AARP®

Fraud Watch Network

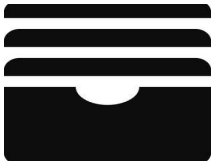
6 Steps to Freeze Criminals out of Your Credit Report *(and it's free!)*

Step 1

Gather your Social Security number, birth date and past addresses. Be familiar with recent borrowing. You may be asked, for instance, about your mortgage balance.

Step 2

Label a physical file folder, "Credit Freeze." You will need to store important information in this folder in the event you want to unfreeze and refreeze your credit.



Step 3

Call or go to one of the three main credit bureaus' websites (below). If you're asked to create an account, write down your username and password. Add it to your folder.

Step 4

To verify your identity, you will need to furnish your past and present addresses (and maybe other personal info).

Step 5

You'll receive or create a PIN. Make sure to write this down and add it to your folder.

Step 6

Repeat this process with the other two credit bureaus. When done, put your folder in a secure place.

Keep in Mind

You can also freeze the credit reports of your family members (children under age 16). Children's credit reports are a hot commodity among thieves, so it's worth considering.

Contact Info to Freeze Your Credit Report

- Equifax: equifax.com • 800-685-1111 • (if in NY) 800-349-9960
- Experian: experian.com • 888-397-3742
- TransUnion: transunion.com • 888-909-8872

When it comes to fraud, vigilance is our number one weapon. You have the power to protect yourself and your loved ones from scams. And if you have been targeted by a scam, call the **AARP Fraud Watch Network Helpline** at **1-877-908-3360** for guidance and support.

THE CON ARTIST'S PLAYBOOK

The Psychology Behind ID Theft, Fraud & Scams

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

AARP® Fraud Watch Network

AARP FRAUD WATCH NETWORK: HELPING YOU GET INSIDE THE MINDS OF SCAMMERS

Fraud is a multi-billion dollar industry with scammers constantly looking for new and ever-more sophisticated ways to steal our personal Information and your hard earned money.

What tricks do con artists use to steal your money? How can you outsmart scammers before they strike?

The AARP Fraud Watch Network is working to empower you in the fight against fraud. It puts proven tools and resources right at your fingertips:

The Con-Artist's Playbook is an inside look at how scammers think, so you can protect yourself and your family.

- Scam alerts, delivered right to your inbox;
- A scam-tracking map featuring warnings from law enforcement and people in your community who are sharing their experiences so you'll know what to watch out for;
- A phone number you can call to talk to AARP volunteers specially-trained in how to spot and report fraud. The AARP Fraud Watch Network Helpline can be reached at 1-877-908-3360.

The Con Artist's Playbook was developed based on hundreds of undercover fraud tapes and hours of interviews with victims and con artists. It shines a spotlight on the common strategies scammers use and gives you the tools to defend yourself against their tricks.

AARP: A HISTORY OF SAFEGUARDING AMERICANS' FINANCIAL SECURITY

AARP began more than 60 years ago when its founder, Dr. Ethel Percy Andrus, discovered a retired teacher living in a chicken coop. She was appalled that a woman who worked her whole life couldn't even afford a place to live. She started AARP to protect the financial security of older Americans. Fighting identity theft and fraud is part of that core mission.

HOW CON ARTISTS THINK...

REELING IN VICTIMS

When authorities ask convicted con artists to describe the trick to scamming people out of money, many say the same thing: "Get them under the ether."

WHAT IS ETHER?

Ether is a heightened emotional state that makes it hard to think clearly and make rational decisions. Think about the first time you fell in love. Were you thinking clearly? Probably not.

To induce ether, the con artist will look for ways to move you out of logical thought and into an emotional reaction. For instance, they might ask you about your relationship with your granddaughter or whether you have concerns about running out of money. Once they find something you care about that triggers emotions, they will "throttle up" on that trigger and get you to focus on it until you are in a heightened emotional state.

A con man named "Rocky" worked as a consultant to numerous fraudulent boiler rooms in the 1980s and 1990s (boiler rooms are where con artists gather and together dial for their next victims). Here he describes how he trained other cons to induce ether:

"Ether is a condition that a master closer puts a prospect in by hitting their fear, greed and urgency buttons. I would tell prospects, I wanted to keep the victim up in the altitude of the ether, because once they drop into the valley of logic, I've lost them."

WATCHDOG WARNING

Wait 24 hours for the excitement of a sales pitch to wear off to give you time to check out the company and the product.

ETHER IS A CONDITION THAT A MASTER CLOSER PUTS YOU IN BY HITTING YOUR FEAR, GREED, AND URGENCY BUTTONS.

MAKING THE PERSONAL CONNECTION

Scammers will develop a victim profile by asking a series of personal questions so they can find your emotional trigger.

Jimmy Edwards worked in 30 fraudulent boiler rooms over an 8-year period before finally being arrested and convicted of fraud. Here is how he describes the con artists' use of profiling to scam people.

"The con gathers an arsenal of information by being personable and being friendly. They are making notes: two children, one with a mental illness, one brother lost in Vietnam. They're using all that information to put together their arsenal and profile the person they are on the phone with so they know which buttons to push to bring the emotion up in that person. When I wrap that in tons of emotion, that blurs, the logic goes out the window, the emotion kicks in, now I've endeared you to me, now I'm no longer the predator on the phone, I'm Jim from New York."

Scammers will ask a series of personal questions to help them find a prospect's emotional trigger.

Another con man said, "I would ask the victim questions I had no business asking and they had no business answering."Some examples:

"Let me ask you something. It sounds like you have a wonderful home there. How much is that mortgage each month?"

"If you don't mind my asking, how long has your husband been deceased?"

WATCHDOG WARNING

Never engage a stranger in a dialogue about your personal life. If you feel yourself getting emotionally excited by an offer, stop and wait at least 24 hours to give yourself time for the ether to wear off and to do some due diligence about the company.

PROMISING BIG WINS

Phantom riches are something you want, but can't have. The con artist will dangle that phantom in front of you in order to get your emotion up so you will make an impulsive decision. According to the Financial Industry Regulatory Authority (FINRA), this is one of the most common tactics found in undercover audiotapes of con pitches.

Jeremy Shipman worked in numerous gold coin scam rooms over a 5-year period. He describes the use of phantom riches this way. "We would tell people that gold would absolutely double in value in the next one to two years and that the prospect would be able to rely on it making them far more money than any other investment vehicle."

Phantom riches are something you want, but can't have. The con artist will dangle them in front of you to get your emotion up, in the hopes of triggering an impulsive decision.

WHAT ARE SOME EXAMPLES OF PHANTOM RICHES?

"And the grand prize is $25,000 in cold, hard cash."

"You are looking at returns that are just astronomical, like 57,000 percent."

"I have a check for you for $232,000 that I have been holding for over a year now."

"I have some excellent news for you. You came out as the grand prize winner."

"The Florida lottery is up to $30 million dollars this Saturday night! If you join our club, you will have 4,800 tickets – that's 4,800 chances to win."

Most of these claims come with a requirement to pay a "processing fee" or "taxes" before you can collect.

WATCHDOG WARNING

Whenever you are approached with this kind of a pitch to win large amounts of money, pay attention to your reaction. Does your heart start beating faster? Does sweat form on your forehead? Do you start imagining all the things you could do with the winnings? These are signs of being under the ether. Never decide to buy in this condition. Virtually all lotteries, prizes and sweepstakes offers that require payment to win are scams.

FRAMING THE PITCH

Scarcity is this idea that we have in our heads that if something is rare or scarce, it must be more valuable. So, the con artist will try to paint a picture that what they have to offer is rare or available only for a limited time.

Stephen Michaels owned and operated fraudulent boiler rooms for over 20 years before being arrested by FBI agents at his home early one morning. Here is how he used the scarcity tactic.

"Now John, back in 1860 from the Philadelphia mint, there were 22,625 of these coins minted. Of those 22,000, only four have survived. Only four for God's sakes, just four remain and are available only from me."

By claiming that there are only four coins left, he gets you to start panicking that if you don't buy now, you may never be able to again.

The con artist will try to paint a picture that what they have to offer is rare or available only for a limited time.

OTHER EXAMPLES OF SCARCITY USED IN FRAUD PITCHES:

"There are only 24 hours left before this offer will expire, so you have to act now."

"You were one of only 17 people selected to win the grand prize."

"We only have four units left on this investment offer so you need to make a decision soon or you will miss out."

WATCHDOG WARNING

Whenever you get approached with an offer that is available only for a limited time or is in limited supply, beware! There are very few legitimate offers out there that can't wait for you to do some due diligence and make a rational decision.

THREATENING FOR MONEY

The use of fear and intimidation is a tactic that has emerged in recent years to badger you into handing over money. It is not uncommon for some con artists from other countries to call a potential victim 50-60 times a day to get them to invest.

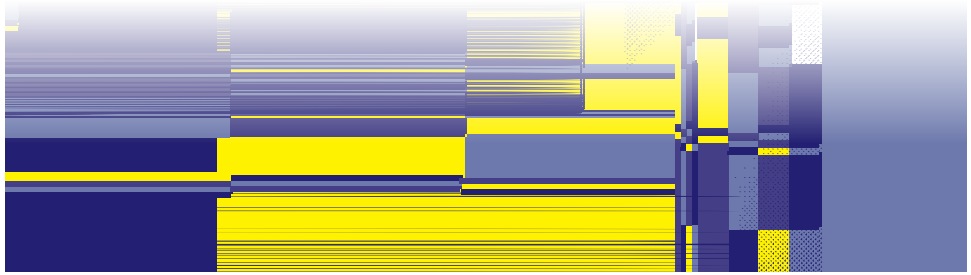
Jean Smith was one such victim. Jean received a call from a man in Jamaica who told her she had won the $7.9 million dollar Jamaican lottery. All she had to do was pay the taxes to collect. Over a 6-month period, this man called Jean hundreds of times and convinced her to wire over $30,000 in taxes and processing fees to Jamaica. When she finally stopped answering her phone, he left voice mail messages on her answering machine:

"Why you don't want to pick up the [expl] phone? Pick up the [expl] phone when I am calling you and stop playing games with me. Want me to come over there and set your home on fire?"

The use of fear and intimidation is sometimes used to badger prospects.

WATCHDOG WARNING

If you know someone who is being harassed by con artists or anyone else for that matter, consider calling the police and filing a report. If you are receiving such calls yourself, let the calls go to voice mail and don't engage. Find out if your phone company can block the caller.



Visit the AARP Fraud Watch Network for tips and other information to help protect against scams.

NOTES:

With offices and resources in every state, AARP is uniquely equipped to help people safeguard themselves against ID theft and fraud. We have a big megaphone to raise awareness about how con artists target their victims and a network of thousands of volunteers trained to inform people about fraud and help those who've been victimized.

Vigilance against scammers is our number one weapon. By being informed about the latest scams and knowing what red flags to look for, you have the power to protect yourself and your family.

Visit the AARP Fraud Watch Network for tips and other information to help protect against scams.

aarp.org/fraudwatchnetwork

aarp.org/fraudwatchnetwork

Watchdog Alerts / Tips & Resources / Free for Everyone

AARP®

Fraud Watch Network

D19949 (1218)

AARP Fraud Watch Network

Cyber Safety Community Presentation
Glossary of Terms

Anti-spyware
Programs designed to search your hard drive for traces of known spyware and adware.

Anti-virus software
A program that scans your hard drive for viruses and other "infections" and isolates any threats it finds.

Encryption
The process of encoding a message so that it can only be read by the sender and the intended recipient.

Firewall
A part of a computer system or network that blocks unauthorized access while permitting outward communication.

Malware
Malicious software that is harmful to a computer user, such as a virus, a worm, spyware or a Trojan horse.

Man in the middle
An attack where the hacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Phishing
An email or text message that looks legitimate but is a scammer trying to get you to share sensitive information.

Private Network
A network that has rules and restrictions that only allows access by authorized users.

Public Wi-Fi
A type of network to which anyone has access.

Spyware
Software that gathers information through the user's Internet connection without his or her knowledge. Once installed, the spyware monitors user activity on the Internet and transmits that information to someone else. Spyware can gather e-mail addresses, passwords and credit card numbers.

Trojan Horse
Malware that is often disguised as legitimate software. Once activated, a Trojan horse can enable hackers to spy on you, steal sensitive data and gain access to your system.

Virtual Private Network
Using the internet to connect to a private network, using encryption and other security measures to limit access to authorized users.

Virus
Malware that copies itself and can cause harm to the computer.

Wardriving
When a hacker drives around in a car with a smart phone or other device looking for unlocked or poorly protected Wi-Fi networks.

Wi-Fi
A wireless networking technology that allows computers and other devices to communicate over a wireless signal.

Worm
Malware that replicates itself to spread to other computers.

AARP Washington

FRAUD WATCH NETWORK

FRAUD & IDENTITY THEFT

- **AARP Fraud Fighter Call Center:** Speak with trained volunteers by calling **877-908-3360**
- **AARP Fraud Watch Network:** Receive notices about scams and fraud attempts in your area by registering your e-mail at www.aarp.org/fraudwatchnetwork
- **Federal Trade Commission Fraud Report:** Visit www.ReportFraud.ftc.gov or call **877-382-4357**
- **Federal Trade Commission Identity Theft Report:** Visit www.identitytheft.gov or call **877-438-4338**
- **Washington State Office of the Attorney General:** Visit www.atg.wa.gov or call **800-551-4636**
- **Fraud Alert Notice:** Contact the three top credit reporting agencies to flag an fraud activity by calling the follow-ing numbers -- Equifax at **888-766-0008** -- Experian at **888-397-3742** -- TransUnion **800-680-7289**
- **Tools to Prevent Fraud:** Thwart scammers by using **USPS Informed Delivery, password managers, alerts and more** by reading *4 Free or Inexpensive Tools to Prevent Fraud* by AARP Washington State Director Doug Shadel at https://www.aarp.org/money/scams-fraud/info-2019/tech-tools-fraud.html
- **Senior Medicare Patrol** - Prevention and reporting of Medicare fraud in WA State, contact State Health Insurance Benefits Advisors (SHIBA) at www.insurance.wa.gov or call **800-562-6900**

COMPUTER & PHONE SAFETY

- **National Cyber Security Alliance:** Find information and resources you need to be safer and more secure online at www.staysafeonline.org
- **Internet Crime Complaint Center:** If you, or someone you know has been scammed, or to report suspicious activity, visit the FBI's Internet Crime Complaint Center at www.ic3.gov
- **Federal Communications Commission:** Stop illegal and spoofed robocalls and texts. Visit www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts or call **882-225-5322**

COVID-19 INFORMATION & REPORTING FRAUDULENT ACTIVITY

- **Washington State Information on Coronavirus:** www.coronavirus.wa.gov or call **800-525-0127**
- **U.S. Dept. of Justice's Coronavirus Fraud Response:** Learn how to better protect you and your family from being victimized by COVID-19 scams and fraud by visting www.justice.gov/coronavirus/combattingfraud
- **Unemployment Insurance Imposter Fraud:** If you suspect you're a victim of UI Imposter fraud, report immedi-ately at www.esd.wa.gov/fraud or by calling **855-682-0785**
- I**RS-Related Coronavirus Scams:** If you think you have been targeted by an IRS-related coronavirus scam which could include IRS imposters, attempts to contact about Economic Impact Payments and others, you can file a complaint with the U.S. Treasury's office at https://www.treasury.gov/tigta/contact_report_covid_complaint.shtml
- **Stimulus Payment:** Check the status of your stimulus payment at www.irs.gov/coronavirus/get-my-payment

FINANCIAL SECURITY

- **Free Credit Reports**: Request your three free credit reports each year at www.annualcreditreport.com or by calling **877-322-8228**. Stagger inquiries to one every trimester for a yearly snapshot from each credit agency.
- **Financial Industry Regulatory Authority:** Verify the validity of investment products at www.FINRA.org or call **844-574-3577**. Check a broker's background and confirm whether s/he is licensed, has had regulatory actions or complaints. BrokerCheck Help Line **800-289-9999** brokercheck.finra.org
- **Charity Verification:** Verify the legitimacy of a charitable organization with the Washington Secretary of State at www.sos.wa.gov/charities or by calling **800-332-4483**. You can also check via Charity Navigator at www.charitynavigator.org or Charity Watch www.charitywatch.org
- **Financial Exploitation:** To report suspected financial exploitation of an adult in Washington State please call **866-ENDHARM** (**866-363-4276**) or report online at www.dshs.gov/altsa.
- **Consumer Financial Protection Bureau:** To report complaints regarding financial institutions, and access assistance with mediation and compensation visit www.consumerfinance.gov or call **855-411-2372**

OTHER USEFUL RESOURCES

- **Do Not Call Registry:** Register your phone for the National Do Not Call Registry managed by the Federal Trade Commission at www.donotcall.gov or call **888-382-1222**
- **Limit Credit and Insurance Offers:** Prevent Consumer Credit Reporting Companies from providing your credit file information for firm offers of credit or insurance at www.OptOutPrescreen.com or call **888-567-8688**
- **USPS Informed Delivery:** View greyscale images of the exterior, address side of letter-sized mail pieces and track packages in one convenient location. Sign up at https://informeddelivery.usps.com
- **Northwest Justice Project:** The Northwest Justice Project provides legal assistance to eligible low-income families and individuals needing help with civil (non-criminal) legal problems in Washington state. Visit www.nwjustice.org/get-legal-help or call **877-387-7111**
- **Washington 2-1-1:** For a free, confidential, one-stop connection to local community services including utility assistance, food, housing, healthcare, elder care, crisis intervention and more dial **2-1-1** or visit wa211.org
- **Washington Department of Labor & Industries:** Confirm that contractors you hire to work at your home are licensed, bonded and insured. www.contractors.lni.wa.gov or call **800-647-0982**

CONNECT WITH AARP WASHINGTON

Website: www.aarp.org/wa **Twitter**: www.twitter.com/aarpwa **Facebook**: www.facebook.com/aarpwa

Instagram: www.instagram.com/aarpwa **YouTube:** www.youtube.com/aarpwashington

Podcast: Search 'podcast AARP Washington State' in your preferred browser

Gift Card Payment Scams

Gift cards are popular and convenient…and not just as gifts. Con artists have latched onto gift cards as a convenient form of payment in their scams.

How these scams work:

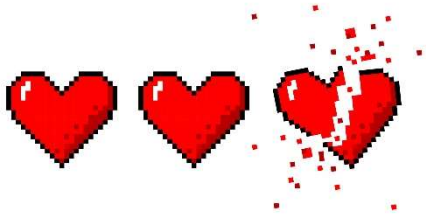
- You are contacted about an urgent financial matter, and are told the quickest way to address the issue is to buy one or more gift cards – often referred to as "electronic vouchers."
- You are told to share the numbers on the back of the gift cards either by reading them over the phone or taking and sending a picture.
- The scammer is able to quickly convert the card balance into cash and then disappear.
- This tactic is common in impostor scams – a call from Social Security warns of a problem with your account; a utility company call warns of an imminent shutoff; you've won big in a lottery and just need to pay some fees upfront; your grandchild faces a financial emergency.

What you should know:

- ANYTIME you are directed to pay some fee or obligation by purchasing a gift card and sharing the numbers off the back, it is a scam.
- If you are confronted by someone directing you to buy gift cards for some obligation, disengage immediately.
- Report it to the Federal Trade Commission at reportfraud.ftc.gov. The data are used to identify trends and build cases against criminals.

To learn more about gift card payment scams, visit aarp.org/giftcards.
For help determining if something is legitimate, or if you have experienced a scam, call the AARP Fraud Watch Network Helpline at 1-877-908-3360.

The Red Flags of Romance Scams



Lots of people meet friends and potential love interests online through dating sites, social media, or mobile apps. It can be a great way to meet people, but recognize that not everyone is who they say they are online.

Beware the romance scam.

It's a red flag if the person:

- Wants to leave the dating site immediately and use personal email or instant messaging to communicate
- Professes love too quickly
- Claims to be from the U.S., but is traveling or working overseas
- Plans to visit, but cancels at the last minute because of a traumatic event or a business deal gone sour
- Asks for money for a variety of reasons (travel, medical emergencies, losses from a financial setback)

What you can do:

- Cut off contact right away if you suspect a scam
- Don't wire money, send cash, or put money on a gift card for someone you have only an online relationship with
- Contact the AARP Fraud Watch Network Helpline at 1-877-908-3360 if you have questions or think you or a loved one has become a victim

AARP Fraud Watch Network