Burns White
ATTORNEYS AT LAW
A Limited Liability Company

Lyle Washowich | Attorney at Law | (412) 995-3004 | ldwashowich@burnswhite.com

April 21, 2023

VIA ELECTRONIC SUBMISSION

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

RE: Supplemental Notice of Data Event

Dear Sir or Madam:

We represent First National Bank of Pennsylvania ("FNB"), located at 12 Federal Street, Pittsburgh, PA 15212, with respect to the recent data incident described herein. We previously notified your Office via correspondence dated November 28, 2022 and December 23, 2022 regarding a hard copy data incident involving one of FNB's outside vendors that affected the security of certain personal information of approximately fifteen (15) Maine residents. We are following up to notify your Office of a second incident involving the same outside vendor, which may affect the security of certain personal information of approximately two (2) additional Maine residents.

The investigation into this event is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, FNB does not waive any rights or defenses regarding the applicability of Maine law, the Maine data breach notification statute, or personal jurisdiction.

Nature of the Data Event

FNB contracts with an outside vendor to provide print and mail services. As previously reported, on or about October 24, 2022, FNB became aware of an issue that occurred at the outside vendor wherein certain printed monthly bank statements ending September 30 and October 6, 2022 were not properly aligned during the printing process. As a result, some statements may have inadvertently included the name and account number of the next printed statement. On December 21, 2022, as previously reported, FNB provided written notice of this incident to potentially affected customers. Upon discovery of this issue, steps were immediately taken to rectify it. FNB worked with its outside vendor to assess the functionality of their systems, mitigate the impact and enhance their quality control processes.

On or about March 7, 2023, FNB became aware of a nearly identical incident that occurred at the same outside vendor wherein certain printed monthly bank statements ending December 31, 2022 were not properly aligned during the printing process. As a result, some statements may have inadvertently included the name and account number of the next printed statement. FNB has taken additional steps to work with its outside vendor to avoid any similar issues going forward. At this time, we are unaware of any identity theft or fraud as a result of this incident or the earlier incident.

Notice to Maine Residents

On or around April 21, 2023, FNB began providing written notice of this incident to the additional potentially affected customers, including approximately two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the data incident, FNB immediately launched an investigation to determine the nature and scope of this incident, as well as determine what data may potentially be affected. FNB provided written notice to the additional customers whose information may have been affected. This notice includes an offer of complimentary access to twelve (12) months of credit monitoring and identity theft protection services, including identity restoration services, through Experian IdentityWorks for impacted individuals.

Additionally, FNB is providing potentially impacted customers with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. FNB will also be providing notice of this event to other regulators as may be required under the applicable state or federal laws.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at (412) 995-3004.

Very truly yours,

/s/ Lyle Washowich

Lyle Washowich

LW/gad

EXHIBIT A

First National Bank of Pennsylvania
3015 Glimcher Blvd
Hermitage, PA 16148

Date

<<Address Line 1>>
<<Address Line 2>>
<<Address Line 3>>
<<Address Line 4>>
<<City>><<State>><<Zip>>

Re: Notice of Data Incident

Dear <<Address Line 1>>:

I am writing to notify you of an incident that occurred at a third-party vendor that may affect the privacy of some of your personal information. First National Bank of Pennsylvania (FNB) takes the protection of your information very seriously, and although we have no evidence of identity theft or fraud as a result of this incident, this letter provides details of the incident, the response and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about March 7, 2023, FNB became aware of an issue that occurred at our outside vendor who provides print and mail services to FNB. Certain printed monthly bank statements ending December 31, 2022, were not properly aligned during the printing process. As a result, some statements may have inadvertently included the name and account number of the next printed statement. Once this issue was discovered, steps were taken immediately to rectify it.

What Information Was Involved? Our investigation determined that your name and account number may have been inadvertently included at the bottom of another customer's monthly bank statement for the statement ending December 31, 2022. At this time, we are unaware of any identity theft or fraud as a result of this incident.

What We Are Doing. Information privacy and security are among our highest priorities. Upon discovering this incident, we immediately worked with our vendor to assess the functionality of their systems, mitigate the impact and enhance their quality control processes to avoid any similar issues going forward.

What You Can Do. We encourage you always to remain vigilant against incidents of identity theft and fraud, and recommend you review your account statements, monitor your credit reports for suspicious activity and detect errors for the next 12 to 24 months. If you suspect fraud in your accounts, please report such activity to FNB immediately by calling (800) 555-5455. Please also review the information contained in the enclosed *Steps You Can Take to Protect Your Information*.

Additionally, we are offering you access to 12 months of credit monitoring and identity theft protection services through Experian IdentityWorks at no cost to you. If you wish to activate these services, you may follow the instructions in the enclosure. Although we are unaware of any identity theft or fraud as a result of this incident, we encourage you to enroll in these services as an added precaution if you feel it is appropriate to do so.

For More Information. We understand that you may have questions about this matter that are not addressed in this letter. If so, please contact our toll-free assistance line at (800) 555-5455, 8:00 AM to 9:00 PM ET, Monday through Friday or 8:00 AM through 5:00 PM ET, Saturday and Sunday. You may also write to FNB at 3015 Glimcher Boulevard, Hermitage, PA 16148, Attn: Legal Department.

Sincerely,

Scot A. Pflug
Chief Information Security Officer
First National Bank of Pennsylvania

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at our expense and at no cost to you, in credit monitoring and identity theft protection services for 12 months provided by Experian IdentityWorks.

If you wish to take advantage of this monitoring service, you must enroll by XX/XX/XXXX.

How to Enroll: To activate this coverage please visit the website listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

Web Site: XXXXXXXXXXX
Activation Code: XXXXXXXXXXX

If you have any questions or would like to enroll by phone, you may call (877) 890-9332.

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- Email Address
- Activation Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We encourage you to enroll today should you feel the need to do so.

Monitor Accounts

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency and having information relating to fraudulent transactions deleted. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit bureaus listed on this page to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies using the following information:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com/personal/credit-report-services

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. All of the addresses where you have lived over the prior five (5) 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, a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the major consumer reporting agencies using the following information:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-916-8800	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft prevention, fraud alerts, security freezes and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information about how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov.

For Iowa residents, you are advised to report suspected incidents of identity theft to local law enforcement or 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.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6300; 1-888-743-0023; or www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or (919) 716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.