



# Fraud Protection

**Older adults in California have lost the most money in the nation due to scams.**

*Let's stop this trend* **and ruin the success of scammers together.**



# Helping keep you safe

Our mission at Patelco is unwavering – we deeply care about our members' financial health and wellbeing.

**We are inspired by the chance to make a difference in our members' lives.**

That includes helping keep our members finances safe from scammers.

More than 369,000 incidents of financial abuse targeting older adults are reported to authorities in the U.S. each year, causing an estimated \$4.8 billion in losses.\*

Fraud and scams are widely underreported, which is why you may not hear about it. Unfortunately, victims tend to feel lost, embarrassed, even shame at falling for something.

We're here to tell you, you are not alone.

We created this booklet to help you, our valued members, protect yourselves from savvy scammers who are using sophisticated methods to trap you into sharing your personal information or send money that is very tough to recover.

Visit our fraud center at [patelco.org/fraud](https://patelco.org/fraud) for additional details on the latest scams.

\*January 2022 analysis of federal and state data by Comparitech, a cybersecurity research company.



## Set up your *Trusted Contact*

Fraudsters are finding ever more sneaky ways to target people.

Part of keeping our members finances safe also includes the ability for our members to add a Trusted Contact to their account.

### **What is a Trusted Contact?**

**A Trusted Contact is a trusted friend or family member who can confirm:**

- your current contact information
- your health status
- the contact information for other authorized parties
- urgent, unusual account activity or other possible red flags

**To add a Trusted Contact, visit a local branch or make an appointment to meet online.**

**Visit [patelco.org/contactus](https://patelco.org/contactus) to get started.**

## Designate someone you trust as your financial *power of attorney*.

A California Financial Power of Attorney is a document that gives a third party the legal authority to make certain financial decisions on your behalf.



## Here are a few tips to consider:

- While you're still able to make financial decisions, choose the right person to do so if you become unable to care for yourself or your affairs
- Consider two people you trust so they can share the workload and responsibility
- Instead of completing a standard power of attorney form, consider customizing for your needs with a lawyer

The federal government's Eldercare Locator can help you find free or low-cost legal assistance at [eldercare.acl.gov](https://eldercare.acl.gov)

## Always stay vigilant when it comes to *scams*

Whether it's a person or a business you're dealing with over the phone, mail, email, in person, or on social media, **it's important to be on high alert.** If you didn't reach out to them first, it's likely a scam if someone is asking you to:

- Hide information or lie to Patelco or any financial institution
- Provide your login credentials to online banking or another account
- Wire them money out of the blue
- Do a transaction involving a foreign country, territory, or another state where you don't have contacts or connections
- Send "extra" money back after they overpaid or over reimbursed you
- Buy gift cards and send them the pin information



## Remember ALWAYS KYPIP (*Keep Your Personal Information Private*)



Patelco respects your privacy and security and will never ask you for:

- Your online banking User ID and Password
- One-time Passcodes for transactions, registrations, or logins
- Your card PIN, security code, or full card number



## What you can do to avoid a *scam*

- 1 Block unwanted calls and text messages.** Take steps to minimize the amount of spam calls and texts you receive by “blocking” and reporting it as junk.
- 2 Don’t give your personal or financial information in response to a request that you didn’t expect.** Legitimate organizations won’t call, email or text to ask for personal information, like your social security number, online banking passwords, account numbers or credit card numbers.
- 3 Resist the pressure to act immediately.** Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them personal information is likely a scammer.
- 4 Know how scammers tell you to pay.** Never pay someone who insists you pay with a gift card or by using a money transfer service. And never deposit a check and send money back to someone.
- 5 Stop and talk to someone you trust.** Before you do anything else, tell someone you trust what happened (a friend, neighbor, family member) or call Patelco directly. Talking about it could help you realize it’s a scam.

*Source: Federal Trade Commission*

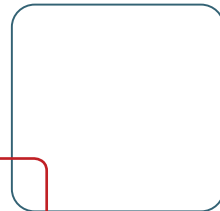
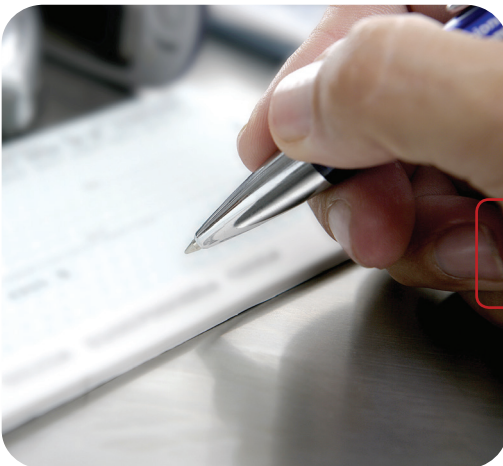
## Check washing *scams*

Thieves and organized crime rings are working overtime to snatch your mail in hopes of finding checks they can alter.

While the vast majority of mail sent through the U.S. Postal Service (USPS) – which handles some 129 billion pieces a year – arrives without incident, mail theft and mail carrier robberies are a growing problem around the U.S.

Thieves will then “wash” the stolen checks with a basic household chemical that can dissolve many kinds of ink. They then make it out to whomever they want, change the dollar amount and forge a signature. They may even put a superglue over the original signature of the check while washing it to keep it looking authentic.

They take their crime one step further and recruit people hurting financially to serve as “runners” and “finish the job”. The runners job is to deposit the forged check, then withdraw the money to give to the criminals, minus a cut for themselves.





## How to keep your mail *secure*

- Take your outgoing mail to a collection box as close to the indicated pick-up time as possible. Or drop off inside the post office for mailing.
- If you choose to leave outgoing mail in your mailbox, don't ever put your mail flag up
- Try not to leave incoming or outgoing mail sitting in your mailbox for an extended time, particularly overnight
- Sign up for Informed Delivery, a USPS free service at **usps.com**. With this service, you will receive an email with images of everything that will be delivered to your home that day, so you'll know what to expect (and what's missing when the carrier drops off your mail)
- If you are going to be out of town, have a neighbor collect your mail or use the USPS Hold Mail service
- Keep an eye on your bank accounts for potential fraud, and report suspicious activity as soon as possible

Source: AARP website

## Steps to take if you suspect mail *fraud*

- 1 **Report suspected mail losses to the USPS**, which uses such reports to identify problem areas and where to focus crime investigations, at **[usps.gov/report](https://usps.gov/report)**, or by calling **877-876-2455**. The agency is offering a \$10,000 reward for information and services leading to the arrest and conviction of persons responsible for “theft, possession, destruction or obstruction of mail”
- 2 **Notify your financial institution immediately** so they can take the proper steps to safeguard your account
- 3 **Report the theft** to your local law enforcement
- 4 **Put a fraud alert** on your credit reports

*Preview and track your mail with  
Informed Delivery by the USPS.  
Sign up for free at **[usps.com](https://usps.com)***

## Sweepstakes and lottery *scams*

You know that saying, “If it’s too good to be true, it probably is”? Well when you hear from someone out of the blue that you’ve won the lottery or a prize of some kind, it’s likely a scam.

## Here's how it works:

- Someone calls you claiming you won a prize or lottery. Scammers may impersonate well-known sweepstakes organizations (like Publishers Clearing House) to build trust
- If you want to claim your winnings, you must send money, cash, or gift cards up front – sometimes thousands of dollars' worth – to cover supposed taxes and processing fees
- Sometimes, fraudsters tell you to send even more money so your winnings will arrive sooner. Of course, no prize is ever delivered

## Grandparent *scams*

Scammers don't have empathy or much of a heart. They will stop at nothing to trick you. Even focusing on your most treasured asset – your grandchildren.

### Here's how this scam may work:

- Scammers call a would-be grandparent and say something along the lines of: "Hi, Grandma, do you know who this is?"
- When the unaware grandparent guesses the name of the grandchild the scammer most sounds like, the scammer is able to instantly secure trust
- The fake grandchild then asks for money to solve some urgent financial problem (such as overdue rent, car repairs, school payment)

- They will typically request the grandparent to pay them via gift cards or money transfer to make it hard to track.

In other versions of this scam, the caller claims to be an arresting police officer, doctor, or lawyer trying to help the grandchild.



## Your best protection is to *pause*

The scammer will prey on your emotions and may beg the grandparent not to tell anyone and use high pressure tactics. Trust your gut, and do not follow through on what's being requested. Immediately hang up and call your grandchild at the number YOU previously had. Do not use the number the fraudster gave you.

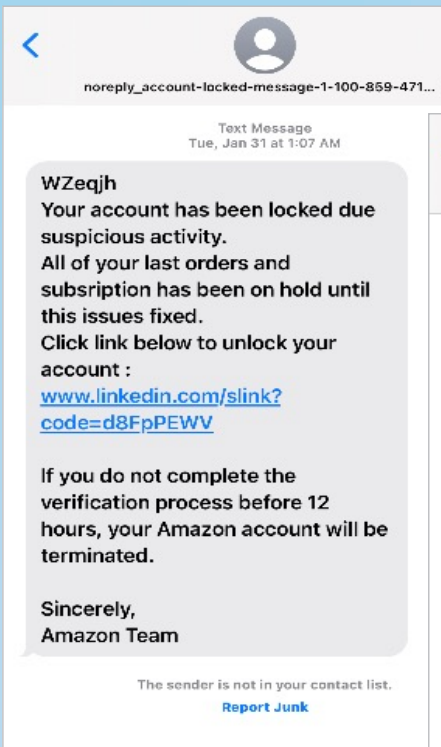




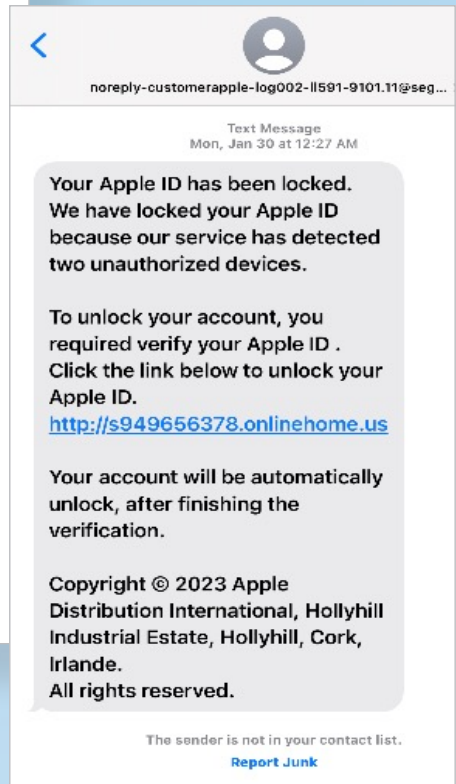
*Did you receive an email or text message from a company you do business with, and you think it's real? Can you tell these are **scams**?*

**When in doubt, always contact them using a website you know is trustworthy.**

## Scam text #1



## Scam text #2



**Make sure you "block and report as junk"**



## How to protect yourself from *texting scams*

The Federal Communications Commission (FCC) recommends the following to help you avoid texting scams:

- Do not respond to texts from unknown numbers, or any others that seem suspicious
- Never share your personal or financial information by text
- Do not tap or click on links in a text message – and if a friend sends you a link that seems out of character, call them to make sure they really sent it
- If you receive a text from a business, call them to verify that it's real – look up their number online rather than contacting a number provided in the text
- Report smishing to your wireless service provider by forwarding unwanted texts to 7726 (or "SPAM")



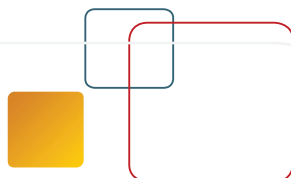
## Romance *scams*

If you're an older adult who's just ventured into online dating, it can be an exciting time. But it's important to act with caution when you are using online dating sites and apps as scammers are waiting to take advantage of your trusting, polite nature and financial stability.

The scammer creates a fake profile from which they message their target on dating apps or social media with sweet messages and big proclamations. They gain your trust and affection — and that's when the asks begin.

**Here are some signs the person you're talking to is actually a scammer:**

- “Love bomb” you: Love bombing is standard among sweetheart scammer tactics. It's when a person lavishes you with excessive flattery, affection, and praise early in the relationship in an effort to manipulate your emotions
- Ask you to move to another app or website to speak privately
- Claim to be a native English speaker, but their spelling, grammar, or accent tell you otherwise
- Say they live in your home country but they're traveling for work
- Have an online profile that doesn't match up with what they've told you, in terms of either photos or biographical details



## How to protect yourself from a *romance scam*

- 1 Take it slowly and ask a lot of questions. Watch for inconsistencies as that might reveal an impostor
- 2 Talk to family and friends about your new love interest and pay attention if they have concerns
- 3 Do a reverse image search of their profile photo using Google's image search. If the same picture shows up elsewhere with a different name attached to it, that's a sign a scammer may have stolen it.

Source: AARP website





## Government impersonation *scams*

The scammers pretend to be from IRS, FBI, U.S. Marshals, court officers and other officials asking for money or in some cases threatening people to get what they want. The fraudster may tell you that you're about to be arrested or punished for some infraction — and that you need to pay a fine or provide information such as your Social Security number.

They may demand payment through cash or gift cards or sometimes going as far as threatening to extort victims with physical or financial harm in order to get more information.

The FBI clearly states that no law enforcement official will ever do any of that.

### **Surprised to get that letter from Social Security?**

Scammers are sending fake letters and attaching the letter to an email or text that closely resemble official Social Security Administration (SSA) and SSA Office of the Inspector General (OIG) letterhead or that of other government agencies, such as the Federal Trade Commission. These scammers are trying to steal your money or personal information.



## How a government *scam* works

These scams primarily use telephone to contact you, but scammers may also use email, text message, social media, or U.S. mail. Scammers pretend to be from an agency or organization you know to gain your trust. Scammers say there is a problem or a prize. Scammers pressure you to act immediately. Scammers tell you to pay in a specific way.

### Tips to avoid being a government scam victim:

- 1 **Hang up the call or ignore the message.** Talk to someone you trust
- 2 **Keep your money and personal information safe.** Do not transfer money or buy gift cards
- 3 **Be skeptical and cautious** of unexpected calls and messages
- 4 **Do not click links** or attachments

Victims of government imposter scams reported losing nearly **\$509 million**.

*Source: Federal Trade Commission*



## Financial exploitation by a *family member*

Unfortunately, scams and fraud can occur at the hands of people we love. Family, friends and caregivers are not immune from skimming a little money here or there for their own purchases, using their care partner's assets irresponsibly, manipulating their estate plan or just brazenly stealing large sums and thinking no one will notice. More often than not, if the victim knows the exploiter, it is a family member.

Exploitation, in all its forms, happens far more than we know because victims and families do not report it. When you suspect you or a loved one has fallen prey to a scam or fraud, resist the urge to assign blame or judge the situation. Manipulators and criminals are good at what they do and often go unnoticed. If the red flags are waving, get organized, be proactive and move forward to help hold wrongdoers accountable.

If you have been the victim of family exploitation, visit the Department of Justice website for detailed guidance at [justice.gov/elderjustice/roadmap](https://www.justice.gov/elderjustice/roadmap)

If you or someone you know is 60 or older and has been a victim of financial fraud, report the incident to the DOJ's **National Elder Fraud Hotline** at **833-FRAUD-11 (833-372-8311)**. Personalized support is available seven days a week from 6:00 a.m. to 11:00 p.m. ET.

## Computer tech support *scams*

With the advancement in technology, scammers take advantage of people who may not be as knowledgeable about computers and cybersecurity.

### Here's how this scam works:

- 1 A pop-up message or blank screen appears on your computer or phone, telling you that there is something wrong with your device
- 2 They provide a customer support number for you to call
- 3 When you call the support number for help, the scammer may either request remote access to your computer and/or demand you pay a fee to have it repaired
- 4 Once you grant remote access, you have now turned over the keys "digitally" to critical identify and financial information, including your bank accounts

*Source: National Council on Aging*



## Action and report the *scam*

Anyone can be a victim of a scam. Taking action and reporting the crime can help put an end to scams and bring criminals to justice.

- Federal Trade Commission (online at [consumer.ftc.gov/scams](https://consumer.ftc.gov/scams) or call 877-382-4357)
- FBI's Internet Crime Complaint Center at [ic3.gov](https://ic3.gov), if the scam occurred online
- BBB Scam Tracker at [bbb.org/scamtracker](https://bbb.org/scamtracker)
- In California, contact your local county **Adult Protective Services office** or call 833.401.0832
- Report Social Security scams at [oig.ssa.gov](https://oig.ssa.gov)



## Being cyber safe

Internet fraud is on the rise. Many of these scams use spoofing, which is when fraudsters pretend to be a legitimate organization or company.

Patelco's website domain and email addresses always end with .org (for example, **karina.johansen@patelco.org** or **twalnut@patelco.org**). You'll never receive a legitimate email from a patelco.net email address or another incorrect domain.

### Keep your devices and software up to date

Outdated electronics can give attackers access to your device through security weaknesses, making you more susceptible to ransomware attacks and viruses. Updates from Apple, Microsoft, Google, and the like do more than just add features. They also provide security updates to keep your data safe.

### To ensure you have the latest security features:

- 1 Turn on automatic system updates for your devices, including your computer, tablet and phone
- 2 Turn on automatic updates for software and apps
- 3 Periodically check your devices and software for updates. If you don't have the latest version, update





## **Use strong passwords**

Passwords are the most common form of account authentication, but they must be complex and confidential to keep your information private.

### **Here are a few tips to come up with strong passwords and keep them secure:**

- Use different passwords on different systems and accounts
- Create the longest password or passphrase — a random combination of words, numbers, and symbols — allowed
- Don't use passwords based on personal information that can be easily accessed or guessed
- Change passwords for important accounts (banks, credit cards, etc.) every three months

## **Enable multi-factor authentication**

For the accounts you use the most, check the security settings for the option to enable multi-factor authentication (MFA) or two-factor authentication (2FA). When you use MFA or 2FA, you'll need to provide at least two pieces of evidence to prove your identity for access to your account.

MFA helps increase online security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement, blocking them from accessing your information.

## **Deep clean your social media**

Social media is full of information about you. Purge your accounts of any personal information you wouldn't want a stranger or thief to have — anything from your home address, employer details or email addresses to photos of vacations and birthdays.



## Did someone claiming to be from *Patelco* call or text you?

With the increase in spoofed caller ID, it's possible that fraudsters appear to be calling you from a Patelco phone number. But if they call you and ask for any of the 5 pieces of information below, you can be sure it's a fraudster. When in doubt, hang up, and call us.

### **5 things we'll never call (or text) and ask**

While we may contact you regarding an account issue or to ask if you made a particular card transaction, we will never contact you out of the blue via phone, email or text and ask for any of these 5 things — ever.

- 1 your card PIN
- 2 your online banking password
- 3 the CVV (3 digits) on the back of your card
- 4 your full account (MICR) number
- 5 personal information, like how long you've been a Patelco member

### **Calls to you vs. calls to us**

Remember that you can always make a call to us at **800.358.8228** and know that you are talking to the right person.

**When you call us (or card security), we might ask you some verifying questions including the information above — but we will never call you and ask for that information!**

*When in doubt, hang up, and call us.*

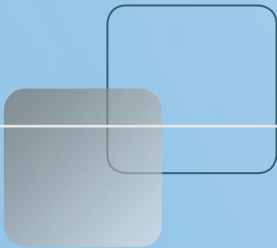
## Reporting fraud to *Patelco*

### **If you suspect your Patelco account has been compromised**

Please contact us as soon as possible if you see suspicious activity on your account. We can review your accounts, place protection on them, and try to recover lost funds.

### **To dispute a debit or credit card transaction**

The easiest and fastest way to submit a card dispute is in **Patelco Online™** or the **Patelco Mobile App**. After you log in, tap or click the account with the transaction, tap or click to select the transaction, and then select Dispute. For answers to common dispute questions, please visit [patelco.org/disputes](https://patelco.org/disputes)



## Patelco's dedicated *fraud-fighting* team

Now available to answer your questions before you send money or share information.

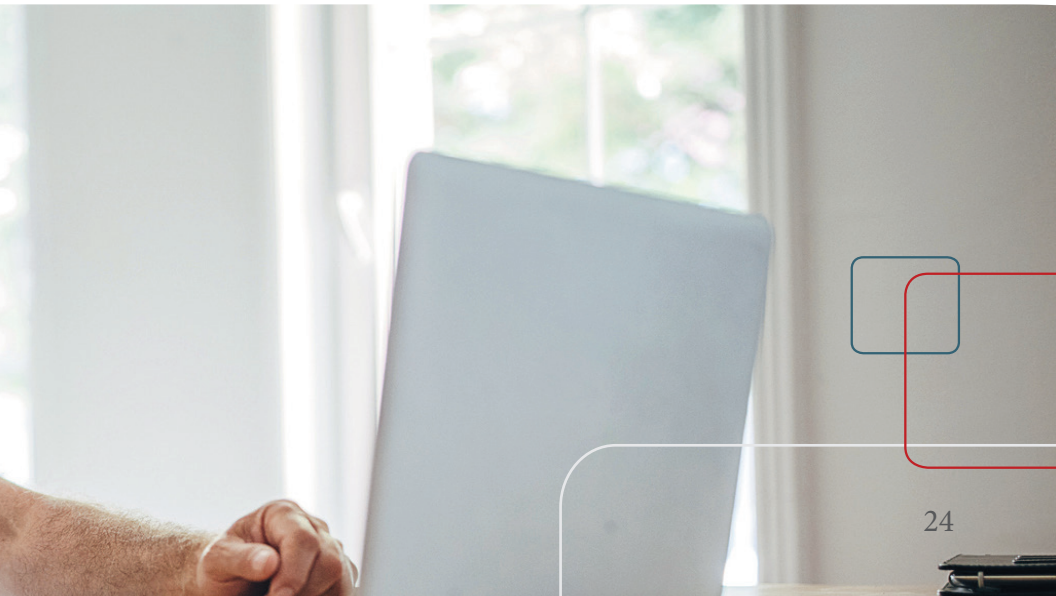
### **Save this number in your contacts (maybe even in your favorites list!)**


Next time you get a call, email or text that seems suspicious and asks you for money or information – call us first at **800.358.8228** and enter extension **5323** when prompted.

Our fraud fighting team is available weekdays 8am to 6:30pm and Saturdays 9am to 2pm.

### **Don't fall for high pressure scam tactics – talk to us before you respond**

Fraudsters prey on your emotions and use sophisticated methods to trap you into sharing your personal information or send money that is very tough to recover. Don't do it – talk to us first, and we'll help you figure out if it's a scam. Visit [patelco.org/contactus](https://patelco.org/contactus) for all the different ways to reach us.



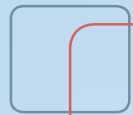


**We're here to tell you - *you're not alone***

Scams are designed to catch you off guard. There's nothing to be ashamed of if you're the victim of a scam. Rest assured that Patelco is here to support you. Together we're in this fight against fraud.

Please visit our Fraud Center regularly for more information on the latest scams, how to avoid being the victim of a scam, and other fraud-related resources and support.

Learn more at **[patelco.org/fraud](https://patelco.org/fraud)**





## *Get connected*

There's support and help available in your community.

Learn more at [patelco.org/resources](https://patelco.org/resources)





## Elder abuse is a *billion-dollar industry*

Experts estimate more than 369,000 incidents are reported of financial abuse targeted to older adults each year. We find that unacceptable and extremely concerning.

Patelco is deeply committed to helping turn that around and feel strongly that educating our members is the greatest prevention.

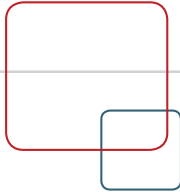
We hope you keep this booklet handy, and that it's helped inform you of best ways to keep your money safe from savvy scammers.

Since 1936, Patelco has proudly served over 450,000 members and communities. Through economic highs and lows, good times and bad times, we are committed to your financial wellbeing, and to helping you thrive and live your best financial life.

*We greatly value your membership and trust.*

[patelco.org](https://www.patelco.org)

Source: *National Council on Aging*



Insured by NCUA