



Burns White Center
48 26th Street
Pittsburgh, PA 15222

t: 412.995.3000

f: 412.995.3300

w: www.burnswhite.com

Lyle Washowich
Attorney at Law

(412) 995-3004
ldwashowich@burnswhite.com

March 3, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

RE: 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 security incident described herein. We are writing on behalf of FNB to notify your Office of an incident that may affect the security of certain personal information of approximately nineteen (19) Maryland 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 Maryland law, the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Data Event

FNB merged into Howard Bank, a Baltimore-based institution, on February 5, 2022. In anticipation of the merger, Howard Bank customers were provided access to FNB's Online Banking. For a brief period of time, the Online Banking profile of certain of these new FNB (and former Howard Bank) customers was inadvertently connected to another Online Banking profile, which could have allowed another FNB customer to view the FNB deposit account numbers of these new FNB customers. Upon discovering its error on February 7, 2022, FNB immediately took steps to correct the issue and prevent future occurrences.

FNB's investigation of this incident determined that the name and FNB account number(s) of the new FNB customers were potentially accessible. At this time we are unaware of any identity theft or fraud as a result of this incident.

Notice to Maryland Residents

On or around March 4, 2022, FNB will begin providing written notice of this incident to potentially affected individual customers, including approximately nineteen (19) Maryland 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

FNB is providing potentially affected 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.

While FNB's investigation has found no evidence that customer account numbers have been accessed as a result of the incident described herein, the written notice to FNB's customers includes an offer of complimentary access to thirty-six (36) months of credit monitoring and identity theft monitoring services through Experian IdentityWorks. Additionally, the written customer notice includes the contact information for a dedicated call center for potentially affected customers to contact with questions or concerns regarding this incident.

Contact Information

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

Very truly yours,

/s/ Lyle Washowich

Lyle Washowich
Burns White LLC

LW/gad

Enclosures

cc: (w/ encls. via electronic mail)

Brian Mancos, Esq., Senior Corporate Counsel, First National Bank of Pennsylvania

Daniel Inadomi, Esq., Member, Burns White LLC

EXHIBIT A

<<Name_1>>
<<Name_2>>
<<Address>>
<<City>><<State>><<Zip>>

[Date]

Re: Notice of Data Breach

On behalf of First National Bank of Pennsylvania, I am writing to notify you of an incident that may affect the privacy of some of your personal information. Although we have no evidence of identity theft or fraud as a result of the incident, this letter provides details about the incident, the response, and resources available to help you protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? As you may be aware, Howard Bank merged into FNB on February 5, 2022. In anticipation of the merger, you were provided access to FNB's Online Banking. It has come to our attention that, for a brief period of time from February 5 until February 7, 2022, your Online Banking profile was inadvertently connected to another Online Banking profile, which could have allowed another FNB customer to view your FNB deposit account numbers. Upon discovering this error, FNB immediately took steps to correct the issue and prevent future occurrences, including providing affected customers with new FNB account numbers. Accordingly, we are providing this notice to you and other customers who may have been affected.

What Information Was Involved? Our investigation determined that your name and current FNB account number(s) were potentially accessible. 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. Although FNB is unaware of any actual or attempted misuse of your information related to this incident, FNB is providing you with complimentary access to 36 months of credit monitoring and identity theft monitoring services with Experian IdentityWorks so that you will be able to better protect against any unauthorized access to or misuse of your personal information. Instructions about how to enroll and receive these services are contained in the enclosed *Privacy Safeguards*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. For the next 12 to 24 months, we encourage you to remain vigilant against incidents of identity theft and fraud. If you suspect fraud in your account, please report such activity to the Bank. Please also review the information contained in the enclosed document, *Steps You Can Take to Protect Your Information*.

For More Information. We understand that you may have questions about this incident 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 Eastern Standard Time, Monday through Friday or 8:00 AM to 5:00 PM Eastern Standard Time, Saturday and Sunday. You may also write to First National Bank of Pennsylvania at 3015 Glimcher Blvd, Hermitage, Pennsylvania 16148, Attn: Legal Department.

Sincerely,

Scot A. Pflug

Scot Pflug
Chief Information Security Officer
First National Bank

Privacy Safeguards

As a precaution, we have arranged to have Experian IdentityWorks protect your identity for 36 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months.

The URL to activate the membership is <https://www.experianidworks.com/3bplus> (please make sure to use the URL that is included with this letter – using a different URL will render the code unusable).

- Unique code to enroll in Experian IdentityWorks identity theft monitoring: {CODE}
- The toll-free number for enrollments and/or questions is (877) 890-9332
- Enrollment end date is May 31, 2022 (prepaid coverage is for 3 years but requires enrollment prior to May 31, 2022)
- Engagement No.: B028219

Steps You Can Take to Protect Your Information

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 either 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

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-800-525-6285

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 law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or www.oag.state.md.us.

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