

## **Notice of Information Security Incident**

The privacy and security of the personal information maintained by First Commerce Bank is of the utmost importance. As such, we wanted to provide information about a recent data security incident.

### **What Happened?**

We recently learned that two First Commerce Bank employee email accounts were accessed by an unauthorized individual.

### **What We Are Doing.**

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we discovered on March 6, 2019, that the impacted email accounts were accessed from May 13, 2017 through January 11, 2019 and contained personal information belonging to a limited number of our customers. We have no evidence that any of the information has been misused.

### **What Information Was Involved?**

The impacted email accounts that were accessed contained names and one or more of the following: financial account information, Social Security numbers, driver's license numbers, credit card account numbers, and/or dates of birth.

### **What To Do.**

This notice provides precautionary measures individuals can take to protect personal information, including placing a fraud alert and/or security freeze on credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

### **For More Information.**

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal information.

**Individuals with further questions regarding this incident can call our dedicated and confidential toll-free response line that we have set up to respond to questions at 877-797-6088.** This response line is staffed with professionals familiar with this incident. The response line is available Monday through Friday, 9:00 am to 9:00 pm Eastern time.

## **– OTHER IMPORTANT INFORMATION –**

### **1. Placing a Fraud Alert.**

You may place an initial 90-day “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**TransUnion LLC**  
P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

## 2. Placing a Security Freeze.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

### **Equifax Security Freeze**

PO Box 105788

Atlanta, GA 30348

<https://www.freeze.equifax.com>

1-800-349-9960

### **Experian Security Freeze**

PO Box 9554

Allen, TX 75013

<http://experian.com/freeze>

1-888-397-3742

### **TransUnion Security Freeze**

P.O. Box 2000

Chester, PA 19016

<http://www.transunion.com/securityfreeze>

1-888-909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

## 3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

## 4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.