DATA BREACHES: How IT IMPACTS THE CUSTOMER & THE FINANCIAL INSTITUTION
DATA BREACHES: How it impacts the customer & the financial institution

**TABLE OF CONTENTS**

- Data Breach Trends
- Financial Institutions Impact
- How First Citizens’ Protects Your Account
- Tips to Help in Preventing Fraud
With so many merchant data breaches in the news, we want you to know that First Citizens’ Federal Credit Union is ready to help if your personal or financial data is ever compromised. We take service to our customers seriously and will do everything we can to ensure that action is taken quickly to help you avoid becoming a victim of identity or account theft.

**Data Breaches:**

Data breaches have been increasing over the past several years. A Verizon report published earlier this year provides a comprehensive summary of global data breaches by breach type. As depicted in table 1 below essentially all types of threats have increased over the past decade with the biggest threats coming from Hacking and Malware.

*Table 1*

![](image)

2014 was an unprecedented year for retailer data breaches. These breaches have been reportedly driven by Malware. Malware can be any type of software that is intended to damage or disable computers or computer systems. In the prevalent malware attacks of 2014 many of the bad actors used software to collect consumer’s bank account information or debit/credit card information. Often times the malware attacks a retailer’s point of sale system, thus data is essentially stolen at the transactional level or Point Of Sale. As reported by several media outlets, many notable retailers were hit with data compromises in late 2013 and 2014. These retailers include, but are

---

DATA BREACHES: How it impacts the customer & the financial institution

not limited to: Target, UPS, Home Depot, Staples, Ab Acquisition (Shaw’s, Star, Albertsons).

Financial Institution & Customer Impact:

In the situation where a retailer’s back-office systems or databases are compromised, resulting in debit or credit card information being compromised, it is the financial institution that suffers losses associated with card fraud, despite the fact that the retailer may not have exercised due care in guarding consumer information. The issuer (typically a bank or credit union) also assumes the liability for losses when a compromised card is used. Since information on large scale consumer-data fraud is initially reported as “a possible data breach” banks and credit unions often face a difficult and costly choice of whether or not to re-issue cards during a “potential” compromise. Card re-issue’s not only have a direct cost (labor, vendor cost, card plastic cost), but also have a significant unquantifiable customer cost due to your inability to use the card during a “lock-out”. The direct costs associated with re-issuing a card can range between $4 and $10 per card. These costs are incurred by the financial institution.

Indirectly, customers are adversely impacted by not being able to use their cards during an immediate lock-out. Interchange fees earned by banks and credit unions for card usage; take a hit for several months as customers must re-register cards with various merchants or wait for card activations.

In several of the retailer related cases described above the data breaches could have been prevented by stronger data-security and encryption measures. These security measures are required by regulation for banks and credit unions.

How First Citizens’ Protects Your Account

When a breach is first reported either through traditional news media or from our subscribed, service-bureaus we immediately initiate our emergency breach procedures. This begins with a review of our entire debit card database to identify any card-transactions with the affected retailer for suspicious activity. In 2014, as a result of the ongoing and growing concerns with consumer fraud, First Citizens’ implemented an additional layer of security to further protect our accounts from being exposed to fraud. While no program is foolproof we believe our additional monitoring and tracking program coupled with the
security measures already in place will serve to further protect our customers from experiencing fraudulent account activity.

First Citizens’ Federal Credit Union Visa® debit cards are monitored 7 days a week, 24 hours a day for fraud detection. In the event that fraud is suspected our customers may be contacted by our Fraud Detection Center’s Voice Response Unit (VRU) or by a live representative from 8:00am – 9:00pm EST, to verify that a transaction is valid. If the customer is unavailable, a message will be left along with a toll free number for the customer to call back. If we are unable to reach the customer, we may block the card at our discretion until we are able to speak with the customer and verify the account activity.

If fraud is suspected on the account, the Fraud Detection Center will contact a customer to verify the transactions in question. You should always bear in mind that we never ask our customers to provide any account information or personal information such as your social security number, PIN number or any other particular account information. We will ask you to confirm the details of selected transactions to identify suspected fraudulent activity; details such as the date of the transaction, the amount of the transaction and or the merchant.

If the charges are valid, customers may continue to use their card. If the charges are not valid, the card will be blocked to prevent any further fraudulent activity.

**Note:** Fraud Prevention cannot stop a charge once it has been approved. They simply block your card to prevent further fraud. The Fraud Department as well as any Member Service Representative at any First Citizens’ Branch Office will work with you to complete the required reports to assist in attempting to recoup any unauthorized paid charges.

**Restricted Transactions**

As part of our efforts to protect our customer's account from fraudulent activity, First Citizens’ Federal Credit Union may from time to time limit certain types of transactions based on the probability that fraud may be involved. All reasonable efforts will be made to contact our customers in advance and provide notice of any limitations we may place on the card; however, the primary concern will be for us to react in a timely manner to prevent and/or limit any potential fraud exposure.

Our Fraud Prevention Service reviews various account and transactional characteristics to determine the likelihood of fraud. An example of such
DATA BREACHES: How it impacts the customer & the financial institution

account behavior may be identifying multiple account transactions being performed within a close proximity of time from the same card number; however, they are being conducted in different states.

**Tips to Help in Preventing Fraud**

**Before you travel**

In the event you will be traveling out of the country and will need to use your debit/credit card you should notify your financial institution. We ask that you notify us as soon as possible. This is so that we can monitor your account closely and to ensure access to your funds when using your First Citizens’ Visa Debit Card. If you will be traveling outside of the United States you will need to contact us at 774-628-7875 in order for us to authorize out of country transactions on your debit card.

Please update your phone numbers with us, including your cell number. You can also provide us with a temporary phone number. Please be sure to let us know when you return so we can remove this temporary number. This will allow Fraud Prevention to reach you during your travels, should it be necessary. If you are traveling abroad please take our contact info with you should you need to contact us.

**Sign up for e-Alerts**

If you have Online Banking or Mobile Banking you can sign up for e-Alerts. This is another effective way that you can monitor your account and your transactions.

**Check your transactions**

We encourage you to regularly monitor your account and if you suspect anything that may not be legitimate. First Citizens’ customers can easily monitor their accounts with online banking and mobile banking and see real-time transaction posting. Please notify us as soon as possible at 1-800-642-7515 so we may work with you to correct the situation. Please remember that First Citizens’ will never request any personal information (such as account numbers, passwords, PINS, or Social Security Numbers, etc.) through a text message, over the phone or through an unsecured email.

**Protecting Yourself**

- Check your credit report on a regular basis to ensure the information is correct.
DATA BREACHES: How it impacts the customer & the financial institution

- Never give personal information over the phone unless you initiated the phone call.
- Never give a credit card number over the phone unless you have initiated the phone call and know that the company is reputable.
- Always verify your print or electronic statements sent by your financial institution for accuracy.

Staying Safe Online

If you are shopping online, always use a secure browser and look for security indicators, like a lock icon in the address box of your browser.