DEBIT CARD FRAUD FAQ

About Debit/Credit Card Fraud

As you have likely learned from local and national media outlets, Debit/Credit Card Fraud and Card Merchant Breaches are at an all-time high. Please know that FNB is monitoring the activity very closely to keep your money safe. Read the Frequently Asked Questions below to learn how FNB is protecting your accounts and what you can do to help.

What do I do if I find fraudulent or unauthorized transactions on my account?

Contact FNB during business hours at 641-472-4121 or call 800-236-2442 24/7 to report a lost, stolen or compromised card.

What preventative measures does FNB take to prevent card fraud?

We work closely with VISA® to monitor account activity. We have a Fraud Detection/Prevention program in place which understands and monitors spending patterns and transactions that match current fraud trends. If a transaction on your account looks suspicious, you may receive a call from our fraud department to verify that you made the charges. Your card may also be blocked if we are unable to reach you to verify the transactions in question. We also offer several free services that allow you to detect fraud as well:

- Online Banking and our mobile app allows you secure and convenient access to your account 24/7. Online enrollment is available on our website.
- E-Statements are available to reduce the risk of your paper statements being stolen. Online enrollment is available on our website.

How can I protect myself from becoming a victim of fraud?

- Monitor your account as often as possible, using online banking, mobile banking, and your periodic e-statement or paper statement. Report any unauthorized transactions immediately.
- Refrain from clicking directly on hyperlinks to avoid being taken to a spoof or fake website.
- Maintain updated virus software on all of your computers.
- Never give out your personal or account information by phone, unless you initiated the call. This includes e-mails, as well.
- Do not give your PIN number to anyone.
- If you suspect that you have given any information to someone that may not be legitimate, call immediately to let us know. We can help you with securing your account.
- Shop with merchants that you know. If a deal seems too good to be true, it probably is.
- Check your credit report at least annually to ensure that it is accurate.
- Notify the bank if any of your contact info (phone numbers, address, etc.) has changed to ensure we can reach you in the event fraud has occurred.

What happens when FNB detects fraud on my debit card?

We will block the affected card or cards. When a card is blocked, it means that the card will no longer work. Blocking can be done for both PIN and signature based transactions. Once a card is blocked, no one will be able to use the card for that transaction type. This is to protect your account and insure that the criminal cannot use the card information to make additional purchases.

We will immediately order you a new card. When we block a card, we will notify you that fraud has occurred on your account, your card has been blocked and a new card has been ordered. You will receive a new card within 7 – 10 business days.

When and how does card fraud occur?

When your card number is used to make a purchase, the information is transmitted through a payment network. A hacker may have gained access to your card information through one of these entities in the payment network. While fraud resulting from a data compromise is rare, it's important to understand that you are protected with Visa's® Zero Liability policy and that FNB continually monitors your account to prevent fraud from occurring.

What are the different ways that a card can be compromised?

Although there are many ways that a card can be compromised, here are the most common ways:

- Merchant or Processor Breach. This type of breach occurs when a hacker is able to infiltrate the payment system of either a merchant or a card processor. They transmit the information back to themselves and then transfer it onto another card for counterfeit use.
- Phishing. With this type of fraud, you are solicited for your personal and/or account information directly by criminals. You can receive e-mails, pop-up windows while surfing the internet or even phone calls trying to persuade you to give out your information. Also, Trojan viruses are installed on your computer without your knowledge, which allow the criminals to gather information directly from your computer or monitor your keystrokes.
- Skimming. This happens when the magnetic stripe information is captured, using a small skimming device. The card is either swiped through the device or the device is hidden behind a legitimate card reader (like at a gas pump or an ATM) and the information is captured and stored for later use. The information can then be transferred onto another card for counterfeit use.

How does FNB respond to a Merchant or Processor Breach?

After a breach has been identified, Visa® provides FNB with a listing of cards that have potentially been involved. Because the risk of impending fraud is much higher on these cards, FNB takes the pro-active step of re-issuing these cards immediately at no cost to the customer. Customers will receive a notification informing them that their card was involved in a breach and that their current card will be disabled soon – typically 1-2 weeks after receipt of the new card.

How do I find out where the breach occurred? Who was the merchant involved?

Because it is an active investigation, sometimes the source of the data compromise is unclear. It would be unfair to damage one company's business or reputation without knowing all the facts of the situation.

As a matter of policy, after security breaches such as this, Visa® works closely with the merchant or processor to ensure the appropriate level of security measures are being taken. The important point to remember is that regardless of who was involved, consumers are fully protected under Visa's® Zero Liability* policy for fraudulent purchases; and we have 1) replaced your compromised card and given you a new number to avoid unauthorized activity on your account and/or 2) are monitoring your account for any unusual activity. Although certain card account data was potentially compromised, that does not mean data related to your account was taken, or that fraud has occurred on your account.

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

With Visa's® Zero Liability* for Unauthorized Charges policy, you are not responsible for fraud on your account. If fraud occurs on your account, you will be required to complete a debit card fraud investigation form listing the fraudulent charges. We make every effort to refund the fraudulent charges as soon as possible.

*Contact the bank for details concerning the VISA® Zero Liability for Unauthorized Charges.

This is not the first time my card has been affected. Why has my card continually been compromised?

Unfortunately, fraud is becoming more and more prevalent. Although card companies like VISA® and card processors continually monitor for breaches, criminals still find ways to breach the payment network. Although FNB cannot control breaches that occur at merchants and card processors, you can rest assured that we will do everything possible to protect your account and minimize your inconvenience when a breach occurs.

When do I get credit for a transaction that I am disputing?

A provisional credit is posted to your account once we have reviewed your case and have all of the required documentation to process your dispute. However if we find that more information is needed to process your dispute or we find that you do not have a valid dispute, we will contact you.