

Fraud Alert Notices and Updates



*Bottom line–
Don't get hooked
by fraudulent
phishing attempts!*

FRAUD ALERT via Text Message

Beware that a text message was received by some members stating to contact their credit union, with the option to text message back the originator. The credit union never sends any such messages and you should not respond in order to protect your accounts. These are fraudulent attempts to obtain your confidential information. If you receive suspicious text messages claiming to be from PTFCU, do not reply by text. Contact us immediately at 866-773-9835, option "0," (outside US 424-233-3091) to report the suspicious activity and ensure that your accounts are in order.

[Click Here](#) to learn more on how to Protect Yourself from Identity Theft.

Credit Union National Association (CUNA) and your financial institution are aware of phone calls, text messages, and emails being made about:

- **Account De-activation**
- **Account Status Alert**
- **Changes to Terms and Conditions**
- **Irregular Activity**

These e-mails and text messages ask that the member call a number in order to have their account reactivated. Some may request that you leave callback information or provide your financial information directly. **All of these messages are fraudulent.** Please do not respond to these messages.

The Credit Union National Association is the trade association for credit unions in the US. CUNA does not maintain any type of customer/member financial information. Additionally, Pacific Transportation FCU would never solicit your personal identification information via email. If you did respond to such a solicitation, you should contact PTFCU directly at **866-773-9835, option 0.**

SMShing Scam Alert Via Text Message

There is a fraudulent text message scam circulating that tells you that your credit card has been deactivated. It then instructs you to go to **www.fcu-activate.org** to get your card activated. Once you access that website, it asks for your Financial Institution's name, card number, expiration date, PIN # and the 3 digit value number located on the signature panel on the back of the card.

There is also another fraudulent text message scam different from the one listed above that tells you to call a toll free number to re-activate your card.

These are both attempts to fraudulently obtain confidential information. Your legitimate card issuer would not send you a text message to get that information. Do not respond to any such text messages and immediately notify PTFCU and your other credit card issuers if you do receive such messages. Contact them at a phone number you know to be legitimate. We may be reached at 866-773-9835, option 0.

Pacific Transportation FCU will **NEVER** contact you via e-mail or phone asking for confidential or sensitive information. We will never ask you for your Account Number, PIN, Social Security Number, Credit Card Number, Name, Address or Birthday via e-mail or phone. If someone is requesting such from you, it is not PTFCU and should be considered fraudulent.

Review your monthly account statements and credit card statements and report any irregularities immediately.

If you have received a suspicious e-mail or other fraudulent correspondence regarding Pacific Transportation Federal Credit Union, please forward it to **administrator@ptfcu.org**.

Take Some Simple Precautions

- Never respond to an unsolicited e-mail that asks for detailed financial information. Know whom you are dealing with.
- Report anything suspicious to the proper authorities. Alert the company or government agency identified in the suspect e-mail through a Web address or telephone number that you know is legitimate.
- You can also contact the Internet Crime Complaint Center at www.ifccfbi.gov—a partnership between the FBI and the National White Collar Crime Center—if you think you have received a phishing e-mail or have been directed to a “phishy-looking” website.

Stop, Look and Call

The Department of Justice advises e-mail users to “stop, look and call” if they receive a suspicious email.

Stop – Resist the urge to immediately respond to a suspicious e-mail—and to provide the information requested—despite urgent or exaggerated claims.

Look – Read the text of the e-mail several times and ask yourself why the information requested would really be needed.

Call – Telephone the organization identified, using a number that you know to be legitimate.

If You've Been Phished!

If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:

- Immediately contact PTFCU or your financial institution
- Contact the three major credit bureaus and request that a fraud alert be placed on your credit report for your accounts and obtain copies of your credit report. The credit bureaus and phone numbers are:

Equifax – 800-525-6285

Experian – 888-397-3742

TransUnion – 800-680-7289

[FREE Annual Credit Report](#) - Toll Free 877-322-8228

- **Always report suspicious activity** If you receive an email you suspect isn't genuine, forward it to the spoofed organization's dedicated email address for reporting such abuse. Below click on any of these websites to submit suspicious activity.

[Federal Trade Commission](#)
[Internet Crime Complaint Center](#)
[Anti-Phishing Workgroup](#)

File a complaint with the Federal Trade Commission at www.ftc.gov or **877-382-4357**. You should also visit the Federal Trade Commission's (FTC) identity theft website at **www.consumer.gov/idtheft** or call **1-877-IDTHEFT** to file a complaint and learn more about how to minimize your risk of damage from identity theft. If you notice any irregular activity on your credit report, contact your local law enforcement agency as well.

Phishing Scam Via Telephone

This fraudulent attempt to capture card numbers is done with an automated telephone service. The system indicates that the members' debit cards have been placed on a hold status, and that in order to activate the cards, the message then asks the member to call a toll free 866 - number and enter their 16-digit card number. There are so many ways for perpetrators to attempt to get personal information, including the use of auto-dialers. It is important to remember to limit the release of personal information in order to protect yourselves from fraud. Please contact PTFCU Member Services at 866-773-9835 if you've received a phone call asking for card-holder information immediately.

What is Phishing?

Everywhere you look articles and newsflashes abound about "phishing." What is it and how can you guard against this type of scam?

The definition of phishing is a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly. These scams often request credit card numbers as well as other sensitive information. Be aware of email containing imbedded links for you to access to update your information.

- Don't open email from an unknown source/sender
- Don't input or reveal personal or confidential information via email
- Personal information such as passwords and credit card, social security, and bank account numbers. A legitimate organization already has this information
- Be selective when giving out your email address

PTFCU will never send you an email requesting your account number or credit card number. If you have a concern about an email received from us please contact Member Services at **866-773-9835, option 0** or email us at **administrator@ptfcu.org**.

To contact us:

PACIFIC TRANSPORTATION
FEDERAL CREDIT UNION
501 W. 190th Street
Gardena, CA 90248

Member Services: **866-773-9835, Option 0**
Monday-Friday, 7 a.m. to 5 p.m.
E-mail: administrator@ptfcu.org

