

RECEIVED

APR 30 2021

CONSUMER PROTECTION



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

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

April 22, 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 MoneyLine Lending (“MoneyLine”) located at 3919 Market Street, Suite A, Camp Hill, PA 17011, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. 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, MoneyLine 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 September 11, 2020, MoneyLine became aware of suspicious activity occurring in an employee email account. MoneyLine launched an investigation to determine the nature and scope of the event, including bringing in third party forensic specialists to assist. MoneyLine immediately took steps to secure the email account, including resetting the account password. Further, the investigative teams reached out to Microsoft and Google to obtain additional information to support the investigation, and also notified federal law enforcement. On September 29, 2020, after a thorough investigation led by third party forensic specialists, MoneyLine confirmed that an unauthorized individual was able to access the employee email account for a period of time.

As part of its investigation, the forensic team reviewed all available evidence and could not confirm how the unauthorized actor accessed the cloud-based email account. However, it is suspected that

Mullen.law

the employee was the victim of a phishing email campaign. The forensic investigation confirmed that this incident was limited to one Office 365 cloud-hosted email account. No other MoneyLine email accounts were impacted, and none of MoneyLine's secure applications or other systems were affected. All Moneyline client data is securely maintained on a separate server at MoneyLine's corporate facility.

Out of an abundance of caution, Moneyline undertook a meticulous review of the messages and attachments stored within the affected email account to determine exactly what information, if any, may have been accessible to the unauthorized actor as a result of this event. This comprehensive review was completed on March 5, 2021. MoneyLine then launched a second review of its internal records to confirm updated address information to provide notice to potentially impacted individuals. This process completed on March 8, 2021.

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

Notice to New Hampshire Resident

On or about April 22, 2021, MoneyLine provided written notice of this incident to affected individuals, which includes approximately one (1) New Hampshire resident. 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, MoneyLine moved quickly to investigate and respond to the incident, assess the security of MoneyLine systems, and notify potentially affected individuals. MoneyLine is also working to implement additional safeguards and training to its employees. MoneyLine is providing access to credit monitoring services for sixty (60) months through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MoneyLine 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. MoneyLine 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.

Office of the New Hampshire Attorney General
April 22, 2021
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

A handwritten signature in black ink, appearing to read 'AF', with a long horizontal line extending to the right.

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/hfh

EXHIBIT A



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>>

Re: Notice of Data Incident

Dear <<Name 1>>:

MoneyLine Lending is notifying you of an incident involving an employee's Office 365 email account that may have impacted your personal information. The employee's email account was managed by MoneyLine's IT Managed Services Provider and hosted in Microsoft's cloud. We take this matter seriously, and write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud from any source, should you feel it is appropriate to do so.

What Happened? On or about September 11, 2020, MoneyLine became aware of suspicious activity occurring in an employee email account. MoneyLine launched an investigation to determine the nature and scope of the event, including bringing in third party forensic specialists to assist. MoneyLine immediately took steps to secure the email account, including resetting the account password. Further, the investigative teams reached out to Microsoft and Google to obtain additional information to support the investigation, and also notified federal law enforcement. On September 29, 2020, after a thorough investigation led by third party forensic specialists, MoneyLine confirmed that an unauthorized individual was able to access the employee email account for a period of time.

As part of its investigation, the forensic team reviewed all available evidence and could not confirm how the unauthorized actor accessed the cloud-based email account. However, it is suspected that the employee was the victim of a phishing email campaign. The forensic investigation confirmed that this incident was limited to one Office 365 cloud-hosted email account. No other MoneyLine email accounts were impacted, and none of MoneyLine's secure applications or other systems were affected. All Moneyline client data is securely maintained on a separate server at MoneyLine's corporate facility.

Out of an abundance of caution, we undertook a meticulous review of the messages and attachments stored within the affected email account to determine exactly what information, if any, may have been accessible to the unauthorized actor as a result of this event.


What Information Was Involved? The investigation confirmed that an unauthorized individual was able to access the cloud-hosted email account that contained personal information relating to certain individuals. Further, the investigation was unable to determine if any specific emails or attachments contained within the account were actually opened or viewed. Although we are not aware of any misuse of personal information stored within the account, out of an abundance of caution, we undertook a thorough, time-intensive audit of the entire contents of the email account to confirm what, if any, personal information may have been accessible to an unauthorized individual as a result of this event. This comprehensive review was completed on March 5, 2021. We then launched a second review of our internal records to confirm updated address information to provide notice to potentially impacted individuals. This process completed on March 8, 2021. We determined the following information related to you may have been viewed without authorization: <<data elements>>.

What We Are Doing. We are committed to maintaining the integrity and security of our client's information, and take this matter very seriously. In response to this event, we took steps to assess the security of our environment and aggressively implement mitigation steps and additional security protocols. Specifically, we reset the email account password, implemented additional password protocols, integrated Multi-factor authentication, and upgraded anti-virus and other system protections. We also worked with third-party forensic specialists to complete a thorough investigation.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information." We have also arranged for 60 months of complimentary credit monitoring and identity restoration services through Equifax. These services include dark web monitoring and insurance coverage of up to \$1 million. Instructions on how to enroll in these services is included in the enclosed "Steps You Can Take to Protect Your Information." You may consider taking steps to further ensure the security of your online accounts. This includes the creation of strong passwords, using different passwords for each of your accounts, and enabling multi-factor authentication.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated information line at 855-654-0921, available Monday through Friday between 9:00 am ET and 9:00 pm ET.

We apologize for any inconvenience or concern this incident causes you.

A handwritten signature in black ink that reads "Stephen A. Gebhardt". The signature is written in a cursive, slightly slanted style.

Stephen Gebhardt

Enclosure

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

Equifax Complete™ Premier

Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click "Continue".
*If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
Once you have successfully signed in, you will skip to the Checkout Page in Step 4.*
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch Gold with 3-in-1 Credit Monitoring automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your Activation Code provided above.

2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.

4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, 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 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.

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 listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include 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 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 agencies listed below:

Experian
P.O. Box 2002
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-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, 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: 400 6th Street NW, Washington, D.C. 20001; 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.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; (888) 743-0023; and www.oag.state.md.us.

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

For Washington D.C. residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.