The Equifax Security Breach

On September 07, 2017, Equifax Inc., one of the nation's three major credit reporting agencies, announced a cybersecurity incident which may impact more than 143 million U.S. consumers. The information accessed primarily includes names, social security numbers, birth dates, addresses, driver's license numbers and credit card information.

Based on Equifax's investigation, the unauthorized access occurred between mid-May and July 2017.

To be clear, Commercial Bank was not compromised and your information was not stolen from our bank. However, Commercial Bank takes the security of our customer information very seriously, and we are providing you with the information we know about this massive breach and the steps you can take to protect your personally identifiable information if you so desire. Following this unprecedented breach, we are also asking our customers to be extra vigilant and report any suspicious activity in your bank accounts to Commercial Bank by calling 1-800-547-8531 or by visiting www.commercial-bank.com.

Commercial Bank strongly encourages our customers to protect themselves by taking these actions:

- Determine whether your information has been impacted by visiting Equifax's self-service portal. Click on "Potential Impacts" and enter your last name along with the last six digits of your social security number. (Note: Use a secure computer with an encrypted connection to further protect your information.)

- Review your account statements to spot any suspicious transactions. You can also monitor your account activity online at any time at www.commercial-bank.com. If you spot any suspicious transactions, please contact us immediately at 1-800-547-8531.

- Consider if you should place an initial fraud alert on your credit report (see www.consumer.ftc.gov/articles/0275-place-fraud-alert).

- Consider if you should freeze your credit file (see www.consumer.ftc.gov/articles/0497-credit-freeze-faqs).

- Review your credit reports for accuracy. Call any one of the three credit reporting agencies to receive your free annual credit report or visit www.annualcreditreport.gov.

Experian®
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion®
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Equifax®
P.O. Box 740241
Atlanta, GA 30374
800-349-5191
www.equifax.com

Watch out for scams

Criminals take advantage of security events such as these for phishing attacks. However, there are precautions you can take to protect yourself.

- Look out for e-mails that ask for confidential information.
    - For security purposes, legitimate organizations do not do this. Equifax will only be notifying the consumers by postal mail.
- Don't believe the scare tactics and threats to disable accounts or impose penalties if you don't verify information.
    - Contact the company directly if you aren't sure.

Basic rules.

- Don't give information to organizations you don't do business with.
- Never submit confidential information by email.
- Don't click on links you aren't sure are authentic.
    - Type the web site into the address bar to be sure it hasn't been messed with.

If you believe you are the victim of identity theft, contact your local law enforcement office and/or your state attorney general. Finally, you may also want to consider reviewing information about recovering from identity theft, which is available from the Federal Trade Commission (FTC) at www.identitytheft.gov or by calling 1-877-IDTHEFT (1-877-438-4338). The FTC also offers general information to protect your online presence at www.consumer.ftc.gov/topics/privacy-identity-online-security.

Equifax has established a dedicated toll-free number to answer questions you may have about the Equifax data breach and its effect on your personally identifiable information. You may call them at 1-866-447-7559.

If you have any questions, feel free to call us at 1-800-547-8531 or by visiting our website at www.commercial-bank.com. Thank you for being a valued customer of Commercial Bank. We look forward to serving you in the future.

CUSTOMER RESOURCES AND RECOMMENDATIONS

Customers will have many questions about the security of their financial assets and personal information. Below is a list of suggested resources.

- Consumers can obtain information about placing an initial fraud alert on their credit report (see https://www.consumer.ftc.gov/articles/0275-place-fraud-alert).
- Consumers can obtain information about freezing their credit file (see https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs).
- If consumers think they are a victim of identity theft, they should contact local law enforcement and their state attorney general's office. Additional information is available at https://www.identitytheft.gov/
- The Federal Trade Commission provides general information to protect a consumer's online presence (see https://www.consumer.ftc.gov/topics/privacy-identity-online-security).

REINFORCE IMPORTANCE OF CUSTOMER ACCOUNT MONITORING

Customers should be vigilant in monitoring accounts for fraudulent and suspicious activity and promptly report any activity to the bank. Often, personal information is sold on the dark web to further social engineering and phishing attacks. If a customer sees suspicious activity and contacts the bank, the bank can act to protect both the customer's account and itself from any additional losses. Additionally, encourage customers to safeguard bank accounts and credit cards by routinely changing online passwords and using strong passwords as well as to enroll in any security and alert systems offered by their banks.

SUMMARY OF RECOMMENDATIONS

- Educate bank employees about the potential for phishing emails and phone calls.
- Consider multiple forms of identification to verify identity when opening a new account.
- Explore what alternative verification information the bank already has to authenticate the customer and match the customer's response against the customer information on file.
- Raise customer awareness that customers may be more prone to phishing and spoofing attacks and suggest that they treat email and any links in email with great care.
- It is important for banks to remind customers that the bank is not responsible for the compromise of the Equifax data.
- In the event of a payment card compromise, ICBA offers a Cyber and Data Breach Toolkit with ready-made templates for banks to use as customer notifications as well as a resource guide for community banks facing payment card compromise.
- Customers should be vigilant in monitoring accounts for fraudulent and suspicious activity and promptly report any activity to the bank.