



VIA ELECTRONIC MAIL and EXPRESS DELIVERY

Office of the Attorney General
Attn: Data Security Incident Notification
33 Capitol Street
Concord, NH 03301
Attorneygeneral@doj.nh.gov

September 15, 2017

Re: Legal Notice of Data Security Incident Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b)

Dear Sire or Madam:

In accordance with the above-referenced provision of New Hampshire law, I am contacting you to inform you of a data security incident.

In May 2017, Lendio was caught in a “phishing” scheme by an unknown individual. Since the breach was discovered, in July 2017, we have been investigating the incident. An unauthorized and unidentified individual obtained access to an employee email account containing various franchise documents.

We have determined that the email account contained franchise applications and company documents. This information included names, addresses, dates of birth, Social Security Numbers, the payment information in conjunction to franchise purchase applications, and some business-related information including Federal Employer Identification Numbers, addresses, and other business contact information.

To protect the potentially compromised individuals, Lendio is responding aggressively. Access to the file account has been updated and blocked to outside threats and we have conducted a full investigation of the matter and determined how the information was obtained. We have notified the Federal Bureau of Investigation (FBI). A thorough review of Lendio’s internal procedures is underway with the goal of further enhancing the security of confidential information.

On or around August 30, 2017, Lendio provided notice to all potential New Hampshire residents whose information has been discovered to be potentially be involved in this incident. While the investigation is ongoing, Lendio has elected to notify individuals that have been potentially impacted. To help relieve concerns and restore confidence, Lendio is offering credit monitoring services at no cost for one (1) year. We have also provided all potentially breached individuals with the steps to take if Identity Fraud occurs.

If you have any questions or comments, please do not hesitate to contact Ethan Hanson, VP Corporate Counsel, Lendio, Inc. 801-858-3322, ext 108, ethan.hanson@lendio.com.

Sincerely,

Ethan Hanson
VP, Corporate Counsel

Enc.

[Date]

Notice of Data Breach

[Name]
[Street]
[City, State, Zip]

Dear [Name],

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened

Lendio was caught in a “phishing” attack on or about the last week of May 2017. We have been investigating the incident since it was discovered in late July and are notifying you now that our investigation has provided us with enough information to believe that an attack in fact occurred and that your personal information was involved. An unauthorized and unidentified individual obtained access to an employee email account containing various franchise documents.

What Information Was Involved

The email account contained franchise applications and company documents. This information included your name, address, date of birth, Social Security number, the payment information you provided in conjunction with your franchise purchase application, and some business-related information including Federal Employer Identification Number, address, and other business contact information.

What We Are Doing

To protect you, Lendio is responding aggressively. Access to the file account has been updated and blocked to outside threats and we have conducted a full investigation of the matter and determined how the information was obtained. We have notified the Federal Bureau of Investigation (FBI). A thorough review of Lendio’s internal procedures is underway with the goal of further enhancing the security of confidential information.

We have worked to rapidly gain an understanding on what Lendio can do to support and protect you by engaging cybersecurity experts. To help relieve concerns and restore confidence following this incident, we are offering you credit monitoring services at no cost to you for one year. This service helps detect possible misuse of your personal information and provide you with identity protection support focused on immediate identification and resolution of identity theft. Instructions for enrolling in this service and additional information describing your services is included with this letter. We urge you to take advantage of these services as soon as possible.

What You Can Do

There are steps you can take to guard against fraud or identity theft. Carefully monitor your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. We have included information on where to access a free credit report in this letter. If you see anything you do not understand, call the credit agency immediately. If you find a fraudulent credit account on your credit reports, report the suspected identity theft to law enforcement, including your local police or sheriff’s office, the office of your state’s Attorney General, and the Federal Trade Commission (FTC). If you file a police report for identity theft, get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the “Additional Resources” reference guide included with this letter that describes additional steps that you may take to help protect yourself, including contact information for the FTC and major credit reporting agencies and information available from these resources about identity theft protection and placing a fraud alert or a security freeze on your credit file.

If you have received a notice from the Internal Revenue Service (IRS) that someone else has filed a tax return using your Social Security number or your efile return was rejected as a duplicate, you should file a Form 14039 "Identity Theft Affidavit" with the IRS. Many states offer similar resources and forms to file that can be obtained by calling your state department of revenue or accessing its website. You may also request the IRS to mail you a transcript of your tax account transactions for specific tax years by visiting <https://www.irs.gov/individuals/get-transcript>. For more information from the IRS about identity theft, visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> or call 800-908-4490 for specialized assistance.

For More Information

If you have questions, please call 1-855-853-6346, Monday through Friday from 8:00 a.m. to 5:00 p.m. Mountain Standard Time. To further assist you, Trudy Dalton, Franchise Administrator, is available to assist you with the information in this letter and help direct you to additional resources as required. She may be contacted via email at tdalton@lendio.com and is available Monday through Friday from 8:00 a.m. to 5:00 p.m. Mountain Standard Time.

Thank you,

Ethan Hanson
VP, Corporate Counsel



Enter your Activation Code: [insert code]

Product Information

Equifax® Credit Watch™ Silver provides you with the following key features:

- Equifax credit file monitoring with alerts to key changes to your Equifax Credit Report
- Automatic Fraud Alerts¹ With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) Data charges may apply.
- Access to one Equifax® credit report
- Up to \$25,000 Identity Theft Insurance²
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.

3. Create Account: Complete the form with your email address, create a User Name and Password, review the Terms of Use and then check the box to accept and click the “Continue” button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

Additional Resources

You are encouraged to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft or www.identitytheft.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit file to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit file if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit file for at least 90 days and you can renew it after 90 days. You may have an extended alert placed on your credit file if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. *You can place an initial fraud alert on your credit file by contacting any of the three national credit reporting agencies at the addresses or toll free numbers listed at the bottom of this page. You must contact all three national credit reporting agencies to place an extended fraud alert on your credit file.*

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. You must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and security freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax
(www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111

Experian
(www.experian.com)
P.O. Box 2002 (credit report
request)
P.O. Box 4500 (credit
disputes)
Allen, TX 75013
1-888-397-3742

TransUnion
(www.transunion.com)
P.O. Box 1000 (credit report
request)
P.O. Box 2000 (credit disputes)
Chester, PA 19016
1-800-680-7289