# Card Risk Solutions

July 30, 2019

## Risk Office Advisory 19516

## Capital One Compromise and Cardholder Fraud Education

☐ 311: Informational; No Action Required
☒ **611: Need to Know; Action May Be Required**
☐ 911: Urgent; Action May Be Required

Debit Card & ATM Programs
Credit Gateway Programs
Full-Service Credit Programs

**Summary**
This Advisory from our Risk Office discusses the compromise of Capital One account and card application information and steps to educate your cardholders to help them avoid disclosing personal information to fraudsters.

The Fiserv Risk Office is providing this Advisory to address the recently announced Capital One breach of more than 100 million credit card applications and accounts.

It was announced in the media today that a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year. At this point in time, 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. We include below tips you can provide to your cardholders about keeping their information safe – even when dealing with you or someone who they think is from your 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 (PII) is combined with stolen card information, resulting in sufficient information to create profiles that fraudsters can use to position themselves as the actual cardholders.

We recommend educating your cardholders on the following points to help them avoid compromising their personal information:

- A text alert from us 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 us. A valid notification will provide information about the suspect transaction and ask the cardholder to reply to the text message with answers such as 'yes', 'no', 'help', or 'stop'. 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. Text caller IDs will be 20733 if you use the standard call center, or 37268 if you use the premium call center (please refer to FYI 17504).

- A phone call from our institution's automated dialer will 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 us directly. If a call is received by the cardholder, claiming to be our call center and asking to verify transactions, no information should have to be provided by the cardholder other than their zip code, and a 'yes' or 'no' to the transaction provided.

- We will NEVER ask you 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. 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, 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.

Should your institution wish to learn about additional fraud prevention tools such as CardValet, Fraud Warning, and Step Up Authentication, please contact your Card Services client executive for more information.