THE FIRST NATIONAL BANK OF ELMER
Since 1903
Banking Simplified

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

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

## NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing because of a cyber incident that may have resulted in the disclosure of your personal information which is described below and which includes your <<b2b_text_1 (Impacted Data)>>.

The First National Bank of Elmer ("FNBE") and its management team are taking an aggressive approach to this incident in order to help protect against potential fraud. We are offering you free of charge the identity monitoring services described in this notice, and **we encourage you to activate those services as soon as possible**.

## What Happened and When

On approximately April 2, 2020, FNBE discovered suspicious activity on one of its employee's email accounts, and that an outside threat actor was able to access the email account and sent a series of emails attempting to set up a fraudulent wire transfer, which FNBE personnel were able to prevent from being completed. FNBE changed the login credentials for all persons with access to its computer systems, implemented additional security measures, and retained legal and technical counsel to determine the source and scope of the outside intrusion. On May 22, 2020, FNBE determined that the outside threat actor probably extracted information from the employee's email account folders.

## What Information Was Involved

We have determined that the data contained in the employee's email folders that was probably extracted included "personal information" of some of FNBE's customers as of April 2, 2020. The personal information included one or more of the following types of information that pertains to you: <<b2b_text_1 (Impacted Data)>>.

## What We Have Done About It

FNBE immediately shut down and disconnected the employee's computer from the network and changed the login credentials for all persons with access to its computer systems in order to ensure that the outside threat actor could no longer access any of its email accounts. Immediately following the discovery of the data breach, we contacted a number of professionals to investigate, assess and respond to the incident. We retained a company with expertise in forensic data breach investigations to try to determine the source of the intrusion, how the outside threat actor gained access to FNBE's computer systems, and whether and the extent to which the outside threat actor extracted information from FNBE's computer systems.

To prevent similar intrusions from happening again, we have implemented additional technological and operational controls on data access and unauthorized intrusion detection using the latest security protocols recommended for our industry. We take security very seriously and have taken all reasonable steps to prevent incidents from happening in the future.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll, a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data - to provide identity monitoring for one year at no cost to you.

Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

## WHAT YOU SHOULD DO

Because we value your security, we are taking this action to notify you following our investigation so that you can take appropriate steps to help protect yourself. Additionally, as noted above, FNBE is offering every affected individual one year of identity monitoring for free.

Identity monitoring helps detect possible misuse of your personal information and provides services focused on identification and resolution of identity theft. This is completely free to you and activating these services will not hurt your credit score. **We encourage you to sign up as soon as possible**. However, in order to get these benefits, you must activate these services – **we cannot do it for you**.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **November 25, 2020** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Finally, we have included an "Additional Steps to Help Protect Your Information" section with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

## For More Information

We apologize for any inconvenience or concern this may have caused. If you have any questions regarding the credit monitoring service, please call 1-888-920-0291, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,

Steven A. Botto
Vice President
Risk Officer

## ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

1. **Review your credit reports.** Even if you choose not to take advantage of the free identity monitoring services, we recommend that you remain vigilant for incidents of fraud or identity theft over the next 12 to 24 months by reviewing your account statements and closely monitoring your credit reports for any unauthorized activity. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months. Contact information for these agencies is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| Phone: 1-800-685-1111 | Phone: 1-888-397-3742 | Phone: 1-888-909-8872 |
| P.O. Box 740256 | P.O. Box 2104 | P.O. Box 105281 |
| Atlanta, GA 30348 | Allen, TX 75013 | Atlanta, GA 30348-5281 |
| www.equifax.com | www.experian.com | www.transunion.com |

Alternatively, you can also order your free annual credit report from the U.S. Federal Trade Commission ("FTC") by:

- Calling 1-877-322-8228;
- Ordering online at www.annualcreditreport.com; or
- Completing the Annual Credit Report Request Form, available at www.ftc.gov/credit, and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Georgia and New Jersey Residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

If you discover any suspicious items, notify your card issuing bank immediately. In the unlikely event that you fall victim to identity theft as a consequence of this incident, they will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. **Security Freeze.** You can place a security freeze on your credit report free of charge. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to obtain your credit report and use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Trans Union Security Freeze Fraud
Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
Phone: 1-888-909-8872

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348 www.
equifax.com
Phone: 1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com
Phone: 1-888-397-3742

In order to request a security freeze, you will 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. A copy of a recent utility bill, bank statement, or insurance statement; and
8. 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 lift the security 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 up to three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus 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. The credit bureaus have up to three (3) business days after receiving your request to remove the security freeze.

3. **Place Fraud Alerts with the three credit bureaus.** An initial fraud alert lasts one year and tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit reporting companies. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three bureaus will send you your credit report to review, free of charge.

To place a fraud alert on your credit report, contact <u>one</u> of the credit reporting companies (you do not need to contact all of them):

| Equifax Fraud Reporting | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 740241 Atlanta, GA 30374-0241 | P.O. Box 9554 Allen, TX 75013 | P.O. Box 2000 Chester, PA 19022-2000 |
| www.alerts.equifax.com | www.experian.com | www.transunion.com |

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. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Also, one way scammers use tax information is by filing fraudulent tax returns in order to get tax refunds. We recommend that you contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 to enable the IRS to try to monitor your account this year, but given the unfortunately large volume of these kinds of scams, they may not be successful in catching all fraudulent activity. For this reason, we recommend that you file your income tax returns as early as possible to help prevent any fraudulent returns from being filed on your behalf.

If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.

If a fraudulent tax return is filed, you will still likely be entitled to receive any refund that you are owed, but it will take some time to work through the process of correcting your tax return with the IRS and state taxing authorities. You will find additional information about tax returns at https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers and https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

   **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338) or www.consumer.gov/idtheft.

   **DC Residents:** Office of the Attorney General for the District of Columbia, 441 4th St NW #1100, Washington, DC 20001; (202) 727-3400 or http://oag.dc.gov.

   **Illinois Residents:** Illinois Attorney General, Consumer Fraud Bureau, 500 South Second Street, Springfield, IL 62701; 217-782-1090 or 1-800-243-0618 (toll free in IL).

   **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; 1-502-696-5300 or www.ag.ky.gov.

   **New York Residents**: For more information on identity theft, we suggest that you visit the New York State

Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

**North Carolina Residents**: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400 or http://www.ncdoj.gov.

**IF YOU ARE A RESIDENT OF ANY OTHER STATES:** Your state Attorney General's Office and website may provide relevant information.

**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.

Kroll | A Division of DUFF & PHELPS

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will 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.

### Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

### Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### $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 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.