



Bridgewater Place • Post Office Box 352
Grand Rapids, Michigan 49501-0352
Telephone 616 / 336-6000 • Fax 616 / 336-7000 • www.varnumlaw.com

Timothy E. Eagle

Direct: 616 / 336-6537
teeagle@varnumlaw.com

January 26, 2018

Attorney General Gordon MacDonald
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2018 JAN 30 AM 11:04

Re: Notice of Data Breach

Dear Attorney General MacDonald:

Pursuant to New Hampshire Statute Sec. 359-C:20(I)(b), we are writing to notify you of a breach of security involving 2 New Hampshire residents. This letter is to provide notification on behalf of our client, Member First Mortgage, LLC, a Michigan limited liability company, that one of its e-mail accounts was subject to unauthorized access. Our client's records indicate that 2 persons are New Hampshire residents having personal information which may have been in the e-mail account. Our client has no indication that any of the personal information stored on the computer network was accessed and/or acquired. Nevertheless, our client wanted to provide notice of the situation.

On December 21, 2017, our client discovered that someone had gained unauthorized access to one of its employee's e-mail accounts. Our client acted immediately to stop the unauthorized access. Subsequent investigation by outside consultants engaged by our client to investigate the incident indicated to our client on or after January 17, 2018 that the subject e-mail account contained personal information of 2 New Hampshire residents. The type of personal information at issue included individuals' names, social security numbers, addresses and mortgage loan account numbers.

Since learning of the incident, our client immediately took steps to secure the internal system against further intrusion, including by verifying that the unauthorized access to the e-mail account had been terminated and that the unauthorized access to the e-mail account did not result in other instances of unauthorized access to other accounts or sources of data. Our client also reported the incident to local law enforcement and to the FBI and is cooperating with their efforts. As noted above, our client also hired a cyber-security firm to assist in conducting an investigation to assess the cause and impact of the breach. Our client anticipates providing notice of the incident to the 2 New Hampshire residents on or about January 26, 2018 by U.S. Mail. A copy of the template letter is enclosed.

If you have any questions or need any help with anything mentioned in this letter, please contact me by e-mail at teeagle@varnumlaw.com or by phone at 616.336.6537.

Our client takes seriously its role in maintaining the security of all individuals' information. Please know that our client is taking steps, including the procedural changes noted above, to reduce the risk of this happening again.

Sincerely yours,

VARNUM

A handwritten signature in blue ink, appearing to read 'TE Eagle', is positioned below the name 'VARNUM'.

Timothy E. Eagle

TEE/bms

12703080_1.docx

Enclosure

January 26, 2018

[FName] [LName]
[Address1]
[Address 2]
[City], [State] [Zip]

Re: Notice of Data Breach

Dear [FName]:

We are sending this letter to you to inform you of a recent incident involving your personal information.

WHAT HAPPENED?

On December 21, 2017, we discovered that someone had gained unauthorized access to one of our employee's email accounts. We believe the unauthorized access may have occurred between approximately November 25, 2017 and December 21, 2017.

We acted immediately to stop any unauthorized access. Subsequent investigation indicated to us on or after January 17, 2018 that some of your personal information was likely contained in the email account that was accessed. We have no indication that any of your personal information stored in the account was actually accessed. Nevertheless, we wanted to provide notice to you so that you would be aware of the situation.

We apologize for any stress, inconvenience or difficulty this may cause you.

WHAT INFORMATION WAS INVOLVED?

The types of personal data that we believe were involved in the breach consisted of individuals' names, social security numbers, addresses, and mortgage loan account numbers. The personal data about you that was potentially accessed included all or some of these categories of data.

WHAT WE ARE DOING

Since learning of the incident, we immediately took steps to secure our internal systems against further intrusion, including by verifying that the unauthorized access to the email account had been terminated and that the unauthorized access to this email account did not result in other instances of unauthorized access to other accounts or sources of data.

We also reported the incident to the Kent County (Michigan) Sheriff's Department as well as the FBI and will cooperate with any efforts either of them may take. In addition, we have hired a

cyber-security firm to assist in conducting an investigation to assess the cause and impact of the breach. Finally, we are identifying further actions to reduce the risk of this situation recurring. You have the right to obtain a police report regarding the breach by contacting the Kent County Sheriff's Department, 701 Ball Ave., NE, Grand Rapids, Michigan 49503 (<https://www.accesskent.com/Departments/BOC/FOIA.htm>). Our notice to you, however, has not been delayed by our dealings with law enforcement.

WHAT YOU CAN DO

We are keenly aware of how important your personal information is to you, and we made arrangements with LifeLock Identity Theft Protection Services for a one-year membership for you at our cost. This service will help detect possible misuse of your personal information and will provide you with identity protection services focused on immediate identification and resolution of identity theft. **Since we are not authorized to enroll you in this program, we strongly encourage you to take the necessary steps to enroll, as outlined on the enclosed information sheet. We urge you to enroll immediately.**

As a security precaution, we also recommend you monitor your accounts for any suspicious activity. The enclosed information sheet outlines steps you should take if you believe your identity has been stolen or may be stolen.

Please review the enclosed information sheet for a list of actions we recommend you take.

FOR MORE INFORMATION

We have a team of people ready to answer questions you may have with respect to the matters described in this letter. Please contact us at 1-800-245-6180 (toll-free) if you have any questions. In addition, if you believe that your information has been used without your authorization, please notify your local law enforcement officials immediately so they can promptly investigate the matter.

We know how disconcerting this is, and we are so sorry for the stress and inconvenience this situation may cause you. We are working diligently to ensure this doesn't happen again.

Sincerely,

Jerry Reed
President & CEO
Member First Mortgage, LLC

Enclosure: Information Sheet

Member First Mortgage Information Sheet

1. **We have arranged for a one-year membership in LifeLock, at no cost to you, to help protect you. To activate your membership, please:**

- Go to LifeLock.com. Click on the red **START MEMBERSHIP** button.
- You will be taken to another page where, below the three protection plan boxes, you can enter the promo code: **MFMJ18** and click the **APPLY** button.
- On the next page, enter your **Member ID**. (Your Member ID is your first name last name plus 5-digit zip code. Ex. JOHNNORTON12345).
- Click the red **START YOUR MEMBERSHIP** button.
- You will receive a confirmation email after enrollment (be sure to follow all directions in this email).

PLEASE NOTE: For your convenience you may enroll by calling LifeLock at 1-800-899-0180 and give the enrollment agent the details listed above.

2. **Once you have completed the LifeLock enrollment process, the service will be in effect and includes:**

- Primary Identity Alert System
- Live Member Support 24/7
- Stolen Funds Reimbursement up to \$25,000
- Personal Expense Compensation up to \$25,000
- Service Guarantee for Lawyers and Experts up to \$1 million
- Identity Restoration Support
- One-Bureau Credit Monitoring
- Annual One-Bureau Credit Report & Credit Score

3. **The Federal Trade Commission (FTC) suggests the following steps if you believe your identity has been stolen or may be stolen. We recommend you do the following:**

- ✓ Place a fraud alert on your credit reports and review your credit reports. Contact any of the three consumer reporting companies below to place a fraud alert on your credit report. **You only need to contact one of the three companies to place an alert.** The company you contact is required to contact the other two companies.

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

Experian. 1-888-EXPERIAN or 1-888-397-3742; P.O. Box 9554, Allen, TX 75013;

www.experian.com;

TransUnion. 1-800-680-7289; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016; www.transunion.com.

- ✓ 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 30348-5281. You can print a copy of the request form at <https://www.annualcreditreport.com/ManualRequestForm.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for those entities is listed above.

- ✓ Carefully review your credit reports. Look for inquiries from companies that you haven't contacted, accounts that you did not open, and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names.
- ✓ Close any accounts that you know, or believe, have been tampered with or opened fraudulently.
- ✓ File your concern(s) with the Federal Trade Commission (FTC). This important information helps law enforcement agencies track down identity thieves. You can contact the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), or by visiting the FTC's website at www.ftc.gov/idtheft, or by writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- ✓ File a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report for this matter by contacting the Kent County Sheriff's Department, 701 Ball Ave., NE, Grand Rapids, Michigan 49503 (<https://www.accesskent.com/Departments/BOC/FOIA.htm>).

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year. We recommend that you carefully review your account statements, monitor your credit reports, and report to law enforcement any instances of actual or suspected identity theft.

4. **Finally, you can request that a security freeze be placed on your credit file by contacting each of the three reporting agencies listed above.**

You may also contact the FTC to receive additional information regarding security freezes. In some states, you have the right to place a security freeze on your credit file. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, even you will need to take special steps when you wish to apply for any type of credit. Please note, because of more stringent security features, **you will need to place a security freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files.** A security freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services. When requesting a security freeze, be prepared to provide your name, address, social security number, and date of birth. If you request a security freeze that is not free from a consumer reporting agency, there may be a fee of up to \$2 to \$12 depending on your state of residence to place, lift, or remove the security freeze. In some circumstances, the reporting agencies may waive the applicable fees.

5. **For Maryland residents:** Please note that you can receive further information on steps you can take to avoid identity theft from the Maryland Office of the Attorney General at 200 St. Paul Place, Baltimore, MD 21202, toll-free (888) 743-0023, or <http://www.marylandattorneygeneral.gov/>.
6. **For New Mexico residents:** You have a right to place a security freeze on your credit report or submit a declaration of removal with a consumer reporting agency pursuant to the Fair Credit Reporting and Identity Security Act. Please see above for more information on security freezes.
7. **For North Carolina residents:** Please note that you can receive further information on steps you can take to avoid identity theft by visiting the North Carolina Attorney General's website at www.ncdoj.gov/, or by contacting the North Carolina Attorney General at 1-877-5-NO-SCAM (toll-free within NC) or 1-919-716-6000 (outside NC), or by mail at Consumer Protection Division, Attorney General's Office, Mail Service Center 9001, Raleigh, NC 27699-9001.
8. **For Rhode Island residents:** Please note that you can receive further information from the Rhode Island Office of the Attorney General at (401) 274-4400 or <http://www.riag.ri.gov/>.

If you have further questions or concerns, please call us toll-free at 1-800-245-6180.