

## **TDECU DEBIT & CREDIT CARD FRAUD FAQs**

**The following FAQs provide information regarding the recent rise in credit and debit card fraud activity in our communities. TDECU is strongly committed to its Members and offers tools and best practices to prevent fraud from happening.**

### **Has TDECU experienced a card data security breach?**

TDECU has not experienced a breach to our card data, and our security systems, which are in place to protect our Members' card information, have not been compromised. Fraudulent activity has been attributed to card compromises at merchants and merchant processors.

While the fraudulent activity is not a result of a breach at TDECU, protecting the assets of our Members remains our highest priority. We take these situations very seriously, and have a dedicated internal fraud team that uses world-class tools and systems to detect and prevent fraud, regardless of the source. Our monitoring of both debit card and credit card activity is completed in real-time and is conducted around the clock – every day of the year. In addition, our teams are working closely with our debit and credit card processors to ensure your hard-earned money is returned to your account(s) as quickly as possible.

### **If there was no breach of TDECU card data and security systems, how did this fraud occur?**

Card fraud is on the rise at merchants, ATMs and gas pumps nationwide and happens when a merchant or merchant's processor is impacted by a card compromise. When a card compromise event occurs, it happens at point-of-sale and merchant systems, not at TDECU.

The recent spike in fraudulent activity is not unique to any one credit union or bank, and is taking place across the U.S. The spike is attributed to last minute attempts by criminals who know the more secure EMV chip-enabled technology rollout is nearing completion, and will make it more difficult for them to commit card fraud.

### **Where are cards being compromised?**

Cards are compromised at merchants. Visa and MasterCard will not disclose to financial institutions where the fraud occurs, relying on merchant(s) to release information to the public when a compromise occurs. As good measure, we recommend that Members not only contact TDECU Member Care when fraudulent activity is suspected, but also reach out directly to any stores or businesses where the Member believes unauthorized purchases were made.

### **Is TDECU re-issuing debit cards because of a breach?**

No, TDECU is not re-issuing debit cards because of a breach. TDECU has not experienced a breach to our card data. TDECU will continue to employ the highest levels of fraud prevention monitoring tools available to ensure the integrity of our Members' accounts.

One of our latest fraud prevention monitoring tools is the EMV chip-enabled debit card. TDECU started issuing EMV chip-enabled debit cards to all active debit card holders on March 1, 2017, and will continue through November 2017 in waves based on expiration dates.

A chip-enabled debit card features EMV technology, which is an embedded microchip that provides an extra layer of protection against fraud. EMV – which stands for Europay, Mastercard® and Visa® – is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. When a chip-enabled card is used for payment, the chip and payment terminal work together to create a unique transaction code that cannot be used again. If someone were able to gain access to that and attempted to use the unique code for a subsequent purchase, the transaction would be denied.

### **How does TDECU protect its Members from fraud?**

TDECU has a dedicated internal fraud team (Security and Investigations Department) that uses world-class tools and systems to detect and prevent fraud. Our monitoring of both debit card and credit card activity is completed in real-time and is conducted around the clock – every day of the year.

To help protect against card fraud, TDECU issues EMV chip cards, the global standard in security, and our Security and Investigations Department works closely with Visa, Inc., our debit card issuer, to research and identify card fraud.

In addition, TDECU's debit and credit card processors utilize Falcon Fraud Prevention Service software to help identify and reduce fraud risk by detecting potentially fraudulent PIN-based and signature-based debit and credit transactions.

Falcon Fraud Prevention Service monitors Member's normal transaction behavior and scores transactions for potential fraud based on a variety of factors. The system then automatically contacts the Member to confirm or deny fraud via multiple contact methods.

In order to provide the highest level of protection, it is very important your mobile phone number and email address be accurate and updated in our system.

Members should also save the Falcon Fraud Prevention Service phone number in their phones:

**For debit cards: 866.236.7970**

**For credit cards: 800.238.8604**

## What should a Member do if they suspect fraudulent activity on their account?

We take protecting our Members' finances seriously. If a TDECU debit or credit card has been lost or stolen, or an account has been compromised, it is important for the Member to take the following steps:

### Compromised Debit Card:

1. Immediately report the fraud to TDECU.
2. Complete a [Debit Card Fraud Affidavit form](#).
3. Upon completion and submission of the form, the Member will receive a copy of the electronically signed debit card fraud affidavit via email.
4. A TDECU representative will contact the Member within 10 business days to finalize their fraud claim.

### Compromised Credit Card:

To report fraud on a TDECU credit card, please contact: (888) 918-7341

### Also:

1. The Member should contact the major credit reporting agencies (credit bureaus) to request a "fraud alert" be placed on their file. This will require creditors to call you before they open an account in your name. (Note: the credit bureaus will not accept an alert for debit card fraud. They record ID theft and loan fraud)  
[Equifax](#): 866.349.5191  
[Experian](#): 888.397.3742  
[TransUnion](#): 800.680.7289
2. Notify local law enforcement agency to file an Identity Theft Report or a Debit/Credit Card Abuse Report.
3. Report situations of consumer fraud to the Federal Trade Commission.

## What tools does TDECU offer to help safeguard against fraud?

To ensure TDECU Members use their debit and credit cards with confidence, we offer the following FREE tools to help put them in control of their card security:

1. [Visa Purchase Alerts](#) allow Members to monitor their card and receive alerts for transactions in real-time; to immediately detect potentially fraudulent activity.

2. Customizable [TDECU Digital Banking Alerts](#) provide alerts via text message, phone call, secure message or email when events occur on a Member's account(s).

## Is there anything else Members can do to protect their card(s) from fraud?

There is no way of stopping criminals from "hacking" into databases of merchants. While the possibility of a card being used fraudulently is low, we recognize the aggravation it causes our Members, and have some tips on how to help avoid fraud. **Tips to Help Minimize the Risk of Debit and/or Credit Card Fraud** Members should do the following:

1. Always know where your card is, and if you misplace it, call TDECU immediately so we can block the card from use.
2. Never write your Personal Identification Number, or PIN, on the card or carry the written PIN with you.
3. Do not share your PIN with anyone.
4. Don't give your account number to anyone on the phone unless you've made the call to a company they know to be reputable. If they've never done business with the company before, do an online search first for reviews or complaints.
5. Carry their cards separately from your wallet. It can minimize losses if someone steals your wallet or purse. And carry only the card you need for that outing.
6. During a transaction, keep your eye on the card. Make sure you get it back before you walk away.
7. Never sign a blank receipt. Draw a line through any blank spaces above the total.
8. Save their receipts to compare with your statement.
9. Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.
10. Report any questionable charges by calling the number on the back of the card.
11. Notify TDECU if your address changes or if you will be traveling.
12. Don't write your account number on the outside of an envelope.
13. Sign up for Visa Purchase Alerts to monitor your Visa debit card account activity and call the number on the back of the card if you see anything suspicious.
14. Register your Master Card credit card with MasterCard SecureCode to help prevent online fraud.
15. Periodically check your credit report with one of the online credit reporting services.