Compromised Card - Frequently Asked Questions

What is a compromised card?

A compromised card is a card that is at risk of being used fraudulently. Cards may be compromised due to computer theft, unauthorized network intrusion, or any type of data breach to any aspect of the payment card environment.

How does Fidelity Bank react to compromise notifications?

Fidelity Bank takes every compromise seriously and encourages issuance of replacement cards for affected customers. Customers will receive written notification if their card data has been compromised.

How long will it take to receive my replacement card?

Replacement cards can be ordered in any Fidelity Bank lobby. If you go into the Kell, Cattleman's, or Burkburnett locations you will receive your replacement card the same day.

What if I do not want to have my card reissued?

Compromises are serious. Fraudulent activity may occur if the affected card is not closed. The fraud dispute process can be more inconvenient to customers than simply having a card replaced. While many customers do not experience fraud when a compromise is reported, the risk exposure still exists if the cards are not closed and replaced.

Does this mean that I have fraud on my account?

Not necessarily. In fact, among the list of card numbers we periodically receive, only a few are affected by fraud. Take the opportunity to review your monthly statement(s). Remember to view your current transaction history using Online or Mobile Banking. Ask your Personal Banker about Card Valet, a product that can turn your card off from a mobile device at the first sign of fraud.

What do I do if I discover fraud on my account?

Contact Fidelity Bank immediately. Any Personal Banker at any Fidelity Bank location can help you file your dispute paperwork.

What if I have preauthorized debits made to the compromised card number?

You should contact the merchant(s) immediately upon receipt of your replacement card and provide them with the new card number and expiration date. This process may be as simple as logging into the corresponding merchant(s) site and updating the information. If this is not the case, you may need to write to them to let them know of a card number change.

There are other authorized users on my checking account. Does this affect their cards too?

Debit cards each have a separate number. Therefore, if one card is compromised, that doesn't necessarily mean the authorized user card is compromised as well. Each card owner will receive a notification if compromised.

Can this information be used to steal my identity?

The information encoded on the compromised card pertains strictly to the card, potentially including the card number and expiration date. Confidential information such as Social Security Numbers, driver's license numbers, addresses and dates of birth are not stored on the card.

What can I do to keep this from re-occurring?

Unfortunately, we have no way of stopping criminals from "hacking" into databases of merchants, and merchants are not subject to the same federal data protection standards as financial institutions. While the possibility of a card being used fraudulently is low, we recognize the aggravation customers face in acquiring a replacement card or to have fraudulent activity removed from their account.