IROQUOIS FEDERAL

Capital One Compromise
How You Can Protect Your Account

Iroquois Federal is providing this information to address the Capital One breach of more than 100 million credit card applications and accounts.

It was announced recently that a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year. Capital One has stated that the vulnerability has been fixed and that it is unlikely that the information was used for fraud or disseminated by the hacker. However, the company is still investigating. Capital One claims 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 would like to take this opportunity to remind everyone of how stolen cardholder information is used to commit fraud.

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. They are also known to call banks posing as cardholders and requesting changes to card limits, mailing addresses and other information. The fraudsters do this by using data stolen through 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. 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.

Here is how you can help avoid a compromise of your 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 you 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.

- A voice message about suspicious activity 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 the transactions with you. If at any point you are uncertain about the questions being asked or the call itself, hang up and call us directly. If you receive a call from a call center asking you to verify transactions, you should be asked to provide no information other than your 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.

- Regularly check your account transactions online, but especially when you are unsure about a call or text message you've received. If anything looks unusual or suspicious, call us directly for assistance.

- We encourage you to enroll in *Card Valet* to help monitor your debit card activity and alert you to any fraudulent transactions immediately. You can access *Card Valet* through our Mobile Banking App in the Manage My Cards menu.

- Monitor your credit score using our online tool called *Credit Sense*. You can access it through online banking and our mobile App. Credit scores are calculated based on the information in your credit report, and if something seems awry, or you see a change in your score, you can use *Credit Sense* to make sure there have been no new accounts opened using your personal information.

Please be assured that we are monitoring debit card activity around the clock, and will alert you via text message or phone call if we see anything unusual or suspicious. If you have any questions or concerns regarding the Capitol One breach or any other security incidents, please call. Together, we can work to help protect your account and your personal information.