

16635



FIRST FEDERAL
BANK & TRUST

March 13, 2020

Name
Address
Boston, MA 02116

Subject: Notification of Data Security Incident

Dear _____:

We are writing to inform you of a data security incident that may have affected your personal information. The privacy and security of your personal information is extremely important to First Federal Bank & Trust ("First Federal"). That is why we are writing to inform you about this incident, offer you complimentary credit monitoring and identity protection services, and provide you with information relating to steps that can be taken to help protect your information.

What Happened? On July 10, 2019, First Federal became aware of unusual activity within its email environment. Upon discovering this activity, First Federal took immediate steps to secure the environment and commence an investigation. In so doing, First Federal engaged an independent cyber forensics firm to determine what happened and whether sensitive information had been accessed or acquired from its digital environment without authorization. On July 31, 2019, the forensics firm determined that an unauthorized individual had gained access to a First Federal employee email account. On February 11, 2020, as a result of additional data analysis, First Federal learned that messages and attachments contained within the impacted email account included some of your personal information.

Though the investigation showed that there was access to the email account, it was unable to confirm that individual messages containing your information were accessed. Further, our fraud monitoring department has not identified any misuse of your data. Nonetheless, out of an abundance of caution, we are writing to inform you of the incident and to provide you with access to complimentary credit monitoring and identity protection services.

What Information Was Involved? The information impacted in connection with this incident may have included the following: names, addresses, Social Security numbers, financial account numbers, driver's license numbers, health insurance policy and/or health insurance subscriber numbers.

What Are We Doing? As soon as First Federal discovered the incident, we took measures described above and we continue to monitor First Federal accounts for fraud. In addition, we are providing you with information about steps that you can take to help protect your personal information and, as an added precaution, First Federal is offering you complementary credit monitoring and identity protection services through Kroll, a global leader in risk mitigation and response. These services include 18 months of Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

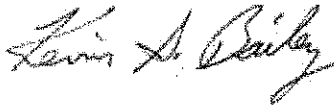
Membership Number: <<Member ID>>

What Can You Do? You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter. In addition, you can enroll in the free credit monitoring services that we are offering to you through Kroll. Enrollment instructions are included with this letter.

For More Information: Further information about how to protect your personal information is included with this letter. If you have questions or need assistance, please contact Kroll at <<Phone Number>>, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Kroll representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Kevin S. Bailey".

Kevin S. Bailey, President/CEO
First Federal Bank & Trust

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant, especially over the next 12 to 24 months, and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400
---	--	--	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.