



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

September 17, 2020

Bruce A. Radke
312.463.6211
312.873.2918 Fax
bradke@polsinelli.com

VIA E-MAIL (NDAG@ND.GOV)

Attorney General Wayne Stenehjem
Office of the Attorney General
600 E. Boulevard Avenue, Dept. 125
Bismarck, ND 58505

Re: Notification of a Data Security Incident

Dear Mr. Stenehjem:

We represent BankNorth in connection with a recent incident that may have impacted the personal information of six hundred twenty four (624) North Dakota residents and are reporting a potential data security incident pursuant to N.D. Cent. Code Ann. § 51-30-02. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While BankNorth is notifying you of this incident, BankNorth does not waive any rights or defenses relating to the incident or this notice, or the applicability of North Dakota law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

BankNorth recently learned a third party gained access to certain BankNorth employees' email accounts without authorization. BankNorth is not aware of any fraud or identity theft to any individual as a result of this incident and does not believe that accessing the personal information contained in the accounts was the primary motive of the third party. Nevertheless, because email accounts were accessed without authorization, and BankNorth cannot confirm exactly what, if any, information may have been viewed or acquired by the third party, BankNorth searched the impacted accounts to determine if they contained any personal information. On July 22, 2020, BankNorth determined that the compromised accounts contained certain personal information about North Dakota residents. The information varies across individuals but may include, depending on the person, their name, address, Social Security number, driver's license number, and date of birth.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California

74338192.2



Attorney General Wayne Stenehjem
Office of Attorney General
September 17, 2020
Page 2

NUMBER OF NORTH DAKOTA RESIDENTS AFFECTED

On July 22, 2020, BankNorth determined that the incident potentially impacted six hundred twenty four (624) North Dakota residents. BankNorth sent notification letters to the potentially impacted North Dakota residents via USPS mail on September 16, 2020. Individuals whose Social Security numbers or driver's license numbers were impacted received an offer for twelve (12) months of complimentary credit monitoring and identity theft protection services. Enclosed is a copy of the notice that BankNorth is sending to the impacted individuals.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, BankNorth promptly launched an internal investigation. BankNorth also engaged a forensic security firm to investigate the incident and confirm the security of its email and computer systems. Based on the results of the investigation, BankNorth reviewed the contents of the email accounts and identified the individuals whose information were in them. Once those individuals were identified, BankNorth worked to identify their addresses, and notified them as soon as possible after that was completed. For individuals whose Social Security numbers or driver's license numbers were impacted, BankNorth also offered a complimentary membership to credit monitoring and identity theft protection services.

BankNorth has also taken steps to reduce the risk of a similar incident from occurring again, including enabling multifactor authentication on all of its employees' email accounts and otherwise enhancing its security measures.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

A handwritten signature in cursive script that reads "Bruce A. Radke".

Bruce A. Radke

Enclosure

BankNorth
340 Main Street, P.O. Box 98
Arthur, ND 58006



[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

C-1034

Dear [REDACTED],

BankNorth is committed to the privacy and confidentiality of its customers, and takes protecting personal information entrusted to us seriously. This is why we are writing to inform you of a recent incident that may have exposed some of your personal information to an unintended audience.

We recently learned that, starting on February 18, 2020, some of your information could have been viewed by a third party that accessed certain BankNorth employees' email accounts without authorization. Upon learning of the incident, we promptly contained the incident by securing the email accounts to prevent further access. We also engaged a forensic security firm to investigate and confirm the security of our email and computer systems.

On July 22, 2020, our investigation determined that the accounts contained some of your personal information. The impacted information for each individual differs but may have included your name, address, Social Security number, driver's license number, financial information such as account number, and/or date of birth. For a very limited number of individuals, the information also included some basic medical information and/or medical insurance information.

At this point, we do not know for certain if any personal information was ever viewed by the unauthorized party, and are not aware of any instances of fraud or identity theft resulting from this incident. Furthermore, we do not believe that accessing personal information was the primary motivation of the third party. However, because your personal information was in the email accounts, and we cannot rule out the possibility that it was accessed, out of an abundance of caution we are notifying you of the incident. We are also offering you a complimentary one-year membership to Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-800-295-9470 Monday through Friday, 8:00 AM to 5:00 PM CST.

Sincerely,

[REDACTED]
[REDACTED]

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: [REDACTED] **PLEASE NOTE THAT THE ACTIVATION CODE IS CASE-SENSITIVE.**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll-free 1-877-322-8228, 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 print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: 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 new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.