



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

February 1, 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 seventy-five (75) 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 is acquiring Howard Bank, a Baltimore-based institution, and it is expected that the transaction will be finalized in February 2022. In anticipation of the acquisition, on or about January 3, 2022, FNB mailed welcome packets to Howard Bank customers to assist with their transition to FNB. For Howard Bank customers with account numbers that duplicated existing FNB account numbers, these packets included certain personal information for the customers, including their name and current Howard Bank and new FNB account and routing numbers.

After the welcome packets were mailed, Howard Bank discovered that certain packets had been delivered to alternate or outdated mailing addresses for a small number of customers. Upon discovering its error, Howard Bank alerted FNB and began calling the affected customers to confirm whether they received the welcome packet from FNB. Following those calls, FNB was unable to confirm whether a select number of customers received the welcome packet. Accordingly, the Bank will be providing written notice of this incident to the customers who may not have received the original welcome packet.

In addition to calling potentially affected customers and providing notice to customers who may not have received the original welcome packet, FNB has been working to assign new account numbers for all affected customers to avoid any potential misuse of their Howard Bank or new FNB account. Affected customers will receive a separate correspondence with their new FNB account and routing numbers. Howard Bank has confirmed that the new FNB account information will be sent to the most up-to-date address for each customer.

Notice to Maryland Residents

On or around February 2, 2022, FNB will begin providing written notice of this incident to potentially affected individual customers, including approximately seventy-five (75) 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

The Bank has advised the potentially affected customers to regularly review their Howard Bank account activity up until the time that their FNB account is opened.

Additionally, the Bank 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. The Bank 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 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 Howard Bank, 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 is merging into First National Bank of Pennsylvania (“FNB”). In anticipation of the merger, on or about January 3, 2022, FNB mailed welcome packets to Howard Bank customers to assist with their transition to FNB. For Howard Bank customers with account numbers that duplicated an existing FNB account number, these packets included notification of a new FNB account number. After the welcome packets were mailed, Howard Bank discovered that certain packets had been delivered to alternate or outdated mailing addresses for a small number of customers. Upon discovering its error, Howard Bank alerted FNB and began calling the affected customers to confirm whether they received the welcome packet from FNB. Following those calls, we were unable to confirm that you received the welcome packet. Accordingly, we are providing this notice to you and other customers who may not have received the original welcome packet.

What Information Was Involved? Our investigation determined that your name and current Howard Bank and new FNB account and routing numbers were included in the welcome packet. 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. In addition to calling potentially affected customers and providing this notice to customers who may not have received the original welcome packet, FNB has been working to assign new account numbers for all affected customers to avoid any potential misuse of their Howard Bank or new FNB account. Affected customers will receive a separate correspondence with their new FNB account and routing numbers. Howard Bank has confirmed that the new FNB account information will be sent to the most up-to-date address for each customer.

What You Can Do. For the next 12 to 24 months, we encourage you to remain vigilant against incidents of identity theft and fraud. We also recommend that you regularly review your Howard Bank account activity up until the time that your FNB account is opened. If you suspect fraud in your Howard Bank 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,



Joseph Howard
EVP, General Counsel
Howard Bank

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Credit 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.



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

CHERRY HILL, NJ

CLEVELAND, OH

March 3, 2022

HARRISBURG, PA

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

PHILADELPHIA, PA

RE: Notice of Data Event

Dear Sir or Madam:

PITTSBURGH, PA

We represent First National Bank of Pennsylvania ("FNB"), located at 12 Federal Street, Pittsburgh, PA 15212, and we are writing on behalf of FNB to supplement the notice we provided to your Office dated February 1, 2022 regarding a recent data security incident. The February 1, 2022 notice is attached hereto as ***Exhibit A***.

PRINCETON, NJ

Howard Bank merged into FNB on February 5, 2022. In anticipation of the merger, on or about January 3, 2022, FNB mailed welcome packets to Howard Bank customers to assist with their transition to FNB. These packets included notification of a new FNB account number, and the packets for certain customers also included a book of starter checks associated with that account. After the welcome packets were mailed, FNB discovered that packets for certain customers had been delivered to an alternate or outdated mailing address. Upon discovering this error, FNB called the affected customers to inquire if they received the welcome packet and checks from FNB. Following these calls, FNB was unable to confirm that one (1) Maryland resident received the welcome packet and checks. Accordingly, on or around March 4, 2022, FNB will be providing written notice to this Maryland resident regarding the event described herein. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit B***.

WHEELING, WV

WILKES-BARRE, PA

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

WILMINGTON, DE

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



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

February 1, 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 seventy-five (75) 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 is acquiring Howard Bank, a Baltimore-based institution, and it is expected that the transaction will be finalized in February 2022. In anticipation of the acquisition, on or about January 3, 2022, FNB mailed welcome packets to Howard Bank customers to assist with their transition to FNB. For Howard Bank customers with account numbers that duplicated existing FNB account numbers, these packets included certain personal information for the customers, including their name and current Howard Bank and new FNB account and routing numbers.

After the welcome packets were mailed, Howard Bank discovered that certain packets had been delivered to alternate or outdated mailing addresses for a small number of customers. Upon discovering its error, Howard Bank alerted FNB and began calling the affected customers to confirm whether they received the welcome packet from FNB. Following those calls, FNB was unable to confirm whether a select number of customers received the welcome packet. Accordingly, the Bank will be providing written notice of this incident to the customers who may not have received the original welcome packet.

In addition to calling potentially affected customers and providing notice to customers who may not have received the original welcome packet, FNB has been working to assign new account numbers for all affected customers to avoid any potential misuse of their Howard Bank or new FNB account. Affected customers will receive a separate correspondence with their new FNB account and routing numbers. Howard Bank has confirmed that the new FNB account information will be sent to the most up-to-date address for each customer.

Notice to Maryland Residents

On or around February 2, 2022, FNB will begin providing written notice of this incident to potentially affected individual customers, including approximately seventy-five (75) 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

The Bank has advised the potentially affected customers to regularly review their Howard Bank account activity up until the time that their FNB account is opened.

Additionally, the Bank 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. The Bank 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 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 B

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

[Date]

Re: Notice of Data Breach

On behalf of First National Bank of Pennsylvania (“FNB”), 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 are likely aware, Howard Bank merged into FNB on February 5, 2022. In anticipation of the merger, on or about January 3, 2022, FNB mailed welcome packets to Howard Bank customers to assist with their transition to FNB. These packets included notification of a new FNB account number and included a book of starter checks associated with that account. After the welcome packets were mailed, FNB discovered that your packet had been delivered to an alternate or outdated mailing address. Upon discovering this error, FNB called you to confirm whether you received the welcome packet and checks from FNB. Following the call, we were unable to confirm that you received the welcome packet and checks. Accordingly, we are providing this notice to you regarding this original welcome packet.

What Information Was Involved? Our investigation determined that your name and new FNB account and routing numbers were included in the welcome packet. 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. In addition to calling potentially affected customers and providing this notice to customers who may not have received the original welcome packet and checks, FNB has been working to assign new account numbers for any affected customers to avoid potential misuse of their Howard Bank or new FNB account.

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

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.