



RECEIVED

Security Alert — Heartland Credit/Debit Card Data Breach

DEPT. OF CONSUMER AFFAIRS

Banking

Privacy Policy

Security Center

Our Online Security Commitment

Our Mobile Security Commitment

TD VoicePrint

Single Use Security Codes

Fraud and Identity Theft

Phishing and Malware

Security Alerts

Other Fraud Risks

ID Protection Resources

Frequently Asked Questions

Glossary of Terms

What happened?

TD Bank and TD Banknorth were recently notified by Visa® that an illegal data intrusion into Heartland Payment Systems' computer network may have resulted in the theft of some of our customers' credit and debit card numbers. The intrusion affected merchants that use Heartland's service throughout the United States.

How does this impact me?

Some TD Bank and TD Banknorth customers are affected and we are working with Visa and other agencies in the preliminary stages of this investigation. However, it is important to note that a security breach of this nature is card information only — no personal information linked to card numbers, such as Social Security numbers, PIN numbers, checking or savings account numbers was disclosed. Additionally, Heartland has stated that no data regarding merchants was compromised.

Working in conjunction with Visa, we are closely monitoring these cards for suspicious activity. We have sophisticated fraud detection software that monitors every card transaction, 24-hours-a-day, seven-days-a-week. And remember, the Visa Zero Liability fraud protection covers you if you have any unauthorized use on your cards. At this time we do not have plans to re-issue credit or debit cards to impacted customers due to the aforementioned fraud detection tools we have in place.

How can I find out more information?

You can read our Frequently Asked Questions below and visit Heartland Payment Systems' website at www.2008breach.com for more information. If you suspect any fraudulent activity on your credit or debit card, you should immediately call the 1-800 number listed on the back of your card(s).

Frequently Asked Questions

Q: I am concerned about my confidential information. What happened?

A: We were recently notified by Visa that an illegal data intrusion into the Heartland Payment Systems computer network may have resulted in the theft of some of our customers' credit and debit card numbers. We take security breaches very seriously and are acting diligently to protect you. We have sophisticated fraud detection software that monitors every card transaction, 24-hours-a-day, seven-days-a-week. It is important to remember that you are protected by Visa's Zero Liability protection policy should you have fraud on your account.

Q: How could this happen?

A: Information that gets compromised can be picked up many different ways with today's modern technology. It is important to remember that you are protected by Visa's Zero Liability protection policy should you have fraud on your account.

Q: Are there other ways my information can be fraudulently obtained?

A: Unfortunately, there are many ways information can be fraudulently obtained. Dumpster diving, mail theft, direct access to personal documents in your home, stolen wallets or purses, online data theft, and impostors are just some of the ways that people obtain confidential information.

Keep in mind that your cards should be safeguarded at all times. Here are some things that you can do to protect yourself:

- Review bank statements for accuracy

- Never give your personal identification number (PIN) for your debit or credit cards by e-mail or phone

- Be suspicious of anyone who call or e-mails you seeking personal information

- When you need to provide a Social Security number or other confidential information ALWAYS know who you are providing this information to and why it is being requested

- Make sure that you are conducting business with legitimate businesses

Tear up or shred confidential information before discarding

Q: Are any of my other cards at risk?

A: The breach reportedly took place over several months during 2008. If you used your debit or credit card during that timeframe, it is possible that your card could be compromised. For current information, refer to the Security Center on our websites at TDBanknorth.com at <http://www.tdbanknorth.com/bank/securityalerts.html> or www.tdbank.com.

Q: Will my debit or credit card be re-issued?

A: No, at this time we do not have plans to re-issue cards which may be affected by this breach unless we detect suspicious activity involving those cards. Rather, TD Bank and TD Banknorth will continue to employ sophisticated systems and procedures to help safeguard your transactions. You will not be responsible for any unauthorized transactions on your debit or credit card accounts. We will monitor card transactions for fraudulent activity. It is important to remember that the Visa Zero Liability fraud protection will cover customers if they have any unauthorized use on their cards. In addition, we have sophisticated fraud detection software that monitors every card transaction, 24-hours-a-day, seven-days-a-week. If you have concerns about your card(s), please call the 1-800 number on the back of your card.

Q: Will it happen again?

A: This did not happen to our systems or network. We cannot guarantee that it will not happen again. However, we employ sophisticated systems and procedures to monitor card activity for potential fraud. We are closely monitoring these cards for suspicious activity, and we have fraud detection software that monitors every card transaction, 24-hours-a-day, seven-days-a-week.

RECEIVED

OCT 29 2024

DEPT. OF CONSUMER
AFFAIRS