



Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

November 29, 2019

File No. 50031.1032

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent M Holdings Securities, Inc. ("M Holdings"), located in Portland, Oregon, in relation to a data security incident involving Mezrah Financial, an M Holdings affiliate firm.

1. Nature of the data security incident.

On July 8, 2019, Mezrah Financial learned that an employee email account had been accessed without authorization. Mezrah Financial disabled access to the account and began an investigation, which included work with a digital forensics firm to determine the scope of the incident. Based on the results of the investigation, it was identified that certain Mezrah Financial employee email accounts appeared to be accessed without authorization from approximately July 1 to July 18, 2019.

As part of the investigation, a thorough review of the accounts involved was completed to determine if personal information may have been affected due to the incident. On October 8, 2019, the investigation revealed that certain individuals' personal information may have been affected. However, the forensics investigation was not able to find address information for all potentially affected persons. Accordingly, M Holdings and Mezrah Financial have worked to gather address information for the potentially affected persons to facilitate individual notification related to the incident. On November 22, 2019, M Holdings provided individual notification to the potentially affected individuals for whom valid address information was found by mailing notification letters to their last known address.

2. Number of New Hampshire residents affected.

M Holdings and Mezrah Financial have identified one (1) New Hampshire resident whose information may have been impacted by the incident. It has been determined that the individual's name and driver's license or state ID card number may have been involved. M Holdings is providing the notified individual 12 months of credit and identity monitoring services at no charge.

3. Steps taken relating to the incident.

Mezrah Financial has taken a number of steps to help prevent a similar situation from arising in the future and to further protect the privacy and security of sensitive information in its possession. These steps include enhanced security within its email platform, enhanced password complexity, enhanced audit logging, and enhanced general information security practices.

4. Contact information.

If you have any questions or need additional information, please contact me at 971.712.2795 or sean.hoar@lewisbrisbois.com.

Sincerely,



Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SBH:BMT

Encl.: Consumer Notification Letter



C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR, 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
[https://app.myidcare.com/account-
creation/protect](https://app.myidcare.com/account-creation/protect)
Enrollment Code:
<<XXXXXXXXXX>>

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

November 22, 2019

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident at Mezrah Financial, an M Holdings Securities, Inc. (“M Holdings”) affiliate firm, that may have involved your personal information. While we do not at this time have definitive evidence that your personal information was misused, in an abundance of caution we are proceeding under that assumption. The privacy and security of your personal information is important to M Holdings and Mezrah Financial. That is why we are informing you about this incident on Mezrah Financial’s behalf, offering you complimentary identity protection services, and providing you with information relating to steps that can be taken to help protect your information.

What Happened? On July 8, 2019, Mezrah Financial learned that an employee email account had been accessed without authorization. Mezrah Financial immediately disabled access to the account, and we began an investigation, which included work with a digital forensics firm to determine the scope of the incident. Based on the results of the investigation, it was identified that certain Mezrah Financial employee email accounts appeared to be accessed without authorization from approximately July 1 to July 18, 2019.

As part of the investigation, a thorough review of the accounts involved was completed to determine if personal information may have been affected due to the incident. On October 8, 2019, the investigation revealed that certain individuals’ personal information may have been affected. It has since been reviewed that the incident may have involved your information. We are therefore informing you of the incident and providing you with access to complimentary identity protection services from ID Experts.

What Information Was Involved? The types of information that may have been impacted include your name, address, <<VARIABLE TEXT LISTING AFFECTED DATA SETS>>.

What Are We Doing? As soon as the incident was discovered, M Holdings and Mezrah Financial took the steps described above. While Mezrah Financial did have certain security measures and protocols in place, Mezrah Financial has since taken measures to further enhance the security of personal information in its possession and to prevent similar incidents from happening in the future. In addition, we have worked with and provided assistance to law enforcement as needed regarding this incident and where required by law.

We are also providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering complimentary identity protection services for one year through ID Experts’ MyIDCare™.

ID Experts is a data breach and recovery services expert and has extensive experience helping individuals who have had an unintentional exposure of personal information. The MyIDCare services include: credit monitoring, CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

To receive MyIDCare services call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> and use the Enrollment Code provided above. Please note that you must enroll in the services no later than **February 22, 2020**.

What You Can Do: You can follow the recommendations on the following page to protect your personal information.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions concerning this incident, please contact 1-800-939-4170, Monday through Friday, 6:00 a.m. to 5:00 p.m. Pacific Time.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Jill Ehret".

Jill Ehret
Chief Compliance Officer

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or your Attorney General. Further recommended privacy protection steps are outlined in the Breach Help – Consumer Tips from the California Attorney General, and can be found at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
--	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.