



LEWIS BRISBOIS BISGAARD & SMITH LLP

Jill M. Szewczyk
1700 Lincoln Street, Suite 4000
Denver, CO 80203
Jill.Szewczyk@lewisbrisbois.com
Direct: 720.292.2024

March 13, 2020

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent First Federal Bank & Trust (“FFB&T”) in connection with a recent data security incident described in greater detail below. FFB&T is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On July 10, 2019, FFB&T became aware of unusual activity within its email environment. Upon discovering this activity, FFB&T took immediate steps to secure the environment and commence an investigation. In so doing, FFB&T 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 FFB&T employee email account. On February 11, 2020, as a result of additional data analysis, FFB&T learned that messages and attachments contained within the impacted email account included personal information. In response, FFB&T took measures to identify the potentially affected individuals and gather their contact information.

Affected information for residents of New Hampshire includes their names and addresses, account numbers, driver’s license numbers, and Social Security numbers. While there is no evidence of the misuse of any personal information, out of an abundance of caution, FFB&T notified the potentially affected population.

2. Number of New Hampshire residents affected.

FFB&T notified one (1) New Hampshire resident regarding this data security incident. Notification letters were mailed via first class U.S. mail on March 13, 2020. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

FFB&T has taken steps in response to this incident to further strengthen the security of its email system in an effort to prevent similar incidents from occurring in the future. In addition, FFB&T has offered all affected individuals 12 months of credit monitoring and identity protection services at no charge to the individual.

4. Contact information.

FFB&T remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2024 Jill.Szewczyk@lewisbrisbois.com.

Sincerely,



Jill Szewczyk of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Consumer Notification Letter



FIRST FEDERAL
BANK & TRUST

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Subject: Notification of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident that may have affected some of 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 identity monitoring services, and provide you with information relating to steps that can be taken to help safeguard 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 the 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 identity monitoring 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 safeguard your personal information and, as an added precaution, First Federal is offering you complimentary identity monitoring services through Kroll, a global leader in risk mitigation and response. These services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://krollbreach.idMonitoringService.com> to activate and take advantage of your identity monitoring services.

*You have until **June 10, 2020** 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 monitor 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 activate in the free identity monitoring services that we are offering to you through Kroll.

For More Information: Further information about how to safeguard your personal information is included with this letter. If you have questions or need assistance, please contact Kroll at 1-844-971-0674, 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 how you can help monitor 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 black ink that reads "Kevin S. Bailey". The signature is written in a cursive style with a large, prominent initial "K".

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	Experian	TransUnion	Free Annual Report
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	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 one (1) year. 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	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov , and	oag.state.md.us	ncdoj.go	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

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>.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.