Debit Card Fraud FAQ's

What is a compromised card?

A compromised card means that information (for example, debit/credit card number, name) has been obtained by an unauthorized source. In most cases, the incident occurs at a location that accepts or processes debit card transactions, such as merchants or a transaction processor. By notifying customers when we discover a potential compromised card, we take every precaution to ensure your account data is handled with the highest level of safety and security. **Receiving a compromised card letter does not mean fraudulent activity has occurred on your account.**

How does a card compromise occur?

There are several ways in which a card compromise may occur. Card Skimming can occur when a skimming device is inserted or attached to an ATM or card reader. The device records the information from cards until it is removed. Then the data is used to produce counterfeit cards.

A breach compromise can occur when a hacker is able to infiltrate the payment system of a merchant or card processor. They transmit the information back to themselves and store the information for later use or then transfer your card information on to another card for counterfeit use.

Are all of the cards on my account at risk if I receive a letter about a possible card compromise?

Not all cards on an account may be impacted, as each customer has a unique card number.

Will there be a charge to get a new card (if necessary)?

No, Uwharrie Bank replaced your card at no charge..

If my debit card is replaced, what else should I do?

Think of ways you have used your card for payments. For instance, if you have a recurring payment set up with your debit card or have it stored online anywhere (for example, Apple iTunes, eBay or Amazon.com), be sure to update your debit card information with these companies.

What else can I do to protect myself against debit card fraud?

1. **Download our e-zMobile** app to monitor your spending, Visit the Apple App Store or Google Play Store (Android Users) and search for e-zMobile. It's free and a great tool to help manage your debit card. To setup Debit Card Alerts through the e-zMobile app:
    - For Apple Apps (iPhone, iPad), log into the app and select **Debit Card Alerts** under the **More** option, which is located on the bottom of the home screen.
    - For Android apps, log into the app and select **Debit Card Alerts** under the **More** option, which is located on the top of the home screen.
2. You can also monitor your accounts through our Online Banking system. To register your debit card, log into **online banking** and select **Debit Card Alerts** from the **Additional Services** option, or from the **Featured** section on the top-right part of your online banking homepage.
3. Update your contact information! Notify the bank if any of your contact information, such as phone numbers or address changes. You can receive text alerts regarding potential fraud on your card. Without a current mobile number, the alert cannot be sent to you.
4. Pay attention to your surroundings. If an ATM or card reader does not look like other machines or suspicious in any way, do not use it. It could have a card skimmer attached. This includes card readers at gas stations and convenience stores.

Am I responsible for the fraudulent charges on my debit card?

You are not responsible for fraud on your account; however, you are expected to contact the bank immediately if fraud is identified. If fraud occurs on your account, you will be required to file a debit card dispute. We make every effort to refund the fraudulent charges as soon as possible.

Who should I contact if I have a fraudulent charge or my card has been lost or stolen?

If your card has not been canceled already, call us immediately at 704-991-2800. We will work with you to complete any necessary paperwork and refund any fraudulent charges.

What does Uwharrie Bank do to protect my information?

Our card processor uses state of the art technology to identify and stay informed of data breaches. From multi-channel monitoring to highly trained professionals, our processor works around the clock to detect and prevent fraud.