

Courtney Jones Kieffer
T (214) 651-4616
F +12146594137
Email:CKieffer@clarkhill.com

Clark Hill
901 Main Street, Suite 6000
Dallas, TX 75202
T 214.651.4300
F 214.651.4330

September 30, 2021

VIA Electronic Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Dear Attorney General John Formella:

We represent Lion Street Financial, LLC (“Lion Street”) as outside legal counsel with respect to a data security incident involving personal information as described below. Lion Street is committed to answering any questions you may have about its data security incident, its response, and steps it has taken to prevent a similar incident in the future.

1. Nature of security incident.

On January 21, 2021, Lion Street became aware of suspicious activity associated with one of its corporate email accounts. Lion Street hired independent computer forensic investigators to investigate. The investigation found that an unauthorized individual had gained access to a limited number of corporate email accounts. Unfortunately, the investigators were unable to determine what emails or attachments, if any, may have been viewed by the unauthorized individual. Lion Street then engaged a vendor to conduct a comprehensive review of the email accounts to identify any personal information that may have been contained in the accounts at the time of the incident. On August 26, 2021, Lion Street determined that names and some combination of individuals’ Social Security Number, date of birth, driver’s license number, medical information, health insurance policy information, or financial account information were present in one of the accessed email accounts.

2. Number of residents affected.

Twenty seven (27) of New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on September 30, 2021, via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken in response to the incident.

Since the incident, Lion Street has changed user passwords, retrained staff on identifying and responding to phishing emails, and started implementing multi-factor authentication on user accounts. Additionally,

September 30, 2021
Page 2

impacted individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

Lion Street takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at ckieffer@clarkhill.com or (214) 651-4616.

Very truly yours,

CLARK HILL



Courtney Jones Kieffer
CK:mkv



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-513-2605
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 30, 2021

NOTICE OF DATA SECURITY INCIDENT

Dear <<First Name>> <<Last Name>>:

We wanted to let you know about a data security incident experienced by Lion Street Financial, LLC, which is affiliated with Mercury Financial Group (“Mercury”), that may have impacted your personal information, including your name and Social Security number. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened?

Earlier this year we became aware of suspicious activity associated with one of our corporate email accounts. Immediately after discovering the suspicious activity, we changed all passwords and enabled additional access controls to protect the accounts. We then hired independent computer forensic investigators to conduct a thorough review of our email environment. The forensic investigators determined that an unauthorized user had gained access to a limited number of corporate email accounts. Unfortunately, the investigators were unable to determine what emails or attachments, if any, may have been viewed by the unauthorized individual. Out of an abundance of caution, we then engaged a vendor to conduct a comprehensive review of the email accounts to determine what information may be at risk. On August 26, 2021, we determined that some of your personal information may have been contained in the email accounts. While we were unable to confirm what emails or attachments may have been accessed, we wanted to notify you of this incident and provide resources to help protect yourself.

What information was involved?

From our review, it appears your name and some combination of your date of birth, driver’s license number, medical information, health insurance policy information, or financial account information may have been present in one of the accessed email accounts.

What are we doing?

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, we have changed the all user passwords, retrained staff on identifying and responding to phishing emails, and started implementing multi-factor authentication on all user accounts.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. I DX identity protection services include: Twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What can you do?

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-513-2605 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is December 30, 2021.

Again, at this time, there is no evidence that your information has been accessed or misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For more information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-513-2605 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Carie Heckler
Chief Compliance Officer
Lion Street Financial, LLC



Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-513-2605 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Six (6) Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.