



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 20 2021

CONSUMER PROTECTION

Kevin M. Mekler
Office: (267) 930-2190
Fax: (267) 930-4771
Email: Kmekler@mullen.law

30725 US Hwy 19 N #337
Palm Harbor, FL 34684

May 13, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Peoples Bank and Trust ("Peoples Bank") located at 101 South Main Street, McPherson, KS 67460, and are writing to notify your office of an incident that may affect the security of some personal information relating to seven (7) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Peoples Bank does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 9, 2021, Peoples Bank learned it was the victim of a sophisticated cybersecurity attack. Upon learning of the attack, we acted quickly to protect our systems and the security of our customers with the assistance of third-party computer forensic specialists to determine the full nature and scope of the event. Peoples Bank also notified federal law enforcement, as well as all required local and federal regulatory agencies of this incident. On April 27, 2021, Peoples Bank learned that certain information on its system could have been subject to unauthorized access including name, address and one or more of the following elements: Social Security number, driver's license number, account number, and date of birth.

2021 MAY 20 PM 1:35

STATE OF NH
DEPT OF JUSTICE

Mullen.law

Notice to New Hampshire Residents

On or about May 13, 2021, Peoples Bank provided preliminary written notice of this incident to all potentially affected individuals, which includes seven (7) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Peoples Bank moved quickly to investigate and respond to the incident, assess the security of Peoples Bank systems, and notify potentially affected individuals. Peoples Bank is also working to implement additional safeguards and training to its employees. Peoples Bank is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Peoples Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Peoples Bank is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2190.

Very truly yours,



Kevin M. Mekler of
MULLEN COUGHLIN LLC

KMK/jej

EXHIBIT A

Peoples

Bank and Trust

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

Peoples Bank and Trust (“Peoples Bank”) is writing to inform you of a recent data privacy event that may involve some of your personal information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so. We sincerely apologize for any frustration or concern this may cause for our customers – you can rest assured that we are taking all the necessary steps to learn as much as we can about this incident.

What Happened? On or about April 9, 2021, Peoples Bank learned it was the victim of a sophisticated cybersecurity attack. Upon learning of the attack, we acted quickly to protect our systems and the security of our customers with the assistance of third-party computer forensic specialists to determine the full nature and scope of the event. Peoples Bank also notified federal law enforcement, as well as all required local and federal regulatory agencies of this incident.

What Information Was Involved? We determined the following types of information relating to you were present in Peoples Bank’s systems and therefore may be accessible to the threat actor during this incident: name, address, Social Security number, driver’s license number, date of birth and account number. Although there is no indication this information was accessed, acquired, or misused by the threat actor, Peoples Bank is providing this notice out of an abundance of caution because the potential exists.

We do want to underscore that our online banking platform was not impacted by this incident. We have no reason to believe that your current balances, card information, or online banking information has been impacted as a result of this incident. Our fortified banking systems are running as expected. You should see no disruption to your usual methods of banking, whether it be online or at one of our branches. Therefore, you should feel confident that we are ready, as always, to help with all your banking needs.


What We Are Doing. We are conducting a robust investigation to help us fully understand the situation. Additionally, while we have safeguards in place to protect data in our care, we are working to review and enhance these protections as part of our ongoing commitment to data security. As an added precaution, we are also offering access to <<CM Length>> months of complimentary credit monitoring and identity restoration services to those impacted by this incident.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud over the next 12 to 24 months, to review your account statements, and monitor your credit reports for suspicious activity and promptly report any incidents of suspected identity theft. You may also review the information contained in the attached “Steps You Can Take to Help Protect Personal Information.” There you will also find more information on the credit monitoring and identity protection services we are making available to you. While Peoples Bank is happy to cover the cost of these services, you will need to complete the activation process. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 535-1792, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Standard Time (except U.S. holidays). You may also write to Peoples Bank at P.O. Box 1226, McPherson, KS. 67460.

The entire Peoples Bank family sincerely apologizes for any inconvenience or frustration this may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Tom Pruitt". The signature is written in a cursive, flowing style.

Thomas Pruitt
President and CEO
Peoples Bank and Trust

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

See last page for credit monitoring instructions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. 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 reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 on 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Peoples Bank is located at 101 S. Main Street McPherson, Kansas 67460.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

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

Complimentary *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion[®], one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)