MALVERN BANK ADVISORY

SECURE USE OF YOUR CREDIT CARD INFORMATION

DID YOU KNOW?

It was announced in the media recently that a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year. Thus far, 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 the perfect opportunity to remind everyone of how stolen cardholder information is used to commit fraud. We include tips below about keeping your information safe - even when dealing with Malvern Bank or someone who you think is from our financial institution. 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 institution, warning of suspicious transaction activities. They are also known to call in to call centers posing as cardholders requesting changes to card information and parameters.

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, to mention just a few. Stolen, personally identifiable information is combined with stolen card information, resulting in sufficient information to create profiles that fraudsters can use to position themselves as the actual cardholders.

TIPS TO KEEP YOUR INFORMATION SAFE

- A text alert warning of suspicious activity on your card will NEVER include a link to be clicked. Never click on a link in a text message that is supposedly from your credit card company. A valid notification will provide information about the suspect transaction and ask the cardholder to respond to the text message with answers such as “yes”, “no”, “help”, or “stop”. It will never include a link. A text alert will always be from a 5-digit number and NOT a 10-digit number resembling a phone number.

- A phone call from an automated dialer should only include a 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 your credit card company directly. If you receive a call from someone claiming to be the call center and asking to verify transactions, no information should have to be provided by you other than your zip code, and a “yes” or “no” to the transaction provided.

- You will NEVER be asked for your PIN or the 3-digit security code on the back of your card. Don't give these out to anyone, no matter what they say. Hang up and call your credit card company 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. The 3-digit CV2 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 - especially if you are unsure about a call or text message you've received. If anything looks amiss, call your credit card company directly for assistance.

- If you have received a voice- or a text-message and are unsure about responding to it, call your credit card company directly for assistance.

- Download the **CardValet®** App. **CardValet®** has many Fraud Protection features to keep your information safe. Available on Google Play or the App Store.

Show Fraud Who’s Boss.
CardValet

GET IT ON Google play

Available on the App Store