

## **Frequently Asked Questions and Answers on Compromised Debit Cards**

### **Background information:**

On rare occasions, Visa USA® will notify Community Banks of Colorado that a number of our customers' debit cards may have had the data compromised on their card. This data compromise does not mean any of our customers' cards have been affected. We regret that Visa does not release any details; however we take the appropriate steps to help protect our customers' accounts by reissuing cards.

### **In the rare event fraud does occur – how am I protected from financial loss?**

As a Community Banks of Colorado Visa® debit cardholder, you are protected with Visa's Zero Liability\*, which means you pay nothing for unauthorized purchases on your account.

\*Visa's Zero liability policy covers U.S. issued cards only and does not apply to commercial credit cards, ATM transactions or PIN transactions not processed by Visa. Cardholders must notify card issuer promptly of any unauthorized use. Visit [www.visa.com/security](http://www.visa.com/security) for more information.

### **Will I need to pay for the replacement card?**

We will replace all cards listed as compromised from Visa® at our expense as a courtesy to our customers.

### **How will I know that my card was compromised?**

We will send a letter with details about your card replacement. Our process to notify and protect customers begins immediately after receiving a list of potentially compromised card numbers from Visa®.

### **Was my card compromised or do I have fraud on my account?**

Not necessarily. We have had a small percentage of data compromised cards. This does not mean fraud has occurred or will occur, but we send out new cards to avoid the potential. As always, attention should be given to your account on a regular basis, and report any unusual activity.

### **What does it mean that my card was compromised?**

A compromised card is a card that is at risk of being used fraudulently. This data compromise, also known as hacking occurs when an individual or group of individuals gain unauthorized access to a computer system for the purpose of corrupting or stealing data. Data is transferred from your card when you make a transaction at a merchant such as a store, gas station, over the internet or on the phone.

### **What information was compromised on my debit card?**

The only information that is encoded on your debit card is your name, debit card number



(which is not your Community Banks of Colorado account number) and the expiration date. Any accounts linked to your debit card are not revealed to a merchant when you make purchases, ATM withdrawals or point of sale transactions.

**Could the bank have prevented this incident?**

The bank has no control over where you use your card and how the merchants store your information. Each merchant must attempt to protect customer's information by ensuring that your information is secure.

**What is Community Banks of Colorado doing to protect my account?**

We will replace all debit cards at our expense to all potentially compromised customers.

In addition to your personal monitoring efforts, Community Banks of Colorado uses sophisticated fraud monitoring services for all of our customers. We actively monitor all debit cards for fraud 24/7.

**I was asked to provide my PIN. Should I be giving out my PIN?**

At no time will our bank or any representative request your PIN (personal identification number) or your full card number. We will ask to verify recent debit card activity with you. If it is determined that your debit card is being used fraudulently, you will instantly have your card blocked to prevent further transactions from occurring and a new card will sent to you.

**Should I continue to use my debit card?**

Until you receive your new card from us, please continue to use your existing debit card, monitor your account activity, and let us know as soon as possible of any unauthorized use of your card. The best way to monitor your account is through our online banking service.

**Why was I not notified by telephone?**

Although we may contact you by telephone, we will focus our efforts on immediately reissuing new cards to reduce inconveniences and possible fraud.

**How long will it take for me to receive a new Card?**

It usually takes 7-10 business days to receive a new card. You will receive a PIN reminder first in the mail and shortly thereafter; you should receive the new card. The PIN reminder will contain your new PIN. If you would like to change your four digit PIN, call 1-800-851-4859. After dialing, follow the prompts to change your password. Press \* # to access the help menu, and make sure to press # after each completed entry.

You may continue to use your current card until receiving a new card.



**What should I do with my old card?**

Once the new card arrives, you should destroy the old compromised card. The bank will place a restriction on the card as of the date on the notification letter, which should provide time for a new card to arrive.

**Why don't you disclose the name of the merchant in the letter that you send me?**

We never receive the names of the merchants involved. We receive a list indicating that an undisclosed merchant's database was compromised. The merchant is protected because law enforcement ultimately investigates the case. Once the case is closed, the merchant may be revealed at a later date.

**Was any Community Banks account information compromised? Should I close my account?**

It is important to know your checking or savings account number was not compromised as part of this breach so it is not necessary to close your account.

**What if I have preauthorized debits made on my comprised card?**

You should contact the merchants immediately upon receipt of your replacement and provide them with the new card number and expiration date. Try the merchant's web site to update, or you may need to write the merchant with the card number change.

**Are my joint account owners'/signers' cards affected?**

Debit cards each have a separate number, so the other card may not be affected. Credit cards have the same number, so both cards must be replaced immediately.

**Can this information be used to steal my identity?**

The information encoded on the card only pertains strictly to the card. Other confidential information such as Social Security numbers, driver's license, addresses and dates of birth are not stored on the card.

**Other appropriate actions for protecting your personal information.**

**Do:**

- Use secure online banking and e-statements to minimize physical data loss.
- Verify account activity on regular basis.
- Shred all personal financial information, such as bills, statements, ATM and debit card receipts and credit card offers.
- Keep your personal documentation in a secure place.
- Call the post office immediately if you are not receiving your mail.
- Be aware of your surroundings when entering your Personal Identification Number (PIN) at an ATM.



- Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- Report lost or stolen credit, debit and ATM cards immediately.
- Closely monitor the expiration dates on your credit and debit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit and debit cards upon receipt.
- Review your credit reports at least annually.
- Use appropriate passwords on your credit and debit cards, bank accounts, and phone cards. Avoid using the obvious passwords — your mother's maiden name, your birth date, or the last four digits of your Social Security Number or phone number. Memorize your numbers and/or passwords.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

**Do NOT:**

- Volunteer any personal information when you use your credit or debit card.
- Give your Social Security number, credit or debit card number, or any bank account details over the phone unless you have initiated the call and know that the business that you are dealing with is reputable.
- Leave receipts at ATMs, bank counters, or unattended gasoline pumps.
- Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- Record your Social Security Number or passwords on paper and store them in your wallet or purse.
- Disclose bank account numbers, credit or debit card account numbers or other personal financial data on any website or online service location, unless you verify a secured authentication key from your provider.

**Please contact your local Community Banks of Colorado branch for further questions.**



Community Banks of Colorado is a Member of the FDIC