



First National Bank

One F.N.B. Boulevard, Hermitage, PA 16148-3363

May 26, 2017

RECEIVED

MAY 30 2017

CONSUMER PROTECTION

**VIA US MAIL**

Attorney General Joseph Foster  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

Re: **Notice of Data Security Incident**

Dear Mr. Foster:

I serve as Corporate Counsel for First National Bank of Pennsylvania ("FNB"), One North Shore Center, 12 Federal Street, Pittsburgh, PA 15212, and I am writing to notify you of a data security incident that may affect the security of personal and/or sensitive customer information of approximately ten (10) New Hampshire residents and one (1) business with its principal place of business in New Hampshire. The investigation into this event is ongoing, and this notice will 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 New Hampshire law or personal jurisdiction.

**Nature of the Data Security Incident**

On or about January 23, 2017, FNB learned of a suspicious email message that was received by an FNB employee on January 10, 2017. FNB immediately launched an investigation and, on January 24, 2017, determined that the security of the FNB employee's email account had been compromised between January 10, 2017 and January 23, 2017, and certain information contained within the email account may have been accessible to an unauthorized and unknown individual(s) during this period of time.

FNB immediately took steps to investigate and mitigate the impact of this incident and identify the information contained in the email account that may have been accessible to the unauthorized and unknown individual(s), with the assistance of a third-party forensic investigation firm. While our investigation is ongoing, we determined on April 27, 2017, after a lengthy programmatic and manual review of information accessible through the email account, that the following types of information relating to customers and consumers may have been contained in a message or attachment and accessible to the unauthorized and unknown individual(s): name, address, and financial account information. However, FNB is unaware of any attempted or actual misuse of the personal information contained within the affected account as a result of this incident.

**Notice to the New Hampshire Residents and Businesses**

The affected email account contained information constituting sensitive customer information as defined by Gramm-Leach-Bliley Act, but not constituting personal information as defined by New Hampshire law,

related to approximately ten (10) New Hampshire residents. The affected email account contained information constituting personal information under New Hampshire law, but not sensitive customer information under the Gramm-Leach Bliley Act, related to one (1) New Hampshire business. On May 26, 2017, FNB will begin mailing written notice of this incident to these approximately ten (10) New Hampshire residents and one (1) New Hampshire business, in substantially the same form as the letters attached hereto as *Exhibit A* and *Exhibit B*.

#### **Other Steps Taken and to Be Taken**

Immediately upon discovery, FNB implemented appropriate measures to stop the data security incident and commenced a comprehensive investigation into this matter. This included the engagement of outside counsel specializing in data security response, as well as a third party forensic investigator.

In addition to providing written notice of this incident to all affected individuals and businesses as described above, FNB is offering all affected individuals access to 36 months of complimentary credit monitoring and identity restoration services with ID Experts, and is providing these individuals and businesses with helpful information on how to protect against identity theft and fraud. FNB is also providing written notice of this incident to other state and federal regulators, where required.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (724) 983-3497.

Sincerely,



Brian M. Mancos  
Senior Corporate Counsel

# Exhibit A



## First National Bank

First National Bank of Pennsylvania  
One FNB Boulevard  
Hermitage, PA 16148  
Mail Code: LGL

<<First Name>> <<Last Name>>  
<<Address>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:  
877-884-4113  
Or Visit:  
[www.idexpertscorp.com/protect](http://www.idexpertscorp.com/protect)  
Enrollment Code: <<XXXXXXXXXX>>

Re: Notice of Data Breach

May 26, 2017

Dear <<First Name>>:

First National Bank of Pennsylvania (FNB) takes the privacy of your information very seriously and, toward that end, deploys various critical safeguards to monitor, detect and protect your account against unauthorized intrusions. We are writing to inform you that our security system has identified a recent incident that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your information, FNB is providing this notice to ensure that you are aware of the incident so that you may take steps to protect yourself against the possibility of identity theft or fraud, using relevant tools offered by FNB, should you feel it is appropriate to do so.

**What Happened?** On or about January 23, 2017, FNB learned of a suspicious email message that was received by an FNB employee on January 10, 2017. FNB immediately launched an investigation and, on January 24, 2017, determined that the security of the FNB employee's email account had been compromised between January 10, 2017 and January 23, 2017, and certain information contained within the email account was accessible to an unauthorized and unknown individual(s) during this period of time.

**What Information Was Involved?** While our investigation is ongoing, we determined on April 27, 2017, that one or more of the following types of information related to you may have been contained in a message or attachment in the affected email account and may have been accessible to the unauthorized and unknown individual(s): name, address, Social Security number, driver's license number, credit card number and/or financial account number. **However, FNB is unaware of any attempted or actual misuse of personal information contained within the affected account as a result of this incident.**

**What We Are Doing.** FNB takes the security of customer and consumer information in our care very seriously. Attempts to gain access to personal information have become more frequent and are increasingly complex, often utilizing sophisticated tactics such as phishing, which involve fraudulent emails that are made to appear legitimate. These threats are also, unfortunately, a part of everyday life for the customers of financial institutions and businesses throughout the United States. FNB has proactive and sophisticated systems and processes in place to immediately identify, act on and notify customers about threats to their information security, whether or not their information was actually compromised. FNB has provided additional employee training and is adopting enhanced procedures relating to information security.

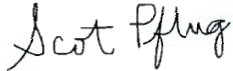
Upon learning of this incident, FNB terminated the unauthorized access and immediately took steps to investigate and mitigate the impact of this incident with the assistance of a third-party forensic investigation firm. FNB's investigation is ongoing. FNB has also provided notice of this incident to the appropriate law enforcement and regulatory authorities.

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 restoration services with ID Experts 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*.

**What You Can Do.** We recommend that you review the enclosed *Privacy Safeguards* document for more information about ways to better protect against the potential misuse of your personal information. FNB also encourages you to enroll and receive the complimentary credit monitoring and identity restoration services provided through ID Experts.

**For More Information.** Again, we take the security of your information very seriously. We apologize for any inconvenience or concern this incident may cause you. We understand that you may have questions that are not addressed in this letter. FNB has established a toll-free inquiry line, staffed with professionals familiar with this event and what you can do to protect yourself from misuse of your information, to assist you with questions regarding the incident. The inquiry line can be reached at 877-884-4113, Monday through Friday from 8:00 AM to 8:00 PM EST, excluding major U.S. holidays.

Sincerely,

A handwritten signature in cursive script that reads "Scot Pflug".

Scot Pflug  
Chief Information Security Officer

Enclosure

## PRIVACY SAFEGUARDS

As an added precaution, FNB has arranged to have ID Experts protect your identity for 36 months at no cost to you.

**1. Website and Enrollment.** Go to [www.idexpertscorp.com/protect](http://www.idexpertscorp.com/protect) and follow the instructions for enrollment using the Enrollment Code provided at the top of this letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

**2. Activate the credit monitoring** provided as part of your MyIDCare membership, which is paid for by FNB. Credit and CyberScan monitoring is/are included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at 877-884-4113 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

We encourage you, over the next 12 to 24 months, to remain vigilant against incidents of identity theft and fraud and to report suspected identity theft incidents to FNB. We encourage you to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. We encourage you to periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
PO Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/securityfreeze](http://www.transunion.com/securityfreeze)

In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for the previous two years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. Fees vary based on where you live, but commonly range from \$0 to \$10.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General. 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 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 of identity theft. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us), or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, [www.ncdoj.com](http://www.ncdoj.com), or 9001 Mail Service Center, Raleigh, NC 27699. For **Rhode Island residents**, the Attorney General can be contacted at (401) 274-4400, <http://www.riag.ri.gov/> or 150 South Main Street, Providence, RI 02903. Approximately four (4) Rhode Island residents were affected by this incident. This notice was not delayed as a result of a law enforcement investigation.

# Exhibit B





## First National Bank

First National Bank of Pennsylvania  
One FNB Boulevard  
Hermitage, PA 16148  
Mail Code: LGL

<<First Name>> <<Last Name>>  
<<Address>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

May 26, 2017

Dear <<First Name>>:

First National Bank of Pennsylvania (FNB) takes the privacy of your information very seriously and, toward that end, deploys various critical safeguards to monitor, detect and protect your account against unauthorized intrusions. We are writing to inform you that our security system has identified a recent incident that may affect the security of information related to your company. While we are unaware of any actual or attempted misuse of your company's information, FNB is providing this notice to ensure that you are aware of the incident so that you may take steps to protect your company against the possibility of fraud, using relevant tools offered by FNB, should you feel it is appropriate to do so.

**What Happened?** On or about January 23, 2017, FNB learned of a suspicious email message that was received by an FNB employee on January 10, 2017. FNB immediately launched an investigation and, on January 24, 2017, determined that the security of the FNB employee's email account had been compromised between January 10, 2017 and January 23, 2017, and certain information contained within the email account was accessible to an unauthorized and unknown individual(s) during this period of time.

**What Information Was Involved?** While our investigation is ongoing, we determined on April 27, 2017, that the following information related to your company may have been contained in a message or attachment in the affected email account and may have been accessible to the unauthorized and unknown individual(s): name, address, and financial account number. **However, FNB is unaware of any attempted or actual misuse of your company's information contained within the affected account as a result of this incident.**

**What We Are Doing.** FNB takes the security of your company's information very seriously. Attempts to gain access to sensitive information have become more frequent and are increasingly complex, often utilizing sophisticated tactics such as phishing, which involve fraudulent emails that are made to appear legitimate. These threats are also, unfortunately, a part of everyday life for the customers of financial institutions and businesses throughout the United States. FNB has proactive and sophisticated systems and processes in place to immediately identify, act on and notify customers about threats to their information security, whether or not their information was actually compromised. FNB has provided additional employee training and is adopting enhanced procedures relating to information security.

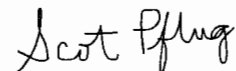
Upon learning of this incident, FNB terminated the unauthorized access and immediately took steps to investigate and mitigate the impact of this incident with the assistance of a third-party forensic investigation firm. FNB's investigation is ongoing. FNB has also provided notice of this incident to the appropriate law enforcement and regulatory authorities.

**What You Can Do.** We recommend that you review the enclosed *Privacy Safeguards* document for more information about ways to better protect against the potential misuse of your company's information.

**For More Information.** Again, we take the security of your company's information very seriously. We apologize for any inconvenience or concern this incident may cause you and your company. We understand that you may have questions that are not addressed in this letter. FNB has established a toll-free inquiry line, staffed with professionals familiar with this event and what you can do to protect against misuse of your company's information, to assist you with questions

regarding the incident. The inquiry line can be reached at 877-884-4113, Monday through Friday from 8:00 AM to 8:00 PM EST, excluding major U.S. holidays.

Sincerely,

A handwritten signature in cursive script that reads "Scot Pflug".

Scot Pflug  
Chief Information Security Officer

Enclosure

## PRIVACY SAFEGUARDS

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your company's account statements and your personal account statements for suspicious activity. While companies do not have credit files, the following information relates to protecting an individual's credit:

Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit <http://www.annualcreditreport.com/> or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. If you choose to do so, however, please note that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
PO Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/securityfreeze](http://www.transunion.com/securityfreeze)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself by contacting 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](http://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. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. **North Carolina** residents may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, [www.ncdoj.com](http://www.ncdoj.com), or 9001 Mail Service Center, Raleigh, NC 27699. This notice was not delayed as a result of a law enforcement investigation.