

Appendix

On March 15, 2021, two of First National Bank Northwest Florida's ("First National") drives and a workstation became non-operational. First National worked to quickly address the incident, launched an investigation, and a forensic investigator was engaged to assist. Although this incident caused disruption, First National was able to quickly recover data from backups and return to normal operational capacity. The original forensic investigation concluded, and the third-party investigator determined, that although an unauthorized party gained access to First National's network between January 23, 2021 and March 15, 2021, all files containing personal information were secure. However, First National learned on August 9, 2021 that the unauthorized party may have accessed certain personal information including the name and one or more of: address, telephone number, Social Security number, passport number, driver's license, state issued identification or other government issued identification number, account number, debit or credit card number and/or telephone call-back password of one Maine resident.

To date, First National has no evidence that any individual has experienced identity theft as a result of this incident. Out of an abundance of caution, First National is offering the Maine resident access to complimentary identity monitoring services for one year through Kroll. This service helps detect possible misuse of personal information and provide identity protection services focused on immediate identification and resolution of identity theft.

To help prevent something like this from happening in the future, First National reset employee passwords, blocked malicious IP addresses identified during the initial investigation, deployed endpoint monitoring protection throughout the network, and is exploring other measures that they may implement to help prevent unauthorized access to the network in the future.

FIRST NATIONAL BANK NORTHWEST FLORIDA

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

First National Bank Northwest Florida (“First National”) understands the importance of protecting information we maintain. We are writing to inform you of a data incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

On March 15, 2021, two of our drives and a workstation became non-operational. We worked to quickly address the incident, launched an investigation, and a third party forensic investigator was engaged to assist. Although this incident caused disruption, we were able to quickly recover data from backups and return to normal operational capacity. The original forensic investigation concluded and the investigator determined an unauthorized party gained access to our network between January 23, 2021 and March 15, 2021 due to a vulnerability of a third party vendor. While the original investigation determined all files containing personal information were secure, First National learned on August 9, 2021, from a subsequent investigation, the unauthorized party may have accessed certain personal information including your <<b2b_text_1(Name, Impacted Data)>>.

To date, we have no evidence that any individual has experienced identity theft as a result of this incident. Out of an abundance of caution, First National is offering you access to complimentary identity monitoring services for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. This service is completely free to you and activating these services will not hurt your credit score. **For more information about Kroll’s identity monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:**

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

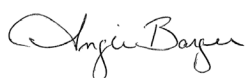
*You have until **December 28, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

We regret any inconvenience or concern this incident may cause you. Further, we encourage you to remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity. You should immediately report any unauthorized activity to the relevant financial institution or credit bureau reporting the activity. To help prevent something like this from happening in the future, we reset employee passwords, blocked malicious IP addresses identified during the initial investigation, deployed endpoint monitoring protection throughout the network, and we are exploring other measures that we may implement to help prevent unauthorized access to our network in the future.

If you would like more information about the incident, we have established a dedicated call center that has the most current, up-to-date information available. It can be reached by calling (855) 545-1989, Monday through Friday, between 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,



Angie Barger, President & CEO



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 will be able to help you determine if it is an indicator of identity theft.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You may contact the First National Bank Northwest Florida at 101 E 23rd Street, Panama City, FL 32405. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New Mexico: A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

New York: You may contact the First National Bank Northwest Florida at 101 E 23rd Street, Panama City, FL 32405 or by telephone at 850) 769-3207. You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Washington: On or about June 14, 2021, the First National Bank Northwest Florida discovered that an unauthorized party gained access to its network. On August 9, 2021, the First National Bank Northwest Florida learned that the personal information of Washington residents was involved in the incident.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.