Financial Safety

Protection so you can focus on what matters most

TRAVIS CREDIT UNION

Protect yourself against threats – in person and online

Keeping you informed about identity theft, online scams, ATM skimmers and other types of frauds and scams is just another way we help protect your financial future. All TCU checking account holders receive free I.D. Theft Assistance, and we offer workshops on how to spot identity theft. Our Web site is updated regularly with the latest scam information.

Identity Theft

Identity theft is a crime of impersonation to obtain your name, Social Security number, drivers license, account number and other sensitive information to commit fraud. This negatively impacts your finances and credit report.

We protect your privacy

We highly regard the privacy and safety of your financial records and personal information. We adhere to a stringent policy regarding your confidential information and use the highest standards of encryption technology to secure your data. Visit *www.traviscu.org* to read the latest financial fraud alerts and scams. Our member service center can help you determine the authenticity of unsolicited telephone calls, emails and other forms of contact.

Minimize your risk

Never give out personal information over the phone, online or through the mail unless you initiate the contact or know the representative.

Protect your financial records. Store your documents in a secure location such as your home safe or lock box. Always shred credit card receipts, billing statements and pre-approved credit offers to protect personal information.

Keep your financial records current. Review your statements monthly to check for fraudulent or questionable charges. Order a free credit report each year from all three major credit reporting bureaus by visiting *www.annualcreditreport.com*. Correct any wrong or outdated report information.

Use your computer and mobile device wisely. Protect yourself from "phishing" scams by not responding to unsolicited email or text messages. Fraudulent e-messages often appear to be from reputable entities, luring you to reveal personal information by linking to a phony site. If you have questions about specific e-messages from Travis Credit Union, please call **(707) 449-4000 or (800) 877-8328**. We will never send you messages instructing you to update personal information.

Before you dispose of your personal computer, delete personal information from the hard drive using a "wipe" utility program. Consult a PC repair service for assistance, if needed.

When your identity is stolen

File a police report. Police documentation is vital to clearing your name and reestablishing your credit.

Notify the fraud department at one of the three major credit bureaus and request a fraud alert be placed on your file. You may also place a "freeze" on your account to prevent new credit from being established without your permission.

Contact all of your creditors to alert them of the theft of your personal information.

Close compromised accounts and open new ones, with mandatory passwords for initiating transactions.

Enroll in an identity theft protection program. Many programs provide ongoing credit monitoring with personal assistance, education and strategies to protect you in the future. We offer members an I.D. Theft Assistance service, which is free with TCU checking.

Fraud and Scams

Beware that when something sounds too good to be true, it is. Unfortunately, familiar scams are reinvented as technology advances. Below are some of the most-used schemes to watch for:

Lottery and sweepstake schemes

Countless scams involve foreign lottery or sweepstake winnings from foreign countries. It is illegal for U.S. citizens to participate in foreign lotteries. Although prize notices are tempting, remember that foreign lotteries or sweepstakes are not legitimate and simply rob you of money. Here are some warning signs:

- You should never have to pay money to receive an award.
- Legitimate awards do not require payment of tax, insurance or attorney fees prior to distribution of funds.
- Scammers may send a fraudulent check to offset the alleged required fees and ask you to wire back the excess funds. Because the check is fake, you'll suffer the financial loss if this fake check is negotiated.
- Most scammers have ties to major crime syndicates, some involving terrorism.

Phishing schemes

Phishers impersonate reputable organizations to trick victims into releasing personal information by phone or through e-mail or text messages. We will never send e-messages instructing you to update personal information. Notice the following warning signs:

- An e-mail describes a serious problem with your billing or other account information and asks you to click on a link to update your data. This takes you to a fake site that looks authentic.

- After connecting to the fake site, you'll be asked to update personal and account information that should already be on file with your legitimate financial institution. Any information you enter will be used for identity theft.

Overpayment schemes

Scammers often use online ads to locate a victim. The scammer expresses a high interest in the ad and overpays the seller via a counterfeit check or a money order. The scammer instructs the seller to wire the excess funds to another party for shipping, insurance or to repay a debt. Overpayment always suggests a scam is taking place.

Counterfeit or stolen check schemes

Scammers often prey on trusting people, convincing them to cash checks in a branch or through an ATM. The scammer claims to need assistance for lack of a bank account and/or an ID for the transaction. The scammer offers to pay a portion for the help. Since the check is fraudulent, the victim takes a loss on the amount "cashed".

Scammers may also send counterfeit checks as part of a "secret shopper" ploy to allegedly test the efficiency of electronic money grams. Victims are instructed to wire the majority of the funds, and then take a loss on any amount used.

Contact us immediately if fraud occurs. There is no shame in being victimized; contact your financial institution for guidance and place fraud alerts on your credit file as soon as you realize the situation. Report suspicious e-mails or calls to the Federal Trade Commission at *www.ftc.gov/idtheft* or by calling **(877) 438-4338.**

I.D. Theft Assistance

Protecting your private information is our priority, and we want to help you if fraud occurs. All of our checking account holders automatically receive free I.D. Theft Assistance. This service includes access to a caseworker who will provide you with a personalized Fraud Resolution Kit and walk you through the resolution process. For assistance, call **(800) 251-2311**, Monday through Friday, 7:00 a.m. to 8:00 p.m. (CT).

Visit ***www.traviscu.org*** to read the latest info on financial fraud alerts and scams.

Mailing & Shipping

Mailing Address
Travis Credit Union
P.O Box 2069
Vacaville, CA 95696

Deposits & Loan Payments Only
Travis Credit Union
P.O Box 8000
Travis AFB, CA 94535

Shipping & Overnight Mail
Travis Credit Union
One Travis Way
Vacaville, CA 95696

Account Access & Information

Web Site Address
www.traviscu.org

Call-24 Phone Banking
(707) 449-4700 or (800) 578-3282

Member Service Center

Account Assistance and Information:
(707) 449-4000 or (800) 877-8328

PhoneLoan™
(707) 451-5350 or (800) 449-4110

Home Loan Center
One Travis Way, Vacaville, CA 95687
(707) 469-2000 or (888) 698-0000

Check Fraud Information
(707) 469-4384 or
(800) 877-8328, ext. 4384#

Debit/Credit Card Fraud Information
(707) 449-4000 or (800) 877-8328

Everyone who lives, works, worships or attends school in Alameda, Colusa, Contra Costa, Merced, Napa, Placer, Sacramento, San Joaquin, Sonoma, Solano, Stanislaus or Yolo County is eligible to join. Certain membership eligibility requirements may apply.

Federally insured by NCUA.

TCU-744 (06/16)