In The News -- Debit Card Compromises

There have been many news items in the past several months relating to data breaches or compromises of consumer debit card information at large (and not so large) retailers. As always, you need to be able to distinguish between perception and reality to determine if any of your information has been used without your permission.

What does a data compromise or breach mean?
Data compromises occur when unauthorized access to a computer system is gained for the purpose of corrupting or stealing data. When you use your debit card at a merchant such as a store, gas station, over the internet or on the phone, your card information is recorded in a database that is retained by the merchant for a period of time. The retained information is typically card numbers and expiration dates. Unauthorized individuals may gain access to the information that is stored and may use it to perform fraudulent activity.

Does this mean that I have fraud on my account?
No. It means that your card information has potentially been compromised. While fraud resulting from a data compromise is rare, we recommend that you review your account and report any suspicious or unauthorized transaction to the bank immediately. Online banking is a great way to monitor account activity and you won't need to wait for a monthly statement.

How does West View Savings Bank react to compromise notifications?
We take every compromise seriously. Customers will receive written notification or a phone call from us if their card information has been potentially compromised. In certain circumstances, West View Savings Bank will issue you a new debit card.

How long will it take for me to receive a new Card?
It usually takes 5-10 business days to receive a new debit card. If you would like to change your four digit PIN, visit a West View Savings Bank location for assistance.

What can I do to keep this from occurring?
Unfortunately, you can't stop criminals from "hacking" into databases. We also recognize the inconvenience customers face in dealing with these situations.

What You Can Do To Protect Yourself

- Never give card information to anyone unless you initiate the transaction.
- When purchasing online, only use secure connections and websites with trusted merchants.
- Don't let others use your card and don't share your PIN with anyone else.
- Use online banking to review your accounts for potential unauthorized activity.
- Have a back-up payment method such as a credit card or cash.
- Contact one of our branches during regular business hours for assistance.

What should I do if I think I am a victim of identity theft?
If you detect fraud on your account, contact us immediately at 412-364-1911. Also --

- Consider placing a fraud alert on your credit report files. A fraud alert lets creditors know to contact you before opening a new account. Just call any one of the three credit reporting agencies at the number below to place a fraud alert:

  Equifax: 1-800-525-628 Experian: 1- 888-397-3742 TransUnion: 1-800-680-7289

- Obtain a free annual credit report from the above credit reporting agencies by going to www.annualcreditreport.com or calling 1-877-322-8228. You should periodically obtain each one of your credit reports and look them over carefully for accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as home address and social security number, that is not accurate or any other suspicious information or activity.