pay this way, it’s a scam.

Check with the real agency. Look up their number. Call them to find out if they’re trying to reach you – and why.

Consumer Alerts

From the Federal Trade Commission



Spread The Word About Social Security Scams

Getting calls saying your Social Security number is suspended because of suspicious activity? It's a scam. The Social Security Administration (SSA) is not calling you, no matter what your caller ID says.

To spread the word about this growing scam, the Consumer Financial Protection Bureau created this fraud prevention placemat in consultation with the FTC and SSA:

Scams involving your Social Security number and benefits are on the rise!

Here are the facts:

- Government employees will not threaten to take away benefits or ask for money or personal information to protect your Social Security card or benefits.
- Scammers can fake your caller ID. So don't be fooled if the call seems to be from the SSA's real phone number (800) 772-1213 or the SSA Inspector General's Fraud Hotline number.
- If a caller asks for your Social Security number, bank account number or credit card information, hang up.

Report suspected scams to the SSA Inspector General at (800) 269-0271 or oig.ssa.gov/report. Visit IdentityTheft.gov/SSA for more tips.



In collaboration with:



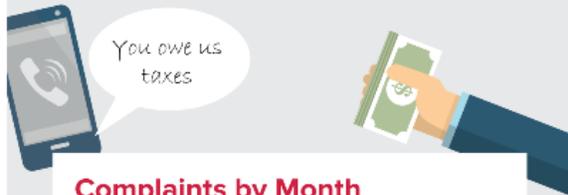
To report these scams, go to ftc.gov/complaint. And for more tips, visit IdentityTheft.gov/SSA.

IRS IMPOSTER SCAMS

on the rise

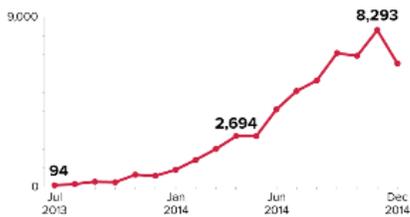
The Internal Revenue Service (IRS) is the government agency that collects federal taxes.

Scammers pretend to be IRS officials to get you to send them money.



Complaints by Month

received by the Federal Trade Commission (FTC)



HOW THE SCAM WORKS



WARNING SIGNS

How will the IRS first contact you?

phone call	NO
email	NO
mail	YES

How will the IRS ask you to pay?

with a prepaid debit card	NO
with a money transfer	NO
won't require a specific type of payment	YES

GOT A CALL?

- Don't give the caller information**
such as your financial or other personal information.
- Write down details**
such as the number and name of the caller.
- Hang up**
- Contact the IRS directly**
If you're worried the call is real, contact the IRS directly at **800-829-1040** or go to **irs.gov**.
- Report the call**
File a complaint with:
 - the Treasury Inspector General for Tax Administration (TIGTA) at **tigta.gov** or **800-366-4484**.
 - the FTC at **ftc.gov/complaint** or **877-FTC-HELP**.
- Warn friends and family**
Tell people you know that these calls are scams.

ftc.gov/taxidtheft

Federal Trade Commission
January 2015





Online Dating Scams

Here's how they work:

You meet someone special on a dating website. Soon he wants to move off the dating site to email or phone calls. He tells you he loves you, but he lives far away — maybe for business, or because he's in the military.

Then he asks for money. He might say it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers, both male and female, make fake dating profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even fake wedding plans — before they disappear with your money.

Here's what you can do:

- 1. Stop. Don't send money.** Never wire money, put money on a prepaid debit card, or send cash to an online love interest. You won't get it back.
- 2. Pass this information on to a friend.** You may not have gotten one of these calls, but chances are you know someone who will get one — if they haven't already.



Romance scams rank number one on total reported losses

People looking for romance are hoping to be swept off their feet, not caught up in a scam. But tens of thousands of reports in Consumer Sentinel show that a scam is what many people find. In 2018, Sentinel had more than 21,000 reports about romance scams, and people reported losing a total of \$143 million – that’s more than any other consumer fraud type identified in Sentinel.¹ These reports are rising steadily. In 2015, by comparison, people filed 8,500 Sentinel reports with dollar losses of \$33 million.

Romance scammers lure people with phony online profiles, often lifting photos from the web to create attractive and convincing personas. They might make up names or assume the identities of real people. Reports indicate the scammers are active on dating apps, but also on social media sites that aren’t generally used for dating. For example, many people say the scam started with a Facebook message.

Once these fraudsters have people by the heartstrings, they say they need money, often for a medical emergency or some other misfortune. They often claim to be in the military and stationed abroad, which explains why they can’t meet in person. Pretending to

need help with travel costs for a long-awaited visit is another common ruse.

Scammers can reap large rewards for time spent courting their targets. The median individual loss to a romance scam reported in 2018 was \$2,600, about seven times higher than the median loss across all other fraud types.² People often reported sending money repeatedly for one supposed crisis after another.

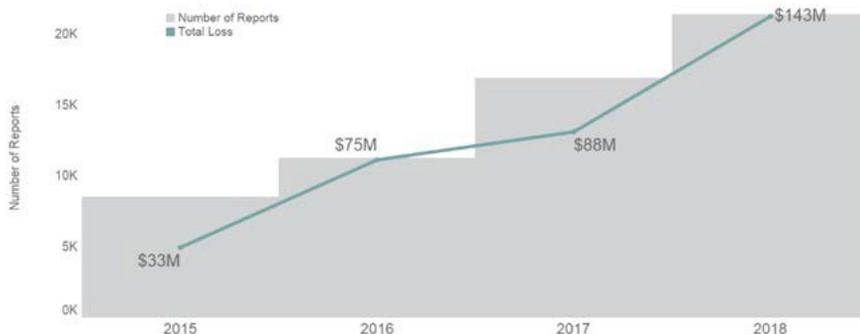
\$2,600

The **median reported loss** to romance scams is about seven times higher than for other frauds (2018).

People who said they were ages 40 to 69 reported losing money to romance scams at the highest rates – more than twice the rate of people in their 20s.³ At the same time, people 70 and over reported the highest individual median losses at \$10,000⁴

Romance Scam Reports Over Time

Reports more than doubled and reported losses increased more than fourfold from 2015 to 2018



Among people who told us how they paid the scammer, the majority said they wired money. The next largest group said they sent money using gift and reload cards (like MoneyPak), and reports of this type of payment increased in 2018. People said they mailed the cards or gave the PIN number on the back to the scammer. Consumers favor these payment methods because they can get quick cash, the transaction is largely irreversible, and they can remain anonymous.

So what can singles do to play it safe while dating online? Here are some tips to help spot bogus suitors:

- Never send money or gifts to a sweetheart you haven't met in person.
- Talk to someone you trust about this new love interest. In the excitement about what feels like a new relationship, we can be blinded to things that don't add up. Pay attention if your friends or family are concerned.

- Take it slowly. Ask questions and look for inconsistent answers. Try a reverse-image search of the profile pictures. If they're associated with another name or with details that don't match up, it's a scam.
- Learn more at ftc.gov/imposters.

Help stop these scammers by reporting suspicious profiles or messages to the dating or social media site. Then, tell the FTC at [FTC.gov/complaint](https://ftc.gov/complaint).

1 Figures based on 21,368 reports submitted directly to FTC and by all Sentinel data contributors in 2018 that were classified as romance scams.

2 Median loss calculations are based on reports submitted in 2018 that indicated a monetary loss of \$1 to \$999,999. Reports provided by MoneyGram, Western Union, and Green Dot are excluded for this calculation as these data contributors report each transaction separately, which typically affects calculation of an individual's median loss.

3 Reporting rates per million population by age calculated using population numbers obtained from the U.S. Census Bureau. U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties and Puerto Rico Commonwealth and Municipios (June 2018), available at <https://www.census.gov/data/tables/2017/demo/pepest/nation-detail.html>.

4 Median loss calculations are based on reports submitted in 2018 that indicated a monetary loss of \$1 to \$999,999. Reports provided by MoneyGram, Western Union, and Green Dot are excluded as these data contributors report each transaction separately, which may affect the median loss.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at [FTC.gov/complaint](https://ftc.gov/complaint). To explore Sentinel data, visit [FTC.gov/data](https://ftc.gov/data).



Tech Support Scams

Here's how they work:

You get a call from someone who says he's a computer technician. He might say he's from a well-known company like Microsoft, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him remote access to your computer or buy new software to fix it.

But is the caller who he says he is? Judging by the complaints to the Federal Trade Commission, no. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

Here's what you can do:

- 1. Hang up.** Never give control of your computer or your credit card information to someone who calls you out of the blue.
- 2. Pass this information on to a friend.** You might know these calls are fakes, but chances are you know someone who doesn't.



Older adults hardest hit by tech support scams

If the mere thought of your computer being hacked frightens you, you're not alone. And tech support scammers know how to exploit that fear to their own advantage. They work to scare you into believing your computer is compromised and then offer to "fix" the problem – for a fee. The FTC's Consumer Sentinel Network got nearly 143,000 reports about tech support scams in 2018.¹

These scams usually start with a phone call or a pop-up warning of a computer problem that gives a number to call. People tell us the scammers often claim to be Microsoft or Apple – they may even spoof caller ID to make it look like one of these companies really is calling. In another twist, they get people who actually do need computer help to call them by posting phony customer support numbers for well-known companies online.

These scammers convince people to hand over remote access to their computer and then make a big show of "troubleshooting." They may open system folders or run scans that seem to show evidence of a problem. Then they ask for money for supposed repairs and things like bogus service contracts.

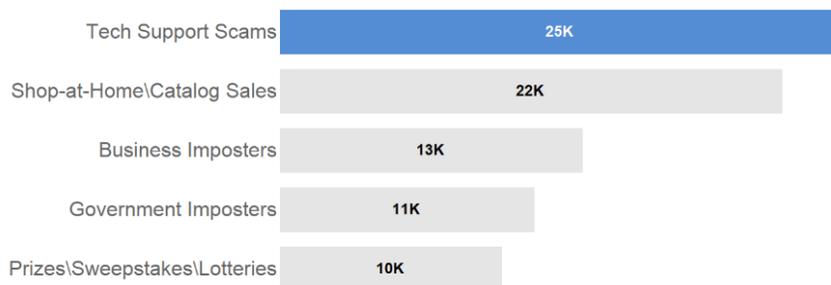
In 2018, people reported losing \$55 million to these scams. And while many people did not lose any money, those who did reported losing hundreds: the median individual reported loss was \$400. Credit cards were the top method of payment people said they used, and that's good news – credit card companies can reverse fraudulent charges. But many others said the scammer convinced them to pay by giving the PIN numbers on the back of gift cards, often iTunes or Google Play cards. For most in this group, the money is simply gone.

Older adults were about **5 times more likely** to report losing money on tech support scams (2018)

Tech support scams stand out for the disproportionate harm they may be causing older adults. While Sentinel data tells us that people 60 and older are both great at reporting fraud and *less likely* than younger people to report losing money to many types of fraud,² they are *far more likely* to report a loss to tech support scams. In 2018, people 60 and over were about five times more likely to report losing money to these scams than younger people.³ In fact, over the past four years, older adults filed more reports of a loss on tech support scams than they did in any other Sentinel fraud category.⁴ The reported median individual loss to tech support scams for older adults was \$500 last year – 25% higher than the median individual loss

Ages 60+ Top 5 Fraud Categories by Number of Reports Indicating a Loss

Older adults filed more **reports indicating a loss on tech support scams** from 2015 to 2018 than on any other Sentinel fraud category



reported by younger people.⁵

But money isn't the only thing people lose on this scam. By allowing scammers remote access to their computer, people hand over control. Scammers can then readily steal sensitive information or install spyware – a form of malware that lets them quietly gather information. People have even been persuaded to log into their bank accounts, often on the pretext of depositing a refund, allowing the scammer to move funds remotely.

Here are some things you can do to avoid these scams:

- Do not click any links or call a number that pops up on your screen warning of a computer problem.
- Hang up on unexpected calls from anyone who claims to be tech support.
- Don't believe your caller ID – it can be easily spoofed.
- Never give control of your computer or share passwords with anyone who contacts you.

- Keep your security software up to date.
- If you need help, contact a computer technician that you trust. Don't just rely on an online search.

If you've been scammed, change any passwords you shared and scan your computer for malware. If you gave your credit card number, tell the credit card company. Check your statement and contact your credit card company to reverse the charges for bogus services. If you later get a call about a supposed refund, you can bet that's part two of the same scam – hang up.

Report tech support scams to the FTC at [FTC.gov/complaint](https://www.ftc.gov/complaint). To learn more, visit [FTC.gov/techsupportscams](https://www.ftc.gov/techsupportscams).

1 Figure based on 142,904 reports to Sentinel in 2018 that were classified as tech support scams. 105,676 of these reports were provided by Microsoft Corporation's Cybercrime Center.

2 For age comparisons of other Sentinel fraud types, see Figure 4 of Protecting Older Consumers 2017 - 2018. A Report of the Federal Trade Commission.

3 Figures based on the number of 2018 tech support scam reports that indicated a monetary loss (\$1 - \$999,999) per million population by age. People who said they were 20 - 59 filed loss reports at a rate of 21.5 reports per million people in this age group, while people who said they were 60 and over filed 104.2 loss reports per million people in this age group. Population numbers obtained from the U.S. Census Bureau: U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties and Puerto Rico Commonwealth and Municipios (June 2018). In 2018, 31,043 tech support scam reports to Sentinel included usable age information.

4 This statement is based on fraud reports filed from 2015 to 2018 by people who indicated an age of 60 and over and who indicated a monetary loss.

5 Median loss calculations are based on reports submitted in 2018 that indicated a monetary loss by people who said they were 60 and over as compared to people who said they were 20 to 59. Not all reports to Sentinel indicate age.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at [FTC.gov/complaint](https://www.ftc.gov/complaint). To explore Sentinel data, visit [FTC.gov/data](https://www.ftc.gov/data).

Scammers Increasingly Demand Payment by Gift Card

Through Consumer Sentinel we hear from people across the country about frauds they encounter in the marketplace. One thing we learn from these reports is how scammers want to be paid. People are telling us that they're increasingly being told to pay with gift cards – specifically, by giving someone the PIN number off the back of a gift card. Often people are specifically asked for certain brands, like iTunes and Google Play cards.

To understand this issue better, we looked at fraud reported directly to the FTC. To avoid skewing the results, we excluded reports about shop-at-home purchases – this Spotlight is not about the use of gift cards to purchase retail goods, but rather their use as a payment vehicle for scams.

We found that from January through September of this year, gift cards and reload cards (like MoneyPak) were reported as a payment method in 26% of the fraud reports in which people told us how they paid, up from just 7% in 2015 – a 270% increase. Con artists favor these cards because they can get quick cash, the transaction is largely irreversible, and they can remain anonymous.

When people report losing money to a scam:

26%

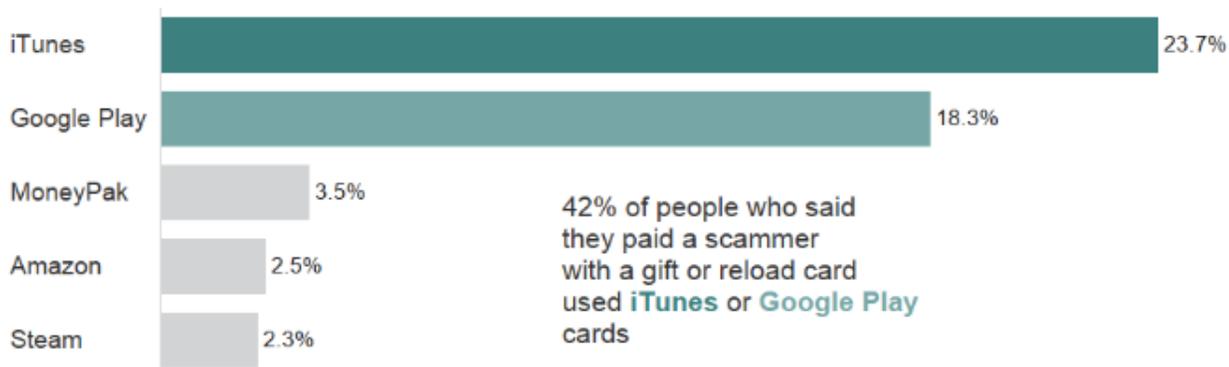
now **pay with a gift card or reload card** compared to

7%

in 2015

Scammers told them:
Go to a specific store
(Walmart, Target, Walgreens, CVS)
Buy a specific card
(iTunes, Google Play)

2018 Most Reported Gift and Reload Card Brands¹



People report that con artists direct them to buy gift or reload cards at well-known stores like Walmart, Target, Walgreens, and CVS. According to these reports, they demand some specific card brands. While these change over time, iTunes cards have been the top card brand by a wide margin since 2016. By contrast, Google Play cards were not reported in significant numbers until this year.

Stepping back to look at all fraud reports available to the FTC from all sources, we found that losses where people reported using gift or reload cards reached \$40 million in 2017, up from \$20 million in 2015 and \$27 million in 2016.² Through September of this year, that number is already \$53 million. And while individual fraud losses using these cards have held steady at a \$500 median loss per incident, people report losing a lot more to some types of scams.³ Tech support scams are a notable example.⁴ When people report paying for fraudulent tech support services with a gift or reload card, the median dollar loss is now \$959, up nearly 60% from \$600 in 2017.

It's not just tech support scams. When people report paying a fraudster with a gift or reload card, about four times out of five the fraud they report is an imposter scam – in fact, gift cards and reload cards are now the

number one reported method of payment for imposter scams. These scammers pose as well-known businesses, family members, friends, or government agencies. They deploy various tactics to compel people to pay. They may pretend to be the IRS and tell people they cannot use other payment methods because of their delinquent tax status. They may even call iTunes cards “payment vouchers.” To avoid alerting store personnel, they often direct people to buy cards from several different stores, and they tell people not to talk to anyone about why they are buying the cards.

Familiarity with these tactics and awareness of the prevalence of gift cards and reload cards as a method of payment for fraud may help people to recognize and avoid a wide range of scams. When someone demands to be paid with a gift card, that's a scam.

Payments to a fraudster made by gift card or reload card should be reported immediately to the card issuer. It may not be possible to stop funds from being withdrawn from the card, but it is important to alert companies to card fraud. Consumers should also report details of the incident to the FTC at [FTC.gov/complaint](https://www.ftc.gov/complaint). To learn more, visit [FTC.gov/giftcards](https://www.ftc.gov/giftcards).

1 Percentages are based on the total number of fraud reports that identify a gift or reload card as a method of payment. Reports provided by data contributors, reports that do not specify a method of payment, and reports classified as “shop-at-home/catalog sales” are excluded. Card brands are identified through keyword analysis of the narratives provided in this subset of reports.

2 Source: *Consumer Sentinel Network Data Book*, Federal Trade Commission (2016 and 2017).

3 Median loss calculations are based on all fraud reports in FTC's Consumer Sentinel Network database that identify gift or reload card as a method of payment and include a dollar loss value of \$1 to \$999,999.

4 Tech support scams typically involve the impersonation of computer companies like Microsoft, and start with a call or popup warning about a computer virus or other technical issue. Victims pay for “repair” of a nonexistent problem.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at [FTC.gov/complaint](https://www.ftc.gov/complaint). To explore Sentinel data, visit [FTC.gov/data](https://www.ftc.gov/data).



FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS

Get a one-ring call? Don't call back.

Who's calling now? That number doesn't ring a bell. Hold the phone, says the Federal Trade Commission. You could be a potential victim of the growing "one-ring" cell phone scam.

Here's how it works: Scammers are using auto-dialers to call cell phone numbers across the country. Scammers let the phone ring once — just enough for a missed call message to pop up.

The scammers hope you'll call back, either because you believe a legitimate call was cut off, or you will be curious about who called. If you do, chances are you'll hear something like, "Hello. You've reached the operator, please hold." All the while, you're getting slammed with some hefty charges — a per-minute charge on top of an international rate. The calls are from phone numbers with three-digit area codes that look like they're from inside the U.S., but actually are associated with international phone numbers — often in the Caribbean. The area codes include: 268, 284, 473, 664, 649, 767, 809, 829, 849 and 876.

If you get a call like this, don't pick it up and don't call the number back. There's no danger in getting the call: the danger is in calling back and racking up a whopping bill.

If you're tempted to call back, do yourself a favor and check the number through online directories first. They can tell you where the phone number is registered.

If you've been a victim of the "one-ring" scam, try to resolve the charges with your cell phone carrier. If that doesn't work, file a complaint with the [Federal Trade Commission](#) and the [Federal Communications Commission](#).

And as a general rule: Read your phone bill often — line by line. If you don't recognize or understand a charge, contact your carrier.



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

What the FTC Facebook settlement means for consumers

July 24, 2019

by Lesley Fair

Attorney, Division of Consumer & Business Education, FTC

The next time users visit Facebook, things might not look different, but big changes are brewing behind the scenes. The FTC's record-breaking \$5 billion settlement (<https://ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>) requires Facebook to conduct a massive overhaul of its consumer privacy practices. The settlement also makes major changes to Facebook's operations and CEO Mark Zuckerberg no longer has sole control over privacy.

First, some background. Facebook is a social networking site, but it makes money by serving up targeted ads based on users' personal information. Many consumers are hesitant about sharing certain data, so Facebook calms that concern by promising that people can control the privacy of their information through the platform's privacy settings.

FTC Settlement with Facebook	
	\$5,000,000,000 Unprecedented penalty
	New privacy structure at Facebook
	New tools for FTC to monitor Facebook

Source: Federal Trade Commission | FTC.gov

The FTC sued Facebook in 2012 for making misleading promises about the extent to which consumers could keep their personal information private. For example, Facebook told users they could select settings to make information available just to “friends.” But despite that promise, Facebook allowed apps used by those friends to access consumers’ information, a decision that put money in Facebook’s pocket. The 2012 FTC order put penalties in place if Facebook made misleading statements in the future about consumers’ control over the privacy of their personal information.

According to the FTC, that’s just what happened. Facebook violated the order by *again* giving companies access to information that consumers said they didn’t want to share. The FTC also alleges Facebook made other misleading statements about how it used facial recognition, consumers’ cell phone numbers, and other personal data.

Here are three things to know about the FTC’s history-making settlement with Facebook.

Facebook will pay the largest civil penalty by anyone anywhere ever in a privacy case.

The \$5 billion settlement is one for the record books. It’s the largest civil penalty ever imposed on a company for violating consumers’ privacy and it’s one of the largest penalties assessed by the U.S. government for a violation of any kind. That tells you just how seriously the FTC takes it when companies break their privacy promises. The settlement also sets a new benchmark if companies fail to honor their promises in the future. (In case you’re wondering about the \$5 billion, by law, it goes to the general fund of the U.S. Treasury. It does not go to the FTC.)

The settlement requires fundamental changes at Facebook and removes CEO Mark Zuckerberg as the company’s consumer privacy decision maker.

The order establishes a new era of privacy transparency at Facebook and at WhatsApp and Instagram, which Facebook owns. It creates an independent committee of Facebook’s board of directors to oversee privacy decisions and requires an independent third-party assessor to evaluate the effectiveness of Facebook’s privacy program. Mark Zuckerberg also must certify every quarter that Facebook is in compliance with the new privacy program. Any false certification will be subject to civil – and criminal – penalties.

As Facebook puts its new privacy program in place, consumers should take a fresh look at their settings.

How much personal information do you really want to share? A platform’s default settings may not be your most privacy-protective option. Whether it’s Facebook or any other platform, revisit your toolbars, privacy settings, etc., to make sure the system is set up to honor your choices and preferences.

Blog Topics: [Privacy, Identity & Online Security](https://www.consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security) (<https://www.consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security>).

Equifax Data Breach Settlement

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. As part of a settlement, Equifax agreed to spend up to \$425 million to help people affected by the data breach.

If you were impacted by the breach, you can:



Sign up for **free credit monitoring for up to 10 years** OR get a **cash payment of \$125** for credit monitoring you already have



Get **free identity restoration services for at least 7 years** that you can use if you are the victim of identity theft or fraud

In addition, you may be eligible for reimbursement and cash payments up to \$20,000 for:



» **Time you spent** protecting your identity or recovering from identity theft, up to 20 hours at \$25 per hour



» **Money you spent** protecting your identity or recovering from identity theft



» **Up to 25% of the cost of Equifax credit or identity monitoring** you bought in the year before the breach

Starting in January 2020, all U.S. consumers will be able to get 6 additional free credit reports per year from Equifax for seven years, regardless of whether they were impacted by the 2017 Equifax data breach. These free credit reports are in addition to the free Equifax credit report consumers are already entitled to under the law.

WHAT TO DO NEXT



The claims process will start after court approval. Go to ftc.gov/Equifax to learn more about the settlement and how to claim the benefits described above.



The Equifax Breach – A Global Settlement



\$575,000,000+ settlement



Free credit monitoring and identity theft services



Strong **data security** requirements

→ **Learn more:** ftc.gov/Equifax

Source: Federal Trade Commission | FTC.gov

Equifax Data Breach Settlement: What You Should Know

Share this page

GET EMAIL UPDATES

July 22, 2019

by Alvaro Puig

Consumer Education Specialist, FTC

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. Under a [settlement filed today](#), Equifax agreed to spend up to \$425 million to help people affected by the data breach. If you were affected by the Equifax breach, you can't file a claim just yet. That's coming. But you can sign up for FTC email alerts about the settlement at ftc.gov/Equifax.

(Not sure that you were affected? The breach claims site will have a tool to let you check. Sign up for an [FTC email update](#) to find out when that tool is up and running.)

Recent Blog Posts

[What the FTC Facebook settlement means for consumers](#)

July 24, 2019

[Equifax Data Breach Settlement: What You Should Know](#)

July 22, 2019

[Medicare does not give out DNA kits](#)

July 19, 2019

[Browse by Topic](#)

Benefits Available To You

1. Free Credit Monitoring or \$125 Cash Payment

You can get at least 4 years of free credit monitoring of your credit report at all three credit bureaus (Equifax, Experian, and TransUnion). On top of that, you can get up to 6 more years of free credit monitoring of your Equifax credit report. That's a total of 10 years of free credit monitoring. (Minors affected by the breach are eligible for even more free credit monitoring.)

If you have credit monitoring that will continue for at least 6 months and you decide not to enroll in the free credit monitoring offered in the settlement, you may be eligible for a cash payment of \$125.

2. Reimbursement for Your Time and Other Cash Payments

You may be eligible for reimbursement and cash payments up to \$20,000 for:

- **time you spent** protecting your identity or recovering from identity theft, up to 20 hours at \$25 per hour
- **money you spent** protecting your identity or recovering from identity theft, like the cost of freezing or unfreezing your credit report or unauthorized charges to your accounts
- **up to 25% of the cost of Equifax credit monitoring or identity protection products** you bought between September 7, 2016 and September 7, 2017

3. Free Identity Restoration Services

You are eligible for **free identity restoration services** for at least 7 years that you can use if someone steals your identity or you experience fraud.

Next Steps

The claims process will start after court approval. To learn more about the settlement, go to ftc.gov/Equifax. We'll update that page when there's new information.

You can also [sign up to get FTC email updates](#) about this settlement.

If you were affected by the breach, you may also receive an email notification after the court approves the settlement. The notification will provide more information about the settlement, the benefits available to people impacted, and how to request the services offered under the settlement.

Impacted by the Equifax breach?

**Learn more.
Claim your benefits.**

ftc.gov/Equifax





FEDERAL TRADE COMMISSION Consumer Information

July 30, 2019

by Seena Gressin

Attorney, Division of Consumer and Business Education

If you needed yet another nudge to start keeping an eye on your credit report to protect against identity theft, Capital One has delivered it with its announcement that a data breach has exposed the personal information of 106 million of its credit card customers and credit card applicants in the United States and Canada.

News of the Capital One breach comes just one week after the Federal Trade Commission announced that Equifax agreed to pay up to \$700 million to settle a lawsuit brought by the FTC, the Consumer Financial Protection Bureau, and 50 states and territories, stemming from the credit reporting giant's 2017 data breach, which affected about 147 million people.

In the Capital One breach, 100 million people in the United States and 6 million in Canada were affected. According to the bank, most of the stolen information came from the credit card applications of consumers and small businesses. The information includes names, dates of birth, addresses, phone numbers, and more, all from applications filed between 2005 and early 2019.

For credit card holders, the stolen information includes credit scores, credit limits, balances, payment history, contact information and some transaction data. The bank says the hacker also stole about 140,000 Social Security numbers, 80,000 linked bank account numbers of secured credit card holders, as well as the Social Insurance Numbers of about one million Canadians.

Capital One has posted information about the breach and says it will notify the people affected and offer them free credit monitoring and identity protection services. However, whether or not you were affected, there is no time like the present to check your free credit report and take other steps to protect against identity theft.

Check out these articles to read the basics about credit reports and credit monitoring. And one more thing: a data breach is a magnet for scammers. Be alert to emails and calls pretending to be from Capital One or the government. Neither the bank nor the government will send an email or call you to ask for credit card or account information or your Social Security number.

Visit [Identitytheft.gov/databreach](https://www.identitytheft.gov/databreach) to learn more about protecting yourself after a data breach.



Identity Theft

Here's how it works:

Someone gets your personal information and runs up bills in your name. They might use your Social Security or Medicare number, your credit card, or your medical insurance – along with your good name.

How would you know? You could get bills for things you didn't buy or services you didn't get. Your bank account might have withdrawals you didn't make. You might not get bills you expect. Or, you could check your credit report and find accounts you never knew about.

Here's what you can do:

- 1. Protect your information.** Put yourself in another person's shoes. Where would they find your credit card or Social Security number? Protect your personal information by shredding documents before you throw them out, by giving your Social Security number only when you must, and by using strong passwords online.
- 2. Read your monthly statements and check your credit.** When you get your account statements and explanations of benefits, read them for accuracy. You should recognize what's there. Once a year, get your credit report for free from AnnualCreditReport.com or 1-877-322-8228. The law entitles you to one free report each year from each credit reporting company. If you see something you don't recognize, you will be able to deal with it.





Your Credit History

Your credit history is important. It tells businesses how you pay your bills. Those businesses then decide if they want to give you a credit card, a job, an apartment, a loan, or insurance.

Find out what is in your report. Be sure the information is correct. Fix anything that is not correct.

How do I check my credit report?

This is easy to do by phone:

- Call Annual Credit Report at 1-877-322-8228.
- Answer questions from a recorded system. You have to give your address, Social Security number, and birth date.
- Choose to only show the last four numbers of your Social Security number. It is safer than showing your full Social Security number on your report.
- Choose which credit reporting company you want a report from. (You get one free report from each company every year.)

That company mails your report to you. It should arrive 2-3 weeks after you call.

What do I do with my credit report?

Read it carefully. Make sure the information is correct:

- Personal information – are the name and address correct?
- Accounts – do you recognize them?
 - Is the information correct?
- Negative information – do you recognize the accounts in this section of the report?
 - Is the information correct?
- Inquiries – do you recognize the places you applied for credit? (If you do not, maybe someone stole your identity.)



Your Credit History

The report will tell you how to improve your credit history. Only you can improve your credit history. It will take time. But if any of the information in your report is wrong, you can ask to have it fixed.

How do I fix mistakes in my credit report?

- Write a letter. Tell the credit reporting company that you have questions about information in your report.
- Explain which information is wrong and why you think so.
- Say that you want the information corrected or removed from your report.
- Send a copy of your credit report with the wrong information circled.
- Send copies of other papers that help you explain your opinion.
- Send this information Certified Mail. Ask the post office for a return receipt. The receipt is proof that the credit reporting company got your letter.

The credit reporting company must look into your complaint and answer you in writing.



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Is someone using your personal information to open new accounts, make purchases, or get a tax refund? **IdentityTheft.gov** can walk you through each step of the recovery process. Here's how to get started.

Visit **IdentityTheft.gov** for our most up-to-date information.

The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- get a **personal recovery plan** that walks you through each step
- **update** your plan and **track** your progress
- print **pre-filled letters & forms** to send to credit bureaus, businesses, and debt collectors
- **report** it to the Federal Trade Commission

Go to **IdentityTheft.gov** and click “**Get Started.**”

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 Identity Theft Report.

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

- To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.
 - **Experian.com/help**
888-EXPERIAN (888-397-3742)
 - **TransUnion.com/credit-help**
888-909-8872
 - **Equifax.com/personal/credit-report-services**
1-800-685-1111

Get updates at **IdentityTheft.gov/creditbureaucontacts**.

A fraud alert lasts one year. It will make it harder for someone to open new accounts in your name.

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.

Did you already order your free annual reports this year? If so, you can pay to get your report immediately. Or follow the instructions in the fraud alert confirmation letter from each credit bureau to get a free report. That might take longer.

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

Step 3: Report identity theft to the FTC.

- Go to **IdentityTheft.gov** 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.

- If you create an account, we'll 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.

CREDIT ALERTS AND FREEZES: Something to think about if you're information has been compromised or stolen: [Initiate a credit freeze](#), thanks to a new federal law, you can freeze and unfreeze your credit file for free. **What is a credit freeze?** A credit freeze allows a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. More information on credit freezes follows on the next several pages of this FTC workbook.



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Free credit freezes are here

September 21, 2018

by Andrew Smith, Federal Trade Commission, Director, Bureau of Consumer Protection

Gail Hillebrand, Bureau of Consumer Financial Protection, Associate Director, Division of Consumer Education and Engagement

Free credit freezes and year-long fraud alerts are here, starting September 21st, thanks to a new federal law. Here's what you should know:

Free credit freezes

Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. Starting September 21, 2018, you can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – [Equifax](https://www.equifax.com/personal/credit-report-services) (<https://www.equifax.com/personal/credit-report-services>), [Experian](https://experian.com/help) (<https://experian.com/help>), and [TransUnion](https://transunion.com/credit-help) (<https://transunion.com/credit-help>). If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

Year-long fraud alerts

A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

Credit freezes and the military

If you're in the military, you'll still have access to active duty alerts, which let you place a fraud alert for one year, renewable for the time you're deployed. The active duty alert also gives you an added benefit: the credit reporting agencies will take your name off their marketing lists for prescreened credit card offers for two years (unless you ask them to add you back on).

You can place a fraud alert or active duty alert by visiting any one of the three nationwide credit reporting agencies – [Equifax](https://www.equifax.com/personal/credit-report-services) (<https://www.equifax.com/personal/credit-report-services>), [Experian](https://experian.com/help) (<https://experian.com/help>) or [TransUnion](https://TransUnion.com/credit-help) (<https://TransUnion.com/credit-help>). The one that you contact must notify the other two. You also can find links to their websites at [IdentityTheft.gov/CreditBureauContacts](http://www.identitytheft.gov/creditbureaucontacts) (<http://www.identitytheft.gov/creditbureaucontacts>).

Issues with a credit freeze

If you think a credit reporting agency is not placing a credit freeze or fraud alert properly, you can submit a [complaint online](https://www.consumerfinance.gov/complaint) (<https://www.consumerfinance.gov/complaint>), or by calling 855-411-2372. If you think someone stole your identity, visit the FTC's website, [IdentityTheft.gov](https://www.identitytheft.gov) (<https://www.identitytheft.gov>), to get a personalized recovery plan that walks you through the steps to take.

For more information, check out [Place a Fraud Alert](https://www.consumer.ftc.gov/articles/0275-place-fraud-alert) (<https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>), [Extended Fraud Alerts and Credit Freezes](https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes) (<https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes>), and [Credit Freeze FAQs](https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs) (<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>). And if you're considering a child credit freeze, you also may want to read [Child Identity Theft](https://www.consumer.ftc.gov/articles/0040-child-identity-theft) (<https://www.consumer.ftc.gov/articles/0040-child-identity-theft>).

Credit Bureau Contacts

Contact the national credit bureaus to request fraud alerts, credit freezes (also known as security freezes), and opt outs from pre-screened credit offers.

Equifax

[Equifax.com/personal/credit-report-services](https://www.Equifax.com/personal/credit-report-services) (<https://www.Equifax.com/personal/credit-report-services>).

800-685-1111

Experian

Experian.com/help (<https://Experian.com/help>).

888-EXPERIAN (888-397-3742)

Transunion

TransUnion.com/credit-help (<https://TransUnion.com/credit-help>).

888-909-8872



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

New Credit Law FAQs

October 4, 2018

by Lisa Weintraub Schifferle

Attorney, FTC, Division of Consumer & Business Education

You've heard about the [new law \(https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here\)](https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here) that makes credit freezes free and fraud alerts last one year. If you have questions, you're not alone. Here are answers to some of the questions we're hearing most.

Q: I already had a credit freeze in place when the new law took effect on September 21, 2018. Is it still in effect?

A: Yes, your credit freeze is still in effect. The next time you lift or replace the freeze, it will be free.

Q: If I paid for a freeze before September 21, do I get my money back?

A: No, the new law does not provide for that. But the next time you lift or place your freeze, it will be free.

Q: Does my credit score stay the same when a credit freeze is in effect?

A: No, your credit score can still change while a freeze is in effect. A freeze on your credit file does not freeze your credit score. For example, creditors can still report delinquent accounts and that may negatively affect your score.

Q: Can I still use my credit card when a credit freeze is in place?

A: Yes, you can still use your credit card and other existing credit accounts. The freeze restricts access to your credit file. That makes it harder for identity thieves to open new accounts in your name. That's because most creditors need to see your credit file before they approve a new account. It also means that, if you're applying for a mortgage, student loan, new credit card, or other credit account, you'll need to lift the freeze first.

Q: I already had a fraud alert in place when the law took effect on September 21, 2018. Do I need to request a new fraud alert if I want a year-long alert?

A: Yes, you should request a new fraud alert. You can make the request at one of the three credit bureaus (Equifax, Experian, or TransUnion), and it will alert the other two.

Q: How is placing a fraud alert different from placing a credit freeze?

A: To place a fraud alert, notify any one of the three credit bureaus and they must inform the other two. The fraud alert stays in place for one year. To place a credit freeze, contact each of the three credit bureaus individually. A freeze stays in place until you ask the credit bureau to temporarily lift it, or remove it altogether. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you'd need to ask all three credit bureaus. For more information, read [Place a Fraud Alert \(https://www.consumer.ftc.gov/articles/0275-place-fraud-alert\)](https://www.consumer.ftc.gov/articles/0275-place-fraud-alert) and [Credit Freeze FAQs \(https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs\)](https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs).

Q: Where can I find the contact information for Equifax, Experian and TransUnion?

A: [IdentityTheft.gov/creditbureaucontacts \(http://www.identitytheft.gov/creditbureaucontacts\)](http://www.identitytheft.gov/creditbureaucontacts) lists all of the URLs and phone numbers that you can use to exercise your rights under the new law.

Q: What can I do if I'm having trouble placing a fraud alert or credit freeze?

A: Call the credit bureaus first to try to straighten things out. Then, if you still think a credit bureau is not placing an alert or freeze properly, report it to the Bureau of Consumer Financial Protection at [consumerfinance.gov/complaint \(http://www.consumerfinance.gov/complaint\)](http://www.consumerfinance.gov/complaint) or 855-411-2372.

Blog Topics: [Money & Credit \(https://www.consumer.ftc.gov/blog/money-%26-credit\)](https://www.consumer.ftc.gov/blog/money-%26-credit).



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

New protections available for minors under 16

March 11, 2019

by Jennifer Leach, FTC, Acting Associate Director, Division of Consumer & Business Education
Desmond Brown, CFPB, Deputy Assistant Director, Office of Community Affairs

Young people now have more protection from identity theft and fraud, thanks to a [new federal law](https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here) (<https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here>) that went into effect September 21st, 2018. The new law lets parents and child welfare representatives of people under 16, as well as legal guardians, request a security freeze, also called a credit freeze, on their behalf. Taking this step can help protect a young person from identity theft and fraud – and it's free.

Identity theft happens when someone misuses your personal information, such as a Social Security number, to open accounts, file taxes, or make purchases. Hackers, thieves, and even people you know might steal your identity. Minors typically don't have credit reports, which means that a young person may not find out about issues with their credit reports until they first try to get credit – perhaps even years later.

While a [security freeze](https://www.consumer.ftc.gov/blog/2018/10/new-credit-law-faqs) (<https://www.consumer.ftc.gov/blog/2018/10/new-credit-law-faqs>) won't affect anything already on your credit report, it restricts access to your report. That makes it harder for identity thieves to open new accounts using your personal information. With the new law, it's free to freeze and unfreeze your credit file at the three nationwide consumer reporting agencies – Equifax, Experian, and TransUnion. To find contact information for placing a free credit freeze, visit [IdentityTheft.gov/credit bureau contacts](http://www.identitytheft.gov/creditbureaucontacts) (<http://www.identitytheft.gov/creditbureaucontacts>).

The new law also lets people like parents, guardians, and representatives acting on behalf of a young person in foster care proactively protect a young person's credit file by freezing it.

If the nationwide credit reporting agencies don't have a file on the child, they will create one so they can freeze it. This record can't be used for credit purposes. It's there just to make sure the child's record is frozen and protected against identity theft and fraud.

Depending on the adult's relationship to the child, there are different procedures to put a freeze in place. Parents need to show proof of their authority, like a birth certificate, to freeze or unfreeze the credit file for their child under 16. The new law says that child welfare or probation agency representatives acting on behalf of a young person in foster care can request a security freeze for that child. They have to show

documentation certifying that the child is in the agency's care, such as a written communication or an official letter from the child welfare or probation agency or its designee. Child welfare agencies who already work with consumer reporting agencies to pull and review credit reports for youth in their care can use the same company contacts and liaisons to facilitate the security freeze process.

For more information about security freezes for children in foster care settings, read the CFPB's guidance. For more information about child identity theft, read the FTC's *Child Identity Theft: What to Know, What to Do* (<https://www.bulkorder.ftc.gov/publications/child-identity-theft-what-know-what-do>), and online *Child Identity Theft* article (<https://www.consumer.ftc.gov/articles/0040-child-identity-theft>). And check out our joint blog (<https://www.consumer.ftc.gov/blog/2018/09/managing-someone-elses-money-new-protection-id-theft-and-fraud-0>), to learn about how the new credit law affects adults who have a guardian or conservator.

Blog Topics: [Privacy, Identity & Online Security](https://www.consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security) (<https://www.consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security>), [Identity Theft](https://www.consumer.ftc.gov/blog/identity-theft) (<https://www.consumer.ftc.gov/blog/identity-theft>).



Charity Fraud

Here's how it works:

Someone contacts you asking for a donation to their charity. It sounds like a group you've heard of, it seems real, and you want to help.

How can you tell what charity is legitimate and what's a scam? Scammers want your money quickly. Charity scammers often pressure you to donate right away. They might ask for cash, and might even offer to send a courier or ask you to wire money. Scammers often refuse to send you information about the charity, give you details, or tell you how the money will be used. They might even thank you for a pledge you don't remember making.

Here's what you can do:

- 1. Take your time.** Tell callers to send you information by mail. For requests you get in the mail, do your research. Is it a real group? What percentage of your donation goes to the charity? Is your donation tax-deductible? How do they want you to pay? Rule out anyone who asks you to send cash or wire money. Chances are, that's a scam.
- 2. Pass this information on to a friend.** It's likely that nearly everyone you know gets charity solicitations. This information could help someone else spot a possible scam.





How to *donate wisely* and **avoid charity scams**



Research the charity



How much
goes to the charity?



Look up the
ratings/report



Never pay by gift card
or wire transfer

Do some research online

- Looking for a charity to support? Search for a cause you care about – like “hurricane relief” or “homeless kids” – and phrases like “best charity” or “highly rated charity.”
- When you consider giving to a specific charity, search its name plus “complaint,” “review,” “rating,” or “scam.”

****FOR CHARITY GUIDANCE: Do an online search for these organizations****

Organizations that can help you research charities

These organizations offer reports and ratings about how charitable organizations spend donations and how they conduct business:

- [BBB Wise Giving Alliance](#)
- [Charity Navigator](#)
- [CharityWatch](#)
- [GuideStar](#)

The IRS’s [Tax Exempt Organization Search](#) tells you if your donation would be tax deductible.

You can find your state charity regulator at [nasconet.org](#). Most states require the charity or its fundraiser to register to ask for donations.

****Here’s a trusted online source****

Keep scammers' tricks in mind

- Don't let anyone rush you into making a donation. That's something scammers do.
- Some scammers try to trick you into paying them by thanking you for a donation that you never made.
- Scammers can change caller ID to make a call look like it's from a local area code.
- Some scammers use names that sound a lot like the names of real charities. This is one reason it pays to do some research before giving.
- Scammers make lots of vague and sentimental claims but give no specifics about how your donation will be used.
- Bogus organizations may claim that your donation is tax-deductible when it is not.
- Guaranteeing sweepstakes winnings in exchange for a donation is not only a scam, it's illegal.

If you see any red flags, or if you're not sure about how a charity will use your donation, consider giving to a different charity. There are many worthy organizations who will use your donation wisely.

Report scams to [FTC.gov/complaint](https://www.ftc.gov/complaint). Find your state charity regulator at [nasconet.org](https://www.nasconet.org) and report to them, too. Share any information you have – like the name of the organization or fundraiser, phone number, and what the fundraiser said.

Be careful how you pay

- If someone wants donations in cash, by gift card, or by wiring money, don't do it. That's how scammers ask you to pay.
- To be safer, pay by credit card or check.
- It's a good practice to keep a record of all donations. And review your statements closely to make sure you're only charged the amount you agreed to donate – and that you're not signed up to make a recurring donation.
- Before clicking on a link to donate online, make sure you know who is receiving your donation. Read [Donating Through an Online Giving Portal](#) for more information.

So how do you know where your money goes, and who gets how much? The best online portals will have this information. It may take you a little bit of research on the website, but you should be able to find this information. Here's what to look for:

- **Where your money goes.** Online giving portals should tell you who gets your donation and how your money gets to the charity or beneficiary you chose.
- **Fees.** The online portal should tell you if it keeps part of your donation as a fee before sending the rest to your chosen charity. Consider whether the charity would get more of your donation if you donated to the charity directly.
- **Timing.** Online giving portals should say how long it will take for the charity to get your donation.
- **Follow-through.** Just in case your donation can't be sent to the charity you chose, the portal should say what happens in that case – and how often that happens.
- **Your info.** Check if you can choose whether or not your information is shared with the charity – or anyone else, and whether the portal gives you a choice.



Health Care Scams

Here's how they work:

You see an ad on TV, telling you about a new law that requires you to get a new health care card. Maybe you get a call offering you big discounts on health insurance. Or maybe someone says they're from the government, and she needs your Medicare number to issue you a new card.

Scammers follow the headlines. When it's Medicare open season, or when health care is in the news, they go to work with a new script. Their goal? To get your Social Security number, financial information, or insurance number.

So take a minute to think before you talk: Do you really have to get a new health care card? Is that discounted insurance a good deal? Is that "government official" really from the government? The answer to all three is almost always: No.

Here's what you can do:

- 1. Stop. Check it out.** Before you share your information, call Medicare (1-800-MEDICARE), do some research, and check with someone you trust. What's the real story?
- 2. Pass this information on to a friend.** You probably saw through the requests. But chances are you know someone who could use a friendly reminder.



Growing wave of Social Security imposters overtakes IRS scam

Claiming to be a government authority is a tried and true way that scammers trick people into sending money. Among the most common government imposters have been scammers pretending to be the IRS – until now. In the past few months, the FTC’s Consumer Sentinel Network database has seen Social Security Administration (SSA) imposter reports skyrocket while reports of IRS imposters have declined sharply. In the shady world of government imposters, the SSA scam may be the new IRS scam.

SSA imposters tell you your Social Security number has been suspended because of suspicious activity, or because it’s been involved in a crime. They ask you to confirm your Social Security number, or they may say you need to withdraw money from the bank and to store it on gift cards or in other unusual ways for “safekeeping.” You may be told your accounts will be seized or frozen if you don’t act quickly.

These scammers often use robocalls to reach people, and the message can be hard to ignore. You may be told to “press 1” to speak to a government “support representative” for help reactivating your Social Security number. They also use caller ID spoofing to make it look like the Social Security Administration

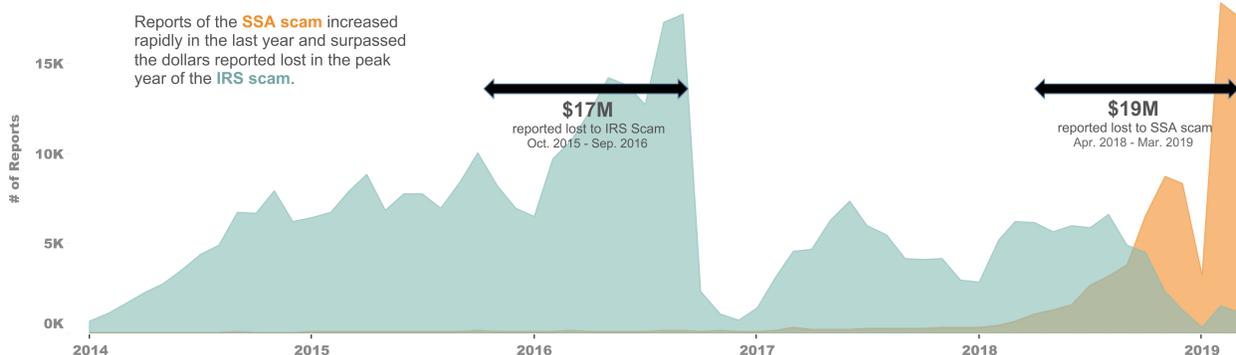
really is calling. With such trickery, these scammers are good at convincing people to give up their Social Security numbers and other personal information.

As the graphic shows, people reported the IRS scam (in blue) in huge numbers for many years, but the new SSA scam (in orange) is trending in the same direction – with a vengeance. People filed over 76,000 reports about Social Security imposters in the past 12 months, with reported losses of \$19 million.¹ Compare that to the \$17 million in reported losses to the IRS scam in its peak year.² About 36,000 reports and \$6.7 million in reported losses are from the past two months alone.

Just 3.4% of people who report the Social Security scam tell us they lost money.³ Most people we hear from are just worried because they believe a scammer has their Social Security number. But when people do lose money, they lose a lot: the median individual reported loss last year was \$1,500, four times higher than the median individual loss for all frauds.⁴ All age groups are reporting this scam in high numbers, with older and younger adults filing loss reports at similar rates.⁵

People report sending money in unconventional ways.

IRS Scam and Social Security Administration Scam Reports



Most often, people say they gave the scammer the PIN numbers on the back of gift cards. Virtual currencies like Bitcoin come in a distant second to gift cards: people say they withdrew money and fed cash into Bitcoin ATMs. With both methods, the scammer gets quick cash while staying anonymous, and the money people thought they were keeping safe is simply gone.

Here are some tips to deal with these imposters:

- **Do not trust caller ID.** Scam calls may show up on caller ID as the Social Security Administration and look like the agency's real number.
- **Don't give the caller your Social Security number or other personal information.** If you already did, visit [IdentityTheft.gov/SSA](https://www.IdentityTheft.gov/SSA)

to find out what steps you can take to protect your credit and your identity.

- **Check with the real Social Security Administration.** The SSA will not contact you out of the blue. But you can call them directly at 1-800-772-1213 to find out if SSA is really trying to reach you and why.
- **Talk about it.** People recognize the IRS scam, but many are getting caught off guard by these new imposters. You can help by telling people that the SSA scam is a new version of the IRS scam.

Report government imposter scams to the FTC at [FTC.gov/complaint](https://www.ftc.gov/complaint). To learn more, visit [ftc.gov/imposters](https://www.ftc.gov/imposters).

1 The FTC was unable to collect reports directly from the public during the government shutdown. Reports collected during that period were provided by Sentinel data contributors.

2 From October 1, 2015 to September 30, 2016, about 140,000 reports of IRS imposter scams were filed and collectively indicated \$17 million of loss.

3 For comparison, 2.8% of IRS scam reports filed from January 2014 through March 2019 indicated a loss. In 2018, 25% of all fraud reports indicated a loss.

4 Median loss calculations are based on reports submitted in 2018 that indicated a monetary loss (\$1 - \$999,999). The median reported individual loss to all frauds was \$371 in 2018.

5 Age comparison based on the number of Social Security imposter reports that indicated a monetary loss per million population by age. People who said they were 20 – 59 filed loss reports at a rate of 8.9 reports per million people in this age group, while people who said they were 60 and over filed 10.0 loss reports per million people in this age group. Population numbers obtained from the U.S. Census Bureau: U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States, States, Counties and Puerto Rico Commonwealth and Municipios (June 2018). Not all reports include usable age information.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at [FTC.gov/complaint](https://www.ftc.gov/complaint). To explore Sentinel data, visit [FTC.gov/data](https://www.ftc.gov/data).



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Ask a health professional before popping that pill

April 10, 2019

by Bridget Small

Consumer Education Specialist

When I was young, I wanted the shoes that would make me run faster and jump higher. Now, I wish my brain would run a little faster when I can't remember my account passwords. Unfortunately, some shady outfits have been trying to “help” people like me by making some mind-blowing claims to sell their dietary supplements.

The FTC just settled charges (<https://www.ftc.gov/news-events/press-releases/2019/04/geniux-dietary-supplement-sellers-barred-unsupported-cognitive>), against four people and a dozen businesses that sold bottles of “cognitive enhancement” supplements through a collection of websites, including fake news websites. The FTC says the defendants falsely claimed Geniux, Xcel, EVO, and Ion-Z could increase users’ focus, concentration, IQ, and brainpower. The settlement bans them from making false or unsupported health claims and requires them to pay over \$600,000.

According to the FTC, the defendants didn’t have proof that Geniux can increase concentration by 312 percent, boost brainpower by up to 89.2 percent, and enhance memory recall. They made these claims on websites designed to look like real news sites and featuring false claims that Bill Gates, Elon Musk and Stephen Hawking got dramatic results from Geniux. The FTC also says that customers — who paid up to \$57 per bottle — couldn’t get a promised 100% money back guarantee.

If you’re considering a dietary supplement, remember: the government doesn’t review (<https://www.consumer.ftc.gov/articles/0261-dietary-supplements>) or evaluate supplements for safety or effectiveness before they’re put on the market. Your health care professional is the most important person to ask whether a supplement is safe for you. Even a natural supplement can be risky depending on your health and the medicine you take. If you see an ad with claims about miracle cures (<https://www.consumer.ftc.gov/articles/0538-dietary-supplement-ads-infographic>), ask a professional about the science behind the claims. If you think a product is being advertised falsely, please tell the FTC at [FTC.gov/Complaint](https://www.ftccomplaintassistant.gov/#crnt&panel1-1). (<https://www.ftccomplaintassistant.gov/#crnt&panel1-1>).

Blog Topics: Health & Fitness (<https://www.consumer.ftc.gov/blog/health-%26-fitness>).



“You’ve Won” Scams

Here’s how they work:

You get a card, a call, or an email telling you that you won! Maybe it’s a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can’t wait for you to get your winnings.

But here’s what happens next: they tell you there’s a fee, some taxes, or customs duties to pay. And then they ask for your credit card number or bank account information, or they ask you to wire money.

Either way, you lose money instead of winning it. You don’t ever get that big prize. Instead, you get more requests for money, and more promises that you won big.

Here’s what you can do:

- 1. Keep your money – and your information – to yourself.** Never share your financial information with someone who contacts you and claims to need it. And never wire money to anyone who asks you to.
- 2. Pass this information on to a friend.** You probably throw away these kinds of scams or hang up when you get these calls. But you probably know someone who could use a friendly reminder.





FEDERAL TRADE COMMISSION

CONSUMER INFORMATION

consumer.ftc.gov

Prize Scams

You've just won \$5,000! Or \$5 million. Or maybe it's a fabulous diamond ring, or luxury vacation? More likely, it's a prize scam, and you'll find the prize isn't worth much — if you get a prize at all. Here's one way to think about it: if you have to pay, it's not a prize.

- About Contests and Prizes
- Signs of a Prize Scam
- Foreign Lotteries
- Text Message Prize Offers
- Check Them Out
- Report a Scam

About Contests and Prizes

Who doesn't want to win something? But before you drop in a quick entry or follow instructions to claim a prize, here are a few things to know:

Legitimate sweepstakes are free and by chance

It's illegal to ask you to pay or buy something to enter or increase your odds of winning.

Prize promoters might sell your information to advertisers

When you sign up for a contest or drawing, you probably will get more promotional mail, telemarketing calls, or spam email instead of a prize.

Prize promoters have to tell you certain things

Telemarketers are legally required to tell you the odds of winning, the nature or value of the prizes, that entering is free, and the terms and conditions to redeem a prize. Sweepstakes mailings also must tell you that you don't have to pay to participate. They also can't claim that you're a winner unless you've actually won a prize. And they're not legally permitted to include fake checks that don't clearly state they're non-negotiable and have no cash value.

Signs of a Prize Scam

Plenty of contests are run by reputable marketers and non-profits. But every day, people lose thousands of dollars to prize scams. Here are some signs you're dealing with a scam:

You have to pay

Legitimate sweepstakes don't make you pay a fee or buy something to enter or improve your chances

of winning — that includes paying "taxes," "shipping and handling charges," or "processing fees" to get your prize. There's also no reason to give someone your checking account number or credit card number in response to a sweepstakes promotion.

A skills contest where you do things like solve problems or answer questions correctly *can* ask you to pay. But these contests also tend to get more difficult and expensive as you advance, leaving contestants with nothing to show for their money and effort.

You have to wire money

You may be told to wire money to an agent of "Lloyd's of London" or another well-known company — often in a foreign country — to "insure" delivery of the prize. Don't do it. Wiring money is like sending cash: once it's gone, you can't trace it or get it back. The same goes for sending a check or money order by overnight delivery or courier, or putting money on a prepaid debit card.

You have to deposit a check they've sent to you

When you do, they'll ask you to wire a portion of the money back. The check will turn out to be a fake, and you will owe the bank any money you withdrew.

You're told they're from the government — or another organization with a name that sounds official

They might say they're from an agency like the Federal Trade Commission and are informing you that you've won a federally supervised lottery or sweepstakes. Or they might use an official-sounding name like "the national consumer protection agency" or the non-existent "National Sweepstakes Bureau." But they're imposters. The FTC doesn't oversee sweepstakes, and no federal government agency or legitimate sweepstakes company will contact you to ask for money so you can claim a prize.

Other scammers might pretend to be a company like Publishers Clearing House or Reader's Digest, which run legitimate sweepstakes. Look for signs of a scam, but if you're still unsure, contact the real companies to find out the truth.

Your "notice" was mailed by bulk rate

It's not likely you've won a big prize if your notification was mailed by bulk rate. Other people got the same notice, too. Check the postmark on the envelope or postcard. Do you even remember entering? If not, odds are you didn't.

You have to attend a sales meeting to win

If you agree to attend, you're likely to endure a high-pressure sales pitch. In fact, any pressure to "act now" before you miss out on a prize is a sign of a scam.

You get a call out of the blue, even though you're on the Do Not Call Registry

Once you register your phone number for free at donotcall.gov, unwanted telemarketing calls should stop within 30 days. Unless the company falls under one of the exemptions, it shouldn't be calling: it's illegal.

Foreign Lotteries

Sometimes a letter you get will say you've won a foreign lottery or sweepstakes. Typically, the letter will include a check. This is a fake check scam. Or a letter will say they're offering you a chance to enter a foreign lottery. The truth is that, even if your name was entered, it's illegal to play a foreign lottery.

Text Message Prize Offers

You get a text message that says you've won a gift card or other free prize. When you go to the website and enter your personal information, you'll also be asked to sign up for "trial offers" — offers that leave you with recurring monthly charges. Worse, the spammer could sell your information to identity thieves.

When you see a spam text offering a gift, gift card, or free service, report it to your carrier, then delete it. Don't reply or click on any links; often, they install malware on your computer and take you to spoof sites that look real but are in business to steal your information.

Check Them Out

Scammers don't obey the law. To avoid a scam, you have to do some research. If you're not sure about a contest or promoter, try typing the company or product name into your favorite search engine with terms like "review," "complaint" or "scam." You also might check it out with your state attorney general or local consumer protection office.

Keep in mind that many questionable prize promotion companies don't stay in one place long enough to establish a track record, so if no complaints come up, it's no guarantee that the offer is real.

Report a Scam

If you think you've been targeted by a prize scam, report it to the FTC.

You also can contact your:

- state attorney general
- local consumer protection office
- local media's call for action lines

If the prize promotion came in the mail, report it to the U.S. Postal Inspection Service.

April 2014



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Fake Debt Collectors

Consumers across the country report that they're getting telephone calls from people trying to collect on loans the consumers never received or on loans they did receive but for amounts they do not owe. Others are receiving calls from people seeking to recover on loans consumers received but where the creditors never authorized the callers to collect for them. So what's the story?

The Federal Trade Commission (FTC), the nation's consumer protection agency, is warning consumers to be on the alert for scam artists posing as debt collectors. It may be hard to tell the difference between a legitimate debt collector and a fake one. Sometimes a fake collector may even have some of your personal information, like a bank account number. A caller may be a fake debt collector if he:

- is seeking payment on a debt for a loan you do not recognize;
- refuses to give you a mailing address or phone number;
- asks you for personal financial or sensitive information; or
- exerts high pressure to try to scare you into paying, such as threatening to have you arrested or to report you to a law enforcement agency.

If you think that a caller may be a fake debt collector:

- **Ask the caller for his name, company, street address, and telephone number.** Tell the caller that you refuse to discuss any debt until you get a written "validation notice." The notice must include the amount of the debt, the name of the creditor you owe, and your rights under the federal Fair Debt Collection Practices Act.
If a caller refuses to give you all of this information, do not pay! Paying a fake debt collector will not always make them go away. They may make up another debt to try to get more money from you.
- **Stop speaking with the caller.** If you have the caller's address, send a letter demanding that the caller stop contacting you, and keep a copy for your files. By law, real debt collectors must stop calling you if you ask them to in writing.
- **Do not give the caller personal financial or other sensitive information.** Never give out or confirm personal financial or other sensitive information like your bank account, credit card, or Social Security number unless you know whom 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.

- **Contact your creditor.** If the debt is legitimate – but you think the collector may not be – contact your creditor about the calls. Share the information you have about the suspicious calls and find out who, if anyone, the creditor has authorized to collect the debt.
- **Report the call.** Contact the FTC and your state Attorney General's office with information about suspicious callers. Many states have their own debt collection laws in addition to the federal FDCPA. Your Attorney General's office can help you determine your rights under your state's law.

February 2012

Related Items

- [Time-Barred Debts \(https://www.consumer.ftc.gov/articles/0117-time-barred-debts\)](https://www.consumer.ftc.gov/articles/0117-time-barred-debts).
- [Debts and Deceased Relatives \(https://www.consumer.ftc.gov/articles/0081-debts-and-deceased-relatives\)](https://www.consumer.ftc.gov/articles/0081-debts-and-deceased-relatives).
- [Coping with Debt \(https://www.consumer.ftc.gov/articles/0150-coping-debt\)](https://www.consumer.ftc.gov/articles/0150-coping-debt).
- [Hiring a Lawyer \(https://www.consumer.ftc.gov/articles/0180-hiring-lawyer\)](https://www.consumer.ftc.gov/articles/0180-hiring-lawyer).



Paying Too Much

Here's how it works:

Everyone pays all kinds of bills. Some are higher than you think they should be. Sometimes, unexpected charges appear on your bill – or sometimes, you might see a fee for a service you don't recall ordering. Are you paying more than you should?

You are your own best advocate. How often does a company figure out that you've overpaid – and refund your money? It could happen – but you're more likely to get money back if you spot the error and point it out.

It means keeping track of what you normally pay, and what the charges are for. You also can ask for a better deal: call to see if there's a promotion you qualify for and how long it will last, or if they can lower your interest rate. They might say no – but if you don't ask, you don't get.

Here's what you can do:

- 1. Read every statement, every time.** Does something look wrong or unfamiliar? Call the company and ask. If you don't like the response you get, ask for a supervisor. And keep written records of your calls.
- 2. Pass this information on to a friend.** Not paying more than you need to might come easily to you. But you probably know someone who could use some friendly encouragement.





FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Timeshares and Vacation Plans

The thought of owning a vacation home may sound appealing, but the year-round responsibility — and expense — that come with it may not. Buying a timeshare or vacation plan may be an alternative. If you're thinking about opting for a timeshare or vacation plan, the Federal Trade Commission (FTC), the nation's consumer protection agency, says it's a good idea to do some homework. If you're not careful, you could end up having a hard time selling your timeshare.

- The Basics of Buying a Timeshare (#basics)
- Before You Buy a Timeshare (#before)
- Timeshare Exchange Systems (#timeshare)
- Selling a Timeshare Through a Reseller (#selling)

The Basics of Buying a Timeshare

Two basic vacation ownership options are available: timeshares and vacation interval plans. The value of these options is in their use as vacation destinations, not as investments. Because so many timeshares and vacation interval plans are available, the resale value of yours is likely to be a good deal lower than what you paid. Both a timeshare and a vacation interval plan require you to pay an initial purchase price and periodic maintenance fees. The initial purchase price may be paid all at once or over time; periodic maintenance fees are likely to increase every year.

Deeded Timeshare Ownership. In a timeshare, you either own your vacation unit for the rest of your life, for the number of years spelled out in your purchase contract, or until you sell it. Your interest is legally considered real property. You buy the right to use a specific unit at a specific time every year, and you may rent, sell, exchange, or bequeath your specific timeshare unit. You and the other timeshare owners collectively own the resort property.

Unless you've bought the timeshare outright for cash, you are responsible for paying the monthly mortgage. Regardless of how you bought the timeshare, you also are responsible for paying an annual maintenance fee; property taxes may be extra. Owners share in the use and upkeep of the units and of the common grounds of the resort property. A homeowners' association usually handles management of the resort. Timeshare owners elect officers and control the expenses, the upkeep of the resort property, and the selection of the resort management company.

“Right to Use” Vacation Interval Option. In this option, a developer owns the resort, which is made up of condominiums or units. Each condo or unit is divided into “intervals” — either by weeks or the equivalent in points. You purchase the right to use an interval at the resort for a specific number of years — typically between 10 and 50 years. The interest you own is legally considered personal property. The specific unit you use at the resort may not be the same each year. In addition to the price for the right to use an interval, you pay an annual maintenance fee that is likely to increase each year.

Within the “right to use” option, several plans can affect your ability to use a unit:

- **Fixed or Floating Time.** In a fixed time option, you buy the unit for use during a specific week of the year. In a floating time option, you use the unit within a certain season of the year, reserving the time you want in advance; confirmation typically is provided on a first-come, first-served basis.
- **Fractional Ownership.** Rather than an annual week, you buy a large share of vacation ownership time, usually up to 26 weeks.
- **Biennial Ownership.** You use a resort unit every other year.
- **Lockoff or Lockout.** You occupy a portion of the unit and offer the remaining space for rental or exchange. These units typically have two to three bedrooms and baths.
- **Points-Based Vacation Plans.** You buy a certain number of points, and exchange them for the right to use an interval at one or more resorts. In a points-based vacation plan (sometimes called a vacation club), the number of points you need to use an interval varies according to the length of the stay, size of the unit, location of the resort, and when you want to use it.

Before You Buy a Timeshare

In calculating the total cost of a timeshare or vacation plan, include mortgage payments and expenses, like travel costs, annual maintenance fees and taxes, closing costs, broker commissions, and finance charges. Maintenance fees can rise at rates that equal or exceed inflation, so ask whether your plan has a fee cap. You must pay fees and taxes, regardless of whether you use the unit.

To help evaluate the purchase, compare these costs with the cost of renting similar accommodations with similar amenities in the same location for the same time period. If you find that buying a timeshare or vacation plan makes sense, comparison shopping is your next step.

- Evaluate the location and quality of the resort, as well as the availability of units. Visit the facilities and talk to current timeshare or vacation plan owners about their experiences. Local real estate agents also can be good sources of information. Check for complaints about the resort developer and management company with the state Attorney General (<http://www.naag.org>) and local consumer protection officials (<http://www.usa.gov/directory/stateconsumer/index.shtml>).
- Research the track record of the seller, developer, and management company before you buy. Ask for a copy of the current maintenance budget for the property. Investigate the policies on management, repair, and replacement furnishings, and timetables for promised services. You also can search online for complaints.

- Get a handle on all the obligations and benefits of the timeshare or vacation plan purchase. Is everything the salesperson promises written into the contract? If not, walk away from the sale.
- Don't act on impulse or under pressure. Purchase incentives may be offered while you are touring or staying at a resort. While these bonuses may present a good value, the timing of a purchase is your decision. You have the right to get all promises and representations in writing, as well as a public offering statement and other relevant documents.
- Study the paperwork outside of the presentation environment and, if possible, ask someone who is knowledgeable about contracts and real estate to review it before you make a decision.
- Get the name and phone number of someone at the company who can answer your questions — before, during, and after the sales presentation, and after your purchase.
- Ask about your ability to cancel the contract, sometimes referred to as a “right of rescission.” Many states — and maybe your contract — give you a right of rescission, but the amount of time you have to cancel may vary. State law or your contract also may specify a “cooling-off period” — that is, how long you have to cancel the deal once you've signed the papers. If a right of rescission or a cooling-off period isn't required by law, ask that it be included in your contract.
- If, for some reason, you decide to cancel the purchase — either through your contract or state law — do it in writing. Send your letter by certified mail, and ask for a return receipt so you can document what the seller received. Keep copies of your letter and any enclosures. You should receive a prompt refund of any money you paid, as provided by law.
- Use an escrow account if you're buying an undeveloped property, and get a written commitment from the seller that the facilities will be finished as promised. That's one way to help protect your contract rights if the developer defaults. Make sure your contract includes clauses for “non-disturbance” and “non-performance.” A non-disturbance clause ensures that you'll be able to use your unit or interval if the developer or management firm goes bankrupt or defaults. A non-performance clause lets you keep your rights, even if your contract is bought by a third party. You may want to contact an attorney who can provide you with more information about these provisions.

Be wary of offers to buy timeshares or vacation plans in foreign countries. If you sign a contract outside the U.S. for a timeshare or vacation plan in another country, you are not protected by U.S. laws.

Timeshare Exchange Systems

An exchange allows a timeshare or vacation plan owner to trade units with another owner who has an equivalent unit at an affiliated resort within the system. Here's how it works: A resort developer has a relationship with an exchange company, which administers the service for owners at the resort. Owners become members of the exchange system when they buy their timeshare or vacation plan. At most resorts, the developer pays for each new member's first year of membership in the exchange company, but members pay the exchange company directly after that.

To participate, a member must deposit a unit into the exchange company's inventory of weeks available for exchange. When a member takes a week from the inventory, the exchange company charges a fee.

In a points-based exchange system, the interval is automatically put into the inventory system for a specified period when the member joins. Point values are assigned to units based on length of stay, location, unit size, and seasonality. Members who have enough points to secure the vacation accommodations they want can reserve them on a space-available basis. Members who don't have enough points may want to investigate programs that allow banking of prior-year points, advancing points, or even "renting" extra points to make up differences.

Whether the exchange system works satisfactorily for owners is another issue to look into before buying. Keep in mind that you will pay all fees and taxes in an exchange program whether you use your unit or someone else's.

TIMESHARE RESALE SCAMS Don't a timeshare? You could be the target of a timeshare resale scam.

TIMESHARE QUICK FACTS

- TIME IS TAKING AWAY YOUR MONEY
- HIGH RESALE PRICES
- HARD TO RESALE

HOW A TIMESHARE RESALE SCAM WORKS

- You sell a timeshare you want to sell.
- You get sold to one company that offers to buy it.
- You pay them to pay money (FTB).
- You pay hundreds or even thousands of dollars.
- You find out there is no buyer, and you can't get your money back.

FEDERAL TRADE COMMISSION
ftc.gov/travel

(<https://www.consumer.ftc.gov/articles/0368-timeshare-resale-scams-infographic>).

Timeshare Resale Scams
Infographic

Selling a Timeshare Through a Reseller

If you're thinking of selling a timeshare, the FTC cautions you to question resellers — real estate brokers and agents who specialize in reselling timeshares. They may claim that the market in your area is "hot" and that they're overwhelmed with buyer requests. Some may even say that they have buyers ready to purchase your timeshare, or promise to sell your timeshare within a specific time.

If you want to sell your deeded timeshare, and a company approaches you offering to resell your timeshare, go into skeptic mode:

- Don't agree to anything on the phone or online until you've had a chance to check out the reseller. Contact the state Attorney General (<http://www.naag.org/>) and local consumer protection agencies (<http://www.usa.gov/directory/stateconsumer/index.shtml>) in the state where the reseller is located. Ask if any complaints are on file. You also can search online for complaints.
- Ask the salesperson for all information in writing.
- Ask if the reseller's agents are licensed to sell real estate where your timeshare is located. If so, verify it with the state Real Estate Commission. Deal only with licensed real estate brokers and agents, and ask for references from satisfied clients.
- Ask how the reseller will advertise and promote the timeshare unit. Will you get progress reports? How often?
- Ask about fees and timing. It's preferable to do business with a reseller that takes its fee after the timeshare is sold. If you must pay a fee in advance, ask about refunds. Get refund policies and promises in writing.
- Don't assume you'll recoup your purchase price for your timeshare, especially if you've owned it for less than five years and the location is less than well-known.

If you want an idea of the value of a timeshare that you're interested in buying or selling, consider using a timeshare appraisal service. The appraiser should be licensed in the state where the service is located. Check with the state to see if the license is current.

Contract Caveats

Before you sign a contract with a reseller, get the details of the terms and conditions of the contract. It should include the services the reseller will perform; the fees, commissions, and other costs you must pay and when; whether you can rent or sell the timeshare on your own at the same time the reseller is trying to sell your unit; the length or term of the contract to sell your timeshare; and who is responsible for documenting and closing the sale.

If the deal isn't what you expected or wanted, don't sign the contract. Negotiate changes or find another reseller.

Resale Checklist

Selling a timeshare is a lot like selling any other piece of real estate. But you also should check with the resort to determine restrictions, limits, or fees that could affect your ability to resell or transfer ownership. Then, make sure that your paperwork is in order. You'll need:

- the name, address, and phone number of the resort
- the deed and the contract or membership agreement
- the financing agreement, if you're still paying for the property
- information to identify your interest or membership
- the exchange company affiliation
- the amount and due date of your maintenance fee

- the amount of real estate taxes, if billed separately

To learn more about vacation ownership, contact the American Resort Development Association. It represents the vacation ownership and resort development industries. ARDA has nearly 1,000 members, ranging from privately-held companies to major corporations, in the U.S. and overseas.

American Resort Development Association

1201 15th Street N.W., Suite 400

Washington, D.C. 20005

(202) 371-6700; Fax: (202) 289-8544

www.arda.org (<http://www.arda.org/>).

July 2012

Related Items

- [How to File a Complaint \(https://www.consumer.ftc.gov/media/video-0054-how-file-complaint\)](https://www.consumer.ftc.gov/media/video-0054-how-file-complaint)
- [Rental Listing Scams \(https://www.consumer.ftc.gov/articles/0079-rental-listing-scams\)](https://www.consumer.ftc.gov/articles/0079-rental-listing-scams)
- [Travel Tips \(https://www.consumer.ftc.gov/articles/0046-travel-tips\)](https://www.consumer.ftc.gov/articles/0046-travel-tips)
- [Battling Bed Bugs \(https://www.consumer.ftc.gov/articles/0139-battling-bed-bugs\)](https://www.consumer.ftc.gov/articles/0139-battling-bed-bugs)
- [Before You Buy Paint \(https://www.consumer.ftc.gov/articles/0253-you-buy-paint\)](https://www.consumer.ftc.gov/articles/0253-you-buy-paint)
- [Shopping for Light Bulbs \(https://www.consumer.ftc.gov/articles/0164-shopping-light-bulbs\)](https://www.consumer.ftc.gov/articles/0164-shopping-light-bulbs)



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Tips for Using Public Wi-Fi Networks

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

To protect your information when using wireless hotspots, send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information.

- How Encryption Works (#encryption)
- How to Tell if a Website is Encrypted (#tell)
- What About Mobile Apps? (#Mobile)
- Don't Assume a Wi-Fi Hotspot is Secure (#assume)
- Protect Your Information When Using a Public Wi-Fi (#protect)

How Encryption Works

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so it's not accessible to others. When you're using wireless networks, it's best to send personal information only if it's encrypted — either by an encrypted

website or a secure Wi-Fi network. An encrypted website protects **only** the information you send **to and from that site**. A secure wireless network encrypts **all** the information you send using that network.

How to Tell If a Website is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server — a powerful computer that collects and delivers content. Many websites, like banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the start of the web address (the “s” is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit, not just when you sign in.

What About Mobile Apps?

Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information properly, so it's a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions — like filing your taxes, shopping with a credit card, or accessing your bank account — use a secure wireless network or your phone's data network (often referred to as 3G or 4G).

If you must use an unsecured wireless network for transactions, use the company's mobile website — where you can check for the **https** at the start of the web address — rather than the company's mobile app.

Don't Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and **aren't** secure. In fact, if a network doesn't require a WPA or WPA2 password, it's probably not secure.

If you use an unsecured network to log in to an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools — available for free online — make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people in your contact lists. In addition, a hacker could test your username and password to try to gain access to other websites — including sites that store your financial information.

Protect Your Information When Using Public Wi-Fi

Here's how you can protect your information when using Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you’re logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don’t stay permanently signed in to accounts. When you’ve finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn’t automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. What’s more, VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don’t protect you on all websites — look for **https** in the URL to know a site is secure.
- Take steps to [secure your home wireless network \(https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network\)](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network).

March 2014

Related Items

- [Invasion of the Wireless Hackers \(https://www.consumer.ftc.gov/media/game-0006-invasion-wireless-hackers\)](https://www.consumer.ftc.gov/media/game-0006-invasion-wireless-hackers)
- [Protect Your Computer from Malware \(https://www.consumer.ftc.gov/media/video-0056-protect-your-computer-malware\)](https://www.consumer.ftc.gov/media/video-0056-protect-your-computer-malware)
- [Computer Security \(https://www.consumer.ftc.gov/articles/0009-computer-security\)](https://www.consumer.ftc.gov/articles/0009-computer-security)
- [Securing Your Wireless Network \(https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network\)](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network)
- [Understanding Mobile Apps \(https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps\)](https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps)



FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Understanding Mobile Apps

If you have a smart phone or other mobile device, you probably use apps – to play games, get turn-by-turn directions, access news, books, weather, and more. Easy to download and often free, mobile apps can be so much fun and so convenient that you might download them without thinking about some key considerations: how they're paid for, what information they may gather from your device, or who gets that information.

- Mobile App Basics (#basics)
- Questions About Your Privacy (#privacy)
- Questions About Advertising (#advertising)
- Malware and Security Concerns (#malware)
- Mobile App User Reviews (#users)
- Kids and Mobile Apps (#kids)

Mobile App Basics

What's a mobile app?

A mobile app is a software program you can download and access directly using your phone or another mobile device, like a tablet or music player.

What do I need to download and use an app?

You need a smart phone or another mobile device with internet access. Not all apps work on all mobile devices. Once you buy a device, you're committed to using the operating system and the type of apps that go with it. The Android, Apple, Microsoft, Amazon, and BlackBerry mobile operating systems have app stores online where you can look for, download, and install apps. Some online retailers also offer app stores. You'll have to use an app store that works with your device's operating system. To set up an account, you may have to provide a credit card number, especially if you're going to download an app that isn't free.

Data Plans and Wi-Fi: Two ways to access the internet from your phone

You can access the internet using a data plan tied to your phone service, or through a Wi-Fi

hotspot. Phone companies generally charge a monthly fee for a data plan that can connect you to the internet.

Wi-Fi connections usually are faster, but you have to be in range of a hotspot to use one. Most public Wi-Fi hotspots – like those in coffee shops, airports, and hotels – don't encrypt the information you send over the internet and are not secure. Get [tips for using public Wi-Fi \(/articles/0014-tips-using-public-wi-fi-networks\)](/articles/0014-tips-using-public-wi-fi-networks).

To set up a home wireless network, you'll need to pay for internet access and a wireless router, and you'll want to take steps to [secure the network \(/articles/0013-securing-your-wireless-network\)](/articles/0013-securing-your-wireless-network).

Why are some apps free?

Some apps are distributed for free through app stores; the developers make money in a few ways:

- Some sell advertising space within the app. The app developers can earn money from the ads, so they distribute the app for free to reach as many users as possible.
- Some apps offer their basic versions for free. Their developers hope you'll like the app enough to upgrade to a paid version with more features.
- Some apps allow you to buy more features within the app itself. Usually, you are billed for these in-app purchases through the app store. Many devices have settings that allow you to block in-app purchases.
- Some apps are offered free to interest you in a company's other products. These apps are a form of advertising.

Questions About Your Privacy

What types of data can apps access?

When you sign up with an app store or download individual apps, you may be asked for permission to let them access information on your device. Some apps may be able to access:

- your phone and email contacts
- call logs
- internet data
- calendar data
- data about the device's location
- the device's unique IDs
- information about how you use the app itself

Some apps access only the data they need to function; others access data that's not related to the purpose of the app.

Remember that someone may be collecting data on the websites you visit, the apps you use, and the information you provide when you're using the device – whether it's the app developer, the app store, an advertiser, or an ad network. And if they're collecting your data, they may share it with other companies. If you are concerned about how your information is being shared, check the “privacy” settings on your device or look for ways to “opt-out” of data collection in the app privacy policy.

How can I tell what information an app will access or share?

It's not always easy to know what data a specific app will access, or how it will be used. Before you download an app, consider what you know about who created it and what it does. The app stores may include information about the company that developed the app, if the developer provides it. If the developer doesn't provide contact information – like a website or an email address – the app may be less than trustworthy.

If you're using an Android operating system, you will have an opportunity to read the “permissions” just before you install an app. Read them. It's useful information that tells you what information the app will access on your device. Ask yourself whether the permissions make sense given the purpose of the app; for example, there's no reason for an e-book or “wallpaper” app to read your text messages.

Why do some apps collect location data?

Some apps use specific location data to give you maps, coupons for nearby stores, or information about who you might know nearby. Some provide location data to ad networks, which may combine it with other information in their databases to target ads based on your interests and your location.

Once an app has your permission to access your location data, it can do so until you change the settings on your phone. If you don't want to share your location with advertising networks, you can turn off location services in your phone's settings. But if you do that, apps won't be able to give you information based on your location unless you enter it yourself.

Your phone uses general data about its location so your phone carrier can efficiently route calls. Even if you turn off location services in your phone's settings, it may not be possible to completely stop it from broadcasting your location data.

Questions About Advertising

Why does the app I downloaded have ads in it?

Developers want to provide their apps as inexpensively as possible so lots of people will use them. If they sell advertising space in the app, they can offer the app for a lower cost than if it didn't have ads. Some developers sell space in their apps to ad networks that, in turn, sell the space to advertisers.

Why do I see the ads I do?

Advertisers believe you're more likely to click on an ad targeted to your specific interests. Some ad networks gather the information apps collect, including your location data, and may combine it with information about your Internet browsing habits or the kind of information you provide when you register for a service or buy something online.

Malware and Security Concerns

Should I update my apps?

Your phone may indicate when updates are available for your apps. It's a good idea to update the apps you've installed on your device and the device's operating system when new versions are available. Updates often have security patches that protect your information and your device from the latest malware.

Could an app infect my phone with malware?

Some hackers have created apps that can infect phones and mobile devices with malware. If your phone sends email or text messages that you didn't write, or installs apps that you didn't download, you could be looking at signs of malware.

If you think you have malware on your device, you have options: you can contact customer support for the company that made your device or you can contact your mobile phone carrier for help.

Mobile App User Reviews

Can I trust all the user reviews I read about an app?

Most app stores include user reviews that can help you decide whether to download. But some app developers and their marketers have posed as consumers to post positive comments about their own products. In fact, the Federal Trade Commission recently sued a company for posting fake comments about the apps it was paid to promote.

Kids and Mobile Apps

What should I know before I download an app for my kids?

In a recent [survey of mobile apps for kids](https://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf) (<https://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>), FTC staff found that kids' apps might:

- collect and share personal information
- let your kids spend real money — even if the app is free
- include ads
- link to social media

What's more, the apps might not tell you they're doing it.

To learn more about an app before you download it, look at screen shots, read the description, content rating and any user reviews, and do some research on the developer. You also can look up outside reviews from sources you respect.

Are there ways to restrict how my kids use apps?

Before you pass the phone or tablet to your kids, take a look at your settings. You may be able to restrict content to what's right for your kid's age, set a password so apps can't be downloaded without it, and set a password so your kids can't buy stuff without it. You also can turn off Wi-Fi and data services or put your phone on airplane mode so it can't connect to the internet.

Keeping Up With Kids' Apps

4 Things your kid's apps might do — but might not tell you*

- They might collect and share personal info: 59% share personal info, 11% get phone
- They might let your kids spend real money — even if the app is free: 84% of new apps that allow purchases within the app are free to download
- They might include ads: 58% include ads, 9% get you ad
- They might link to social media: 22% link to social media, 9% get you ad

*Based on Mobile Apps for Kids: How Parents Don't Get Along the Inside of It, by the FTC.

What you can do
The best way to check out apps for your kids? Try them out yourself.

At the online app store

- Look at screen shots
- Follow a link to read about the developer
- Read the description, content rating, and user reviews

On your couch

- Download and play the app with your kids
- Talk to your kids about your rules for using apps

On your phone or tablet

- Change your settings, if your phone or tablet allows it
 - Restrict content to what's right for your kid's age
 - Set a password so apps can't be downloaded without it
 - Set a password so your kids can't buy stuff without it
- Search for outside reviews of the app from sources you respect
- Turn off Wi-Fi and data services or put your phone on airplane mode so it can't connect to the internet

Federal Trade Commission | March 2013 | input@ftc.gov/mobileapps

(<http://articles/0351-keeping-kids-apps-infographic>)

Keeping Up With Kids' Apps Infographic

The best way to keep up with kids' apps is try them out yourself and talk to your kids about your rules for using apps.

February 2017

Related Items

- [Tips for Using Public Wi-Fi Networks \(https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks\)](https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks)
- [Computer Security \(https://www.consumer.ftc.gov/articles/0009-computer-security\)](https://www.consumer.ftc.gov/articles/0009-computer-security)



Home » News & Events » Media Resources » The Do Not Call Registry » Enforcement

The Do Not Call Registry

ENFORCEMENT
ROBOCALLS

Enforcement



ENFORCEMENT OF THE DO NOT CALL REGISTRY

The FTC takes aggressive legal action to make sure telemarketers abide by the Do Not Call Registry. To date, the Commission has brought 131 enforcement actions against companies and telemarketers for Do Not Call, abandoned call, robocall and Registry violations. The Mortgage Investors litigation produced the largest settlement for Do Not Call violations, resulting in civil penalty payments of \$7.5 million. To date, 121 of these FTC enforcement actions have been resolved, and in those cases the agency has recovered over \$49 million in civil penalties and \$71 million in redress or disgorgement.

Your top 5 questions about unwanted calls and the National Do Not Call Registry

March 9, 2015

by Bikram Bandy

Attorney, Division of Marketing Practices, FTC

1. How can I make it stop?

You signed up for the [Do Not Call Registry](#) ages ago, but you're suddenly getting a bunch of unwanted calls. What can you do?

Hang up. When you get illegal sales calls or [robocalls](#), don't interact in any way. Don't press buttons to be taken off the call list or to talk to a live person. That just leads to more calls. Instead, hang up and file a complaint at [donotcall.gov](#).

Investigate whether call blocking can help.

If you're getting repeated calls from the same number, your phone company may be able to block that number, but first ask whether there's a fee for this service.

If you're getting unwanted calls from a lot of different numbers, look into a call blocking solution. There are online call blocking services, call blocking boxes, and smartphone apps that block unwanted calls. Do an online search to look for reviews from experts and other users, and find out whether the service costs money.

2. Why me?

Your number is on the Do Not Call Registry, so why are you still getting calls?

Because of scammers. Most legitimate companies don't call if your number is on the Registry. If a company is ignoring the Registry, there's a good chance that it's [a scam](#).

We've seen a significant increase in the number of illegal sales calls — particularly robocalls. Advances in technology have made it cheap and easy for scammers to make illegal calls from anywhere in the world, and to hide from law enforcement by displaying fake caller ID information.

3. What are you doing about it?

The FTC has sued hundreds of companies and individuals for placing unwanted calls. The FTC also is [leading several initiatives](#) to develop technology-based solutions. Those initiatives include a series of robocall contests that challenge tech gurus to design tools that block robocalls and help investigators track down and stop robocallers. We're also encouraging industry efforts to combat caller ID spoofing.

4. Is anyone listening?

You filed a complaint — or several complaints — and you want to know when you'll hear back from the FTC.

Due to the volume of complaints we get, we can't respond directly to each one. But please keep the complaints coming because the FTC and other law enforcement agencies analyze complaints to spot trends and to take legal action against wrongdoers. To date, the FTC has brought more than a hundred lawsuits against companies and individuals for Do Not Call violations.

5. But I gave you the phone number of the company that called me?!

Current technology makes it easy for scammers to fake or "spoof" caller ID information, so the number you reported in your complaint probably isn't real. Without more information, it's difficult for us to identify the actual caller. Nonetheless, the FTC analyzes complaint data to identify illegal callers based on calling patterns. The agency also is pursuing a variety of technology-based solutions to combat illegal calls and practices.

Still have more questions? Check out the FTC's updated [FAQs about the Do Not Call Registry](#).

10 Years of Do Not Call

Protecting Consumer Privacy



105
cases



\$118 Million
in civil penalties
ordered by courts



\$737 Million
in other recovery
ordered by courts

Nov. 7
2007

6 Settlements

FTC announces 6 settlements: Craftmatic Industries, ADT Security Services, and Ameriquest Mortgage Company, among them.

July 27
2010

200 Million Numbers

DNC Registry tops 200 million numbers.

Aug. 31
2011

Refunds

FTC returns \$3.2 million to auto warranty robocall victims.

Nov. 1
2012

5 Robocall Companies Shut Down

FTC charges 5 companies with making millions of illegal robocalls from "Rachel" and others at "Cardholder Services."

Robocalls

New technologies present a new challenge to DNC enforcement.



34
cases



\$51 Million
in civil penalties
ordered by courts



\$198 Million
in other recovery
ordered by courts





****For more information, visit [FTC.gov/calls](https://www.ftc.gov/calls)****

How to stop unwanted calls ON A MOBILE PHONE



See what **built-in features** your phone has.



See what services your **carrier** offers.



Download a **call-blocking app**.

- Some apps are **free**, but others charge a monthly **fee**.
- Some apps will **access your contacts**.
- Calls might be **stopped, ring silently**, or go straight to **voicemail**.



Report unwanted calls at [ftc.gov/complaint](https://www.ftc.gov/complaint)

FEDERAL TRADE COMMISSION • [ftc.gov/calls](https://www.ftc.gov/calls)

Related Resources

You can find a list of some call-blocking apps for mobile phones at [ctia.org](https://www.ctia.org), a website for the U.S. wireless communications industry. Your options will depend on the type of device you have:

How to stop unwanted calls ON A LANDLINE



See what services your **carrier** offers.



Some services are **free**, but others charge a monthly **fee**.



Install a **call-blocking device**.

Some use **blacklists** to

- stop unwanted calls
- divert calls to voicemail

Some use **whitelists** of approved numbers.



Report unwanted calls at [ftc.gov/complaint](https://www.ftc.gov/complaint)

FEDERAL TRADE COMMISSION • [ftc.gov/calls](https://www.ftc.gov/calls)

Related Resources

For company-specific information about blocking calls on landlines and phones that use the internet, go to [ftc.gov](https://www.ftc.gov).



Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

...Pass it ON

Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the scammers and stop them before they can get someone's hard-earned money. It really makes a difference.

