



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 28, 2021

VIA E-MAIL

Office of the Maine Attorney General
Security Breach Notification
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Event

Dear Sir or Madam:

We represent Bank of Labor, located at 756 Minnesota Avenue, Kansas City, Kansas 66101, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) Maine 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, Bank of Labor does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

It was determined on August 17, 2021, that a certain employee email account was accessed without authorization. Unfortunately, the investigation was not able to determine whether any specific email was accessed or viewed. In an abundance of caution, a programmatic and manual review of the contents of the account was done to determine whether sensitive information was present in the emails at the time of the incident. This process completed on September 15, 2021. It was at that time it was determined that personal information for three (3) Maine residents may have been accessible. It cannot be confirmed whether information related to the Maine residents was actually accessed by the unauthorized individual; however, Bank of Labor is currently locating any additional address information and will be notifying affected individuals and will update your office if such notice occurs.

The information that could have been subject to unauthorized access includes name, address, payment card number, and payment card expiration date.

Notice to Maine Residents

On or about October 25, 2021, Bank of Labor will provide written notice of this incident to all affected individuals, which includes three (3) Maine 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, Bank of Labor moved quickly to investigate and respond to the incident, assess the security of Bank of Labor systems, and notify potentially affected individuals. Bank of Labor is also working to implement additional safeguards and training to its employees. Bank of Labor is providing access to credit monitoring services for one (1) year, through Epiq Corporate Services, Inc., to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Bank of Labor 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. Bank of Labor is 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) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EXHIBIT A



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

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

<<Country>>

Re: Notice of Data Security Incident

Dear <<Name 1>> <<Name 2>>:

Bank of Labor 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.

What Happened? On or about August 17, 2021, Bank of Labor became aware of unusual activity within an employee mailbox account. We immediately began an investigation to determine the nature and scope of the activity. Through the investigation, we learned that the email account was subject to unauthorized access. We acted quickly to protect our systems and the security of our customers with the assistance of third-party computer forensic specialists, who confirmed that the unauthorized access was limited to one email account. The investigation could not conclusively rule out that an unauthorized actor may have accessed data related to you within the Bank of Labor employee’s email account. We are therefore notifying you about this event out of an abundance of caution. Bank of Labor also notified federal law enforcement and regulators about this incident.

What Information Was Involved? Bank of Labor, with the assistance of third-party forensic investigators, conducted an extensive programmatic and manual review of the accessed account to identify the types of information stored therein and to whom it relates. On September 21, 2021, we confirmed that the following types of information relating to you were present in the impacted email account: your <<name, address, and your social security number, driver’s license number, account number and date of birth>>. Although we do not have concrete evidence that any of your information was accessed, acquired, or misused, Bank of Labor is providing this notice in an abundance of caution.

What We Are Doing. Information privacy and security are among our highest priorities. Bank of Labor is conducting a robust investigation to help us fully understand the situation. Additionally, while we have strict security measures 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 <<12/24>> months>> of complimentary credit monitoring and identity restoration services to those impacted by this incident. <<language re issuing replacement credit cards, as applicable-to be supplied by client and incorporated herein by MC>>

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 Bank of Labor 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 <<confirm appropriate methods of contact with client, as they will likely not be engaging notification & call center vendors>>You may also write to Bank of Labor at 756 Minnesota Avenue, Kansas City, KS 66101.

The entire Bank of Labor family sincerely apologizes for any inconvenience or frustration this may have caused. Bank of Labor remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Robert McCall
President
Bank of Labor

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for <<one year/two years>> provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 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, three-bureau 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 following 6-digit telephone pass code <<699049 for 12 months/ 699104 for 24 months>> 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 **January 31, 2022**. 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®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your credit monitoring benefits, need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

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: 441 4th St. NW #1100 Washington, D.C. 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.

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 violator. 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/>.

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 are 9 Rhode Island residents impacted by this incident.