



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

July 12, 2023

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent LINKBANK located at 2010 Fruitville Pike, Lancaster, PA 17601, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) Maryland residents. By providing this notice, LINKBANK does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 19, 2023, LINKBANK was alerted to suspicious activity relating to an employee's email account. LINKBANK quickly began an investigation and determined that one employee email account was subject to unauthorized access. LINKBANK then engaged in a time intensive review of the email account to identify any sensitive information potentially at risk. As a result of this review, LINKBANK determined that certain information may have been subject to unauthorized access; however, no evidence of actual access or acquisition was found.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, and financial account information.

Notice to Maryland Residents

On or about July 12, 2023, LINKBANK began providing written notice of this incident to approximately two (2) Maryland 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, LINKBANK moved quickly to investigate and respond to the incident, assess the security of LINKBANK systems, and identify potentially affected individuals. Further, LINKBANK notified federal law enforcement regarding the event. LINKBANK is also working to implement additional safeguards and training to its employees. LINKBANK is providing access to credit monitoring services for 12 months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, LINKBANK 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. LINKBANK 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.

LINKBANK is providing written notice of this incident to relevant state and federal regulators, as necessary.

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

EJF/kld
Enclosure

EXHIBIT A

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

July 5, 2023

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>>:

LINKBANK is writing to provide information regarding a recent event that may affect the privacy of some of your information. Although we do not have evidence of any identity theft or fraud occurring as a result of this event, this letter provides details of the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so. We also encourage you to enroll in the complimentary credit monitoring services offered through TransUnion. Enrollment instructions are provided within this letter.

What Happened? On or about April 19, 2023, LINKBANK was alerted to suspicious activity relating to an employee's email account. LINKBANK quickly began an investigation and determined that one employee email account was subject to unauthorized access. LINKBANK then engaged in a time-intensive review of the email account to identify any sensitive information potentially at risk. As a result of this review, LINKBANK determined that your information may have been subject to unauthorized access; however, we found no evidence that it was, in fact, accessed or acquired.

What Information Was Involved? Our investigation determined that the following types of your information may have been contained within the email account: <<Breached Elements>> and your name.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of the activity, LINKBANK promptly commenced an investigation to confirm the nature and scope of the event. This investigation and response included confirming the security of LINKBANK's systems, reviewing the contents of relevant data for sensitive information, and notifying potentially affected individuals associated with the sensitive information. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures to strengthen the security of our systems. We have also reported this event to federal law enforcement as well as applicable regulatory authorities, as required by law.

As an added precaution, we are also offering twelve months of complimentary access to credit monitoring services through TransUnion. Individuals who wish to receive these services must enroll by following the enrollment instructions that were previously provided to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud over the next 12 to 24 months by reviewing your account statements, monitoring your free credit reports for suspicious activity, and reporting any suspected incidents of identity theft to your financial institution. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you. While we will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 833-627-2660, Monday through Friday from 9:00 a.m. to 9:00 p.m. [ET] (excluding U.S. holidays). You may also write to LINKBANK at 2010 Fruitville Pike, Lancaster, PA 17601.

Sincerely,

Brent Smith
President
LINKBANK

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months 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 unique 12-letter Activation Code <<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 following 6-digit telephone pass code <<Telephone Passcode>> 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.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. 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, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, 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.)

You can sign up for the *myTrueIdentity* online 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 credit file at TransUnion®, 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.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent.

However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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 <https://www.marylandattorneygeneral.gov/>.

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>.