THE STEPHENSON National Bank & Trust

Financial Solutions from Advisors You Trust

SNBT HOME

Capital One Breach - Cardholder Fraud Education

A hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year. At this point, Capital One is saying that the vulnerability has been fixed and that it is "unlikely that the information was used for fraud or disseminated by this individual." However, the company is still investigating. It was also noted that "no credit card account numbers or log-in credentials were compromised and that over 99% of Social Security numbers were not compromised."

Although only Capital One customers are impacted by this breach, we consider this is the perfect opportunity to remind everyone of how stolen cardholder information is used to commit fraud. Below are some tips about keeping your information safe – even when dealing with someone who you think is from your bank.

Fraudsters have become increasingly adept at getting cardholders to share the information they need to commit fraud by posing as financial institution call center agents, or by sending text messages that look like they are coming from your bank, warning of suspicious transaction activities.

The fraudsters do this by using information stolen through data breaches at health insurance providers, reward program providers, credit bureaus, merchant terminals, and social media sites, as well as through malware programs deployed on personal computers.

Educate yourself to avoid compromising your personal information:

- A text alert from us warning of suspicious activity on your card will NEVER include a link. **Never click on a link in a text message that is supposedly from us.** A valid notification will provide information about the suspicious transaction and ask you to reply with answers such as 'yes', 'no', 'help', or 'stop' – but it will never include a link.
- **A text alert from us will always be from a 5-digit number and NOT a 10-digit number resembling a phone number.** Capital One text caller IDs will be 20733 or 37268. SNBT text caller IDs will be 48179.
- **A phone call from our Fraud Detective will only include request for your zip code, and no other personal information, unless you confirm that a transaction is fraudulent.** Only then will you be transferred to an agent who will ask questions to confirm that you are the actual cardholder before going through your transactions with you. If at any point, you are uncertain about questions being asked, or the call itself, hang up and call us directly.
- **We will NEVER ask for your PIN or the 3-digit security code on the back of your card.** Don't give them out to anyone, no matter what they say. Hang up and call us directly. Fraudsters will often ask cardholders to verify fake transactions. When the cardholder says no, they did not perform those transactions, the fraudster then says that their card will be blocked, a new card will be issued, and that they need the card's PIN to put it on the new card. Many people believe this and provide their PIN. Obtaining the 3-digit security code on the back of the card will allow a fraudster to conduct card-not-present transactions.
- **Regularly check your account online to see if there are any suspicious transactions that have occurred**, but especially if you are unsure about a call or text message you've received. If anything looks amiss, call us directly for assistance.
- ***If you have received a voice- or a text-message from us and are unsure about responding to it, call us directly for assistance.***

If you would like to learn about additional fraud prevention tools such as CardValet, Fraud Detective, or eAlerts, please contact us at 715-732-1732 or visit www.snbt.com