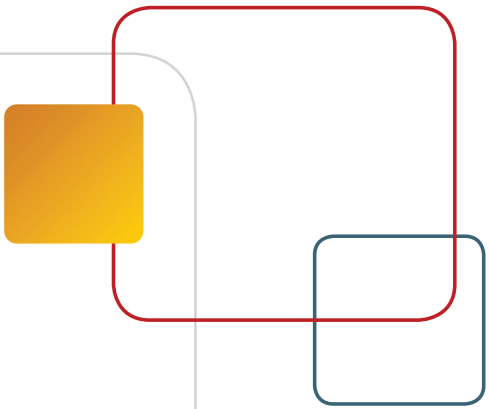
Patelco CREDIT UNION

Fraud Protection

1 in 10 adults will fall victim to a scammer or fraudster this year.*

Let's ruin their success together.



*Source: LegalJobs

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.

But there's one main critical issue that will get in the way of that, and that is fraudsters. And more and more of our Patelco members are falling victim to scams.

Chances are you or someone you know has already been scammed or been the victim of fraud. 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. Patelco is here to support you – offer educational information, guidance if you've been the victim of a fraud or a scam, and provide a caring, non-judgmental ear.

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.

We hope this information reinforces what you may already know, teaches you valuable information, and gives you tools to help start conversations with people you care about.

Visit our fraud center at patelco.org/fraud for additional details on the latest scams.

Protecting yourself from *fraud*

Take the steps to help prevent fraud by being hypervigilant and always following best practices.

Avoid being a *victim*. Common *red flags*

Fraudsters are finding ever more sneaky ways to target people.

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

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. Especially if you didn't reach out to them first, be on alert if you encounter any of the following:

- An unusual payment request
- A request for your personal information
- Requests to cash checks for someone or transfer money for them
- A request for money from someone you've never met
- Something that looks too good to be true
- An unusual or out-of-character message from friends or family
- A request to communicate outside the platform or channel where you made contact

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 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

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

Fake debt collector *scams*

In this scam, fraudsters threaten legal action to pressure you to pay a fake debt. In late 2022, the Federal Trade Commission (FTC) returned more than $1 million to victims of scams.

To protect yourself from similar scams:

- **Understand your finances.** Keep records of past and current debts, so you won't get fooled by a fake debt
- **Request a "debt validation letter."** This requires the debt collection agency to prove they're legally collecting a debt you owe
- **Regularly review your credit report** so you stay aware of the status of all your accounts
- **Know your rights**, including those covered under the **Fair Debt Collection Practices Act**

Digital payment scams (like *Zelle, Venmo*)

- **Never send digital payments to people you don't know or trust**
- **Never share your online banking User ID or password.** Patelco will NEVER contact you and ask for it — and there's no reason anyone else needs it, ever.
- **Never do a "test" transfer with any third-party payment service.** Don't fall for someone pretending to be from Patelco asking you to do a "test" transaction or transfer. Patelco will NEVER ask you to do a test transfer, ever.
- **Never use digital payment to make utility bill or credit card payments.** A scammer may pretend to be a utility company or wireless carrier asking you to send a payment with a digital platform. Most digital payment platforms cannot currently be used to pay utility or credit card bills.
- **Do not send money back to someone who "accidentally" sent you money via digital payment.** Scammers will send money from stolen accounts and then ask the recipient to send the money back — but the money sent back is your real money, while the money that you "accidentally" received is stolen.

  If someone reaches out to you and says that they sent you money accidentally, tell them to reach out to their bank or credit union to resolve it. Never send the money back to them.

Text message *Scams* (also known as smishing)

- Smishing often looks legitimate and tends to prey on fear or excitement to encourage you to act
- You may be offered free prizes, gift cards or coupons
- Some smishing scams even promise to help pay off debt like student loans
- Other smishing messages might say there's suspicious activity on your account, contain a fake package delivery notification, or falsely claim there is a problem with your payment information

More signs that a text is a *scam*:

- It asks you to tap or **click a link** to verify your personal information
- It asks you to **provide your personal information** by calling or texting a phone number
- It comes **from an unknown or unfamiliar number**
- The sender **claims to be a government agency** such as the Internal Revenue Service (the government rarely, if ever, initiates contact by phone or text)

Fake messages from *scammers*

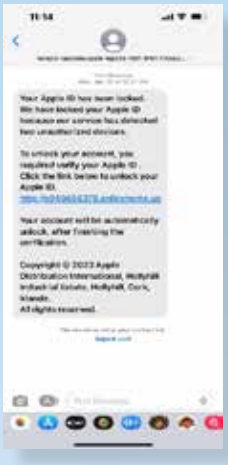
- Say they've noticed some suspicious activity on your account
- Claim there's a problem with your payment information
- Send you a fake invoice and tell you to contact them if you didn't authorize the purchase
- Send you a fake package delivery notification

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



Scam text #3

Make sure you "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*

Have you ever seen the MTV show Catfish? Well, romance scammers work in a similar way to catfishes. 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. They'll ask for money to come see you, for unexpected expenses, or for a family emergency. In return, all you'll receive is a lower account balance.

Don't fall head over heels for love, follow our tips on how to handle romance scammers:

- If you suspect you're talking to a scammer, stop communication immediately
- If you haven't met in person, don't send money or gifts
- Do a reverse image search of their profile image using a search engine – this may help show you if you're communicating with someone who has stolen another person's photo
- Don't send images of yourself in your birthday suit – these are often sought by scammers for blackmail
- Talk to trusted friends or family about your new love interest and see if they have any concerns

It's a great time to revisit our YouTube video on romance scams at **youtube.com/Patelcocu**

Money wiring *scams*

Scammers are always looking for new twists on an old scam – and one of their favorite payment methods is wire transfers. Why wire transfers? They allow fraudsters to move money out of your reach quickly and are hard to trace.

Before sending a wire transfer, ask yourself these questions:

1. Did you receive a call claiming to be from the government or a well-known company (e.g., Walmart, PG&E, Amazon) advising that you owe them money?

If yes, you've been targeted. Government organizations will send you official paper mail — not phone calls, texts or emails — for money owed.

2. Have you received an unexpected call from someone who claims to be a friend or relative that needs cash for an emergency?

Family emergency scams are on the rise. Fraudsters will claim they need your help to get out of jail, pay a hospital bill, or leave a foreign country. Do not send the money — and don't hide information about the nature of the wire transfer if your bank or credit union asks.

3. Is the person asking for a wire transfer to someone you've met only on social media, an online forum or a dating website?

If yes, you're the target of a romance scam. This con game uses fake profiles on social media, dating sites, online forums, and apps. After earning your trust, they create stories to appeal to your emotions with the goal of separating you from your money. They may interact with you romantically, offer you a job or business opportunity, or pretend they'll invest your money.

4. Were you sent a check (or another type of payment) and instructed to deposit it and then wire the money back to the sender or another person?

If someone you don't know sends you a check (or other type of payment) and asks you to wire it back to them, you're dealing with a fraudster. Don't cash the check or accept the payment, and don't wire money back.

Pet *Scams*

Better Business Bureau (BBB) advises extreme caution when shopping for a pet online, especially in light of scammers' evolving tactics.

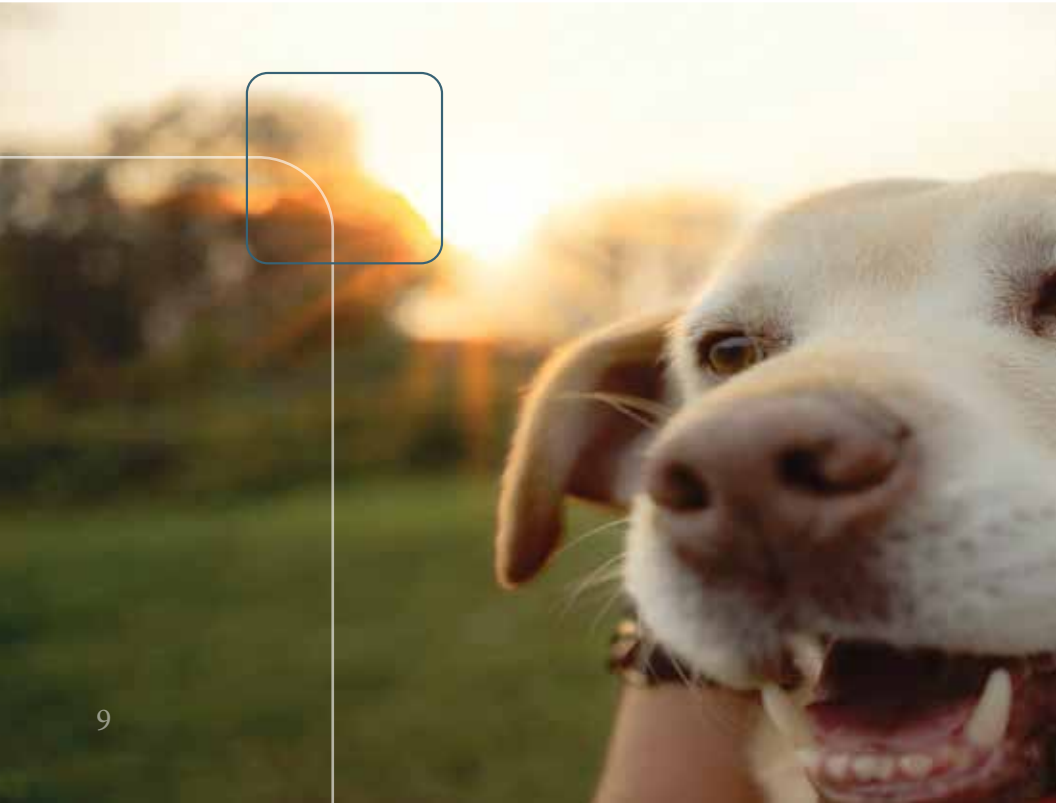
Here's what scammers do:

- Scam criminals use social media and other free websites to advertise pets that do not exist. Expensive animals, like bulldogs or toy breeds, are offered at very low prices
- They steal and post pictures of animals that are often stolen from real sites
- The fraudsters don't make arrangements for an in-person meeting with a potential buyer and often ask victims to send money to a third party who will take over responsibility for transporting the animal
- The thieves will develop bogus websites that appear to be legitimate transport companies and even illegally use logos from other companies
- Once they've hooked you, the requests for money on one pretext or another will continue as long as you continue to send money
- The scammer's requests for money look something like this:
  - ☐ need victim to buy or rent a special crate for the pet
  - ☐ animal needs special insurance or shots
  - ☐ pet is stuck at an airport in transit and additional money is needed for food and water
  - ☐ threatens the potential buyer with criminal charges for "animal abandonment" unless more money is forthcoming

These scammers are criminals. They're preying on your emotions. Their goal is to take your money.

Here's what to do to protect yourself from a *pet scam*:

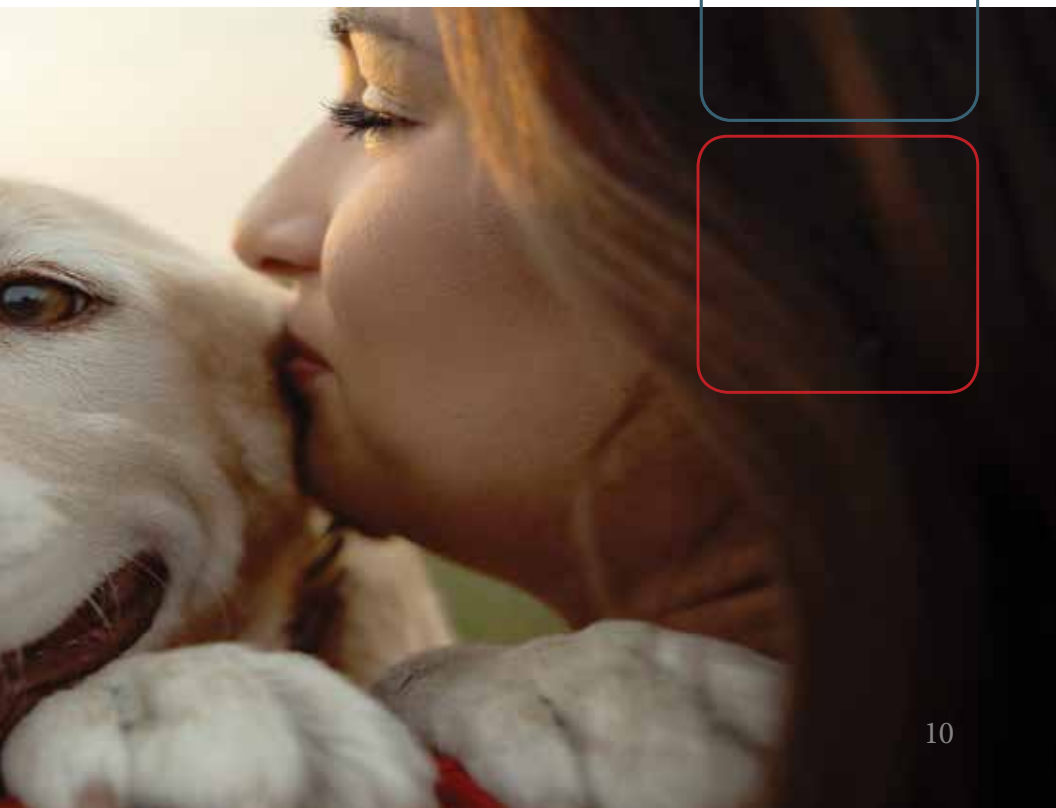
- If you see an offer that is too good to be true, it probably is
- Don't buy or adopt a pet unless you can meet the pet in person
- Don't deal with someone who won't take payment by credit card, which offers you far greater protection in case of fraud or dispute
- Use friends and family for pet breeder referrals
- Do consider adopting from a local shelter or rescue group, instead of buying a pet online. **Check out a local animal shelter online** for pets you can meet before adopting



Take 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** or call 877-382-4357)
- FBI's Internet Crime Complaint Center at **ic3.gov**, if the scam occurred online
- BBB Scam Tracker at **bbb.org/scamtracker**
- **PetScams.com**, an online watchdog that catalogs and reports on pet-related fraud



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 **patelco.org/locations**). 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.

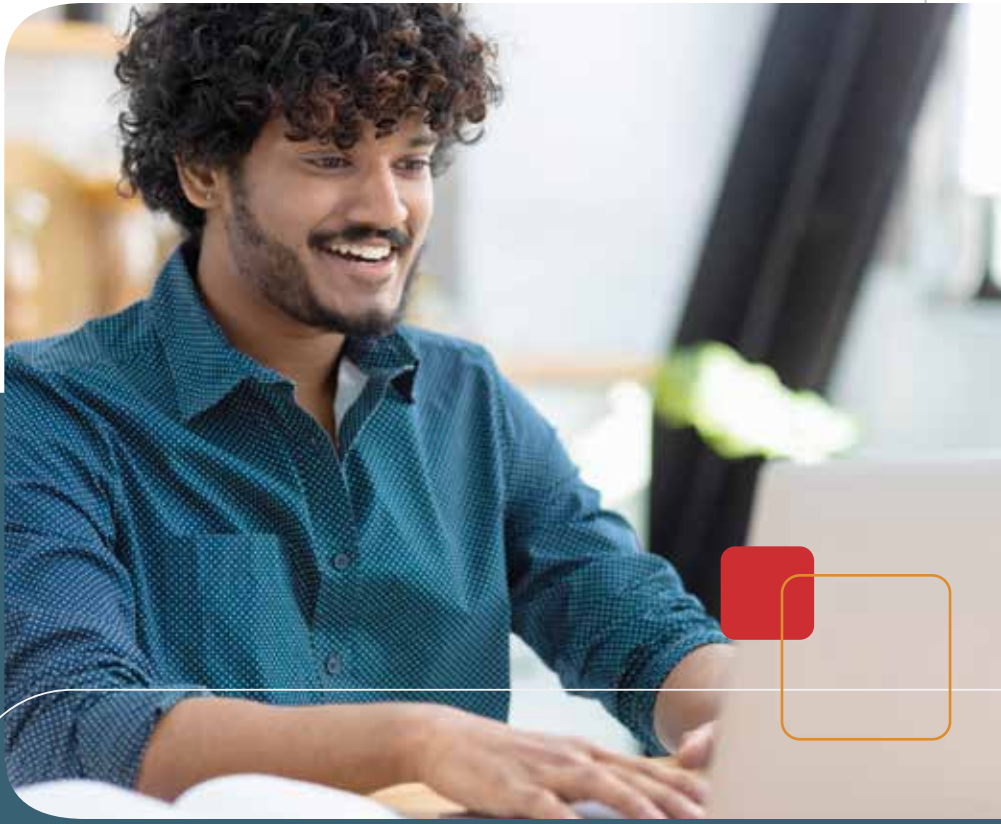
To ensure you have the latest security features:

- Turn on automatic system updates for your devices, including your computer, tablet and phone
- Turn on automatic updates for software and apps
- 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.

Don't let fraudsters pressure you
Fraudsters know we're more likely to give up sensitive information if we feel threatened, pressured, or afraid. Beware of any threats to "immediately" close your account or block your card if you don't provide certain 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. Visit **patelco.org/contactus** to chat live, meet on zoom or make an appointment at your nearest branch.

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**

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 play 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.

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. Patelco is here to support you – offer educational information, guide you if you've been the victim of a fraud or a scam, and provide a caring, non-judgmental ear.

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.

patelco.org/fraud

Patelco CREDIT UNION

EQUAL HOUSING OPPORTUNITY

Insured by NCUA