

# BakerHostetler

STATE OF NH  
DEPT OF JUSTICE  
2020 MAR 25 AM 9:57

## Baker&Hostetler LLP

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600

F 713.751.1717

[www.bakerlaw.com](http://www.bakerlaw.com)

Will Daugherty

direct dial: 713.646.1321

[wdaugherty@bakerlaw.com](mailto:wdaugherty@bakerlaw.com)

March 24, 2020

### VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General MacDonald:

On behalf of our client, Legacy Mutual Mortgage (“Legacy”), this report is to notify you of a data security incident.<sup>1</sup>

Legacy’s ongoing investigation into an email security incident recently determined that an unauthorized party could have accessed personal information in some Legacy employees’ email accounts. Upon learning of the incident, Legacy immediately took steps to secure the accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Legacy’s investigation determined that an unauthorized person obtained access to the email accounts at various times between approximately May 24, 2019 and September 16, 2019. The investigation was not able to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, Legacy conducted a thorough review of the emails and attachments that may have been accessed and, on January 28, 2020, determined that the emails or attachments to the emails may have included the names and Social Security numbers of four New Hampshire residents.

Today, Legacy is beginning to mail notification letters to the four New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20 via United States Postal Service First-Class mail. Enclosed is a sample copy of the letter. Legacy is offering one year of complimentary credit monitoring and identity theft protection services through Experian to individuals that had a Social Security number contained in the emails or attachments. Legacy also established a call center for the individuals to call with any questions regarding the incident.

---

<sup>1</sup> This notice does not waive Legacy’s objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

March 24, 2020

Page 2

To help prevent a similar incident from occurring in the future, Legacy is providing additional training to employees regarding phishing emails and implemented enhanced security measures, including multi-factor authentication.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Will Daugherty". The signature is stylized with a large, sweeping initial "W" and a long, horizontal flourish extending to the right.

Will Daugherty  
Partner

Enclosure



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

At Legacy Mutual Mortgage ("Legacy") we are committed to protecting the privacy of your information. We are writing to inform you about an incident involving some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

Our ongoing investigation into an email security incident recently determined that an unauthorized party could have accessed personal information in some Legacy employees' email accounts. Upon learning of the potential unauthorized access, we immediately took steps to secure the accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Our investigation determined that an unauthorized person obtained access to the email accounts at various times between approximately May 24, 2019 and September 16, 2019. The investigation was not able to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, Legacy conducted a thorough review of the emails and attachments that may have been accessed and, on January 28, 2020, determined that the emails or attachments contained some of your personal information, including your <<b2b\_text\_1(Impacted Data)>>.

Although, to date, we have no evidence of any misuse of your information as a result of this incident, we assure you that we take this incident very seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As a precaution, **we are offering you a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup> Credit 3B.** This product provides you with identity detection and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.**

We regret this incident occurred and any inconvenience it may cause. To help prevent a similar incident from occurring in the future, we are providing additional training to employees regarding phishing emails and implemented enhanced security measures, including multi-factor authentication. If you have any questions, please call 1-800-737-5591, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Don Kalbacher  
Chief Operation Officer

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

- Ensure that you **enroll by:** <<b2b\_text\_2(enrollment deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** <<Member ID>>

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057** by <<b2b\_text\_2(enrollment deadline)>>. Be prepared to provide engagement number <<b2b\_text\_3(engagement number)>> as proof of eligibility for the identity restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Maryland, New York, or North Carolina**, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)
- *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>
- *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**If you are a resident of Maryland**, the mailing address of Legacy Mutual Mortgage is 3503 Paesanos Parkway San Antonio, Texas 78231.

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report 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 report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report 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 a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

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 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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.