



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

December 5, 2023

Via Email Reporting

Office of the Attorney General
Attn. Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: IDtheft@oag.state.md.us

RE: First National Bank at Darlington - Notice of Data Breach

Dear Sir or Madam:

We represent First National Bank at Darlington (“FNBD”), a full-service bank with branches in Lafayette County, Wisconsin, as data security and incident response counsel. This submission is provided pursuant to the Maryland Personal Information Protection Act, MD CODE ANN. COM. LAW § 14-3501, *et seq.* which requires disclosure to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

First National Bank at Darlington learned of suspicious activity involving one employee email account on July 11, 2023. FNBD shut down access to the account and reset network passwords. FNBD commenced an investigation into the activity that included partnering with computer forensic specialists. The investigation identified unauthorized access to an employee email account occurred on July 10, 2023, by someone outside the organization. Specifically, FNBD confirmed that certain emails and attachments that could have been viewed by the unknown actor contained sensitive personal information. FNBD conducted a thorough review of those items to identify whom the information belongs and completed the review on November 9, 2023. The types of personal information determined to be impacted include the resident’s name, driver’s license, and Social Security number.

On December 5, 2023, FNBD provided notice of the incident to one (1) Maryland resident via U.S. regular mail. A sample copy of the notice is attached as Exhibit “A” for your records.

The notice to the potentially affected individual includes encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit

www.fmglaw.com



Maryland Office of the Attorney General

December 5, 2023

Page 2

reports, immediately reporting errors or suspicious activity to the financial institution or appropriate service provider, and filing a report with law enforcement, the state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. FNBD also included contact information for the major consumer reporting bureaus and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so. As an additional precautionary measure, FNBD offered those affected individuals whose Social Security numbers were potentially accessed, twelve months of credit monitoring and identity restoration services through Experian.

After discovering the incident, FNBD reset passwords and implemented multi-factor authentication for all logins to FNBD email accounts. FNBD partnered with computer forensics professionals to thoroughly investigate the incident and performed a comprehensive review of files for the presence of personal information. In addition, FNBD continues to review its policies and procedures for ways to enhance the existing protections in place for the organization going forward. FNBD is notifying other state and federal regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit “A”



Return Mail Processing
PO Box 999
Suwanee, GA 30024

4 1 623 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



December 5, 2023

Dear Sample A. Sample:

First National Bank at Darlington (“FNBD”) takes the security and privacy of your personal information seriously. As part of that commitment, we are notifying you of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened

On July 11, 2023, we learned of suspicious activity involving one employee email account. FNBD shut down access to the account and reset network passwords. We commenced an investigation into the activity that included partnering with computer forensic specialists. Our investigation identified unauthorized access to an employee email account occurred on July 10, 2023, by someone outside our organization. Specifically, we confirmed that certain emails and attachments that could have been viewed by the unknown actor contained sensitive personal information. We conducted a thorough review of those items to identify whom the information belongs and completed the review on November 9, 2023.

What Information Was Involved

You are receiving this letter because, based on our review, information including your [impacted data elements] was present within one or more emails or attachments that were accessible by someone outside our organization on July 10, 2023. We note that we have no indication that any information was misused but we are notifying you so that you may take advantage of the resources we are offering you, should you find it appropriate to do so.

What We Are Doing

Upon discovery of the incident, we reset passwords to all user accounts and implemented multi-factor authentication to prevent future unauthorized access. We partnered with specialists to perform a diligent investigation to confirm no other email accounts were affected and conduct a thorough review of all emails and attachments within the impacted account. We are notifying individuals accordingly and we continue to review our policies and procedures for ways to enhance the existing protections we have in place for our organization going forward.

As an added precaution to help protect your identity, we are offering a complimentary twelve (12) month membership of identity theft protection services through Experian’s IdentityWorks. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: February 29, 2024 (Your code will not work after this date)

- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by February 29, 2024. Please be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or the appropriate service provider. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation titled "Additional Steps to Help Protect Your Information" for contact information and resources you may take advantage of to protect against fraud or misuse, should you find it appropriate to do so.

For More Information

First National Bank at Darlington is very sorry for any concern or inconvenience this incident has caused or may cause you, but please know that we remain committed to protecting the information entrusted in our care. If you have any other questions or concerns, you may contact [REDACTED] toll-free Monday through Friday from 8 am – 8 pm Central time (excluding major U.S. holidays). Please be prepared to provide engagement number [REDACTED].

Sincerely,

Amy Smith

Amy Smith
Vice President
First National Bank at Darlington

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax 1-800-525-6285 P.O. Box 105069 Atlanta, GA 30348 www.equifax.com	Experian 1888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion 1-800-680-7289 P.O. Box 2000 Chester, PA 19022 www.transunion.com
---	---	--

Report Suspected Fraud. 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.marylandattorneygeneral.gov, and toll-free at (888) 743-0023 or (410) 528-8662.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877 890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.