



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

March 10, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent First Home Mortgage Corporation (“First Home”) located at 6211 Greenleigh Ave Ste 300, Baltimore, MD 21220, and are writing to notify your office of an incident that may affect the security of some personal information relating to one thousand seven hundred forty-seven (1,747) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, First Home does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about November 30, 2021, First Home discovered suspicious activity involving an employee’s business email account. In response to that incident, First Home promptly took steps to secure its email environment and investigated the nature and scope of the activity, with the assistance of third-party cybersecurity specialists. Through this investigation, First Home learned that an unauthorized actor accessed the email account and may have accessed or downloaded email messages. First Home then performed a lengthy and labor-intensive process to determine whether the accessible account contained protected personal information and to whom that information belonged. That process was completed on February 9, 2022.

The information that could have been subject to unauthorized access includes name, driver's license number, Social Security number, credit card information, online account credentials, medical and health information, and financial information.

Notice to Maryland Residents

On or about March 11, 2022, First Home will provide written notice of this incident to all affected individuals, which includes one thousand seven hundred forty-seven (1,747) Maryland residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

First Home takes the confidentiality and security of information in its care very seriously. In conjunction with its initial investigation of this incident, First Home took steps to secure its email environment and to review existing policies and procedures in an effort to reduce the likelihood of a similar future incident. First Home is providing access to credit monitoring services for twenty-four (24) months, through Kroll, to individuals whose information was potentially impacted by this incident, at no cost to those individuals.

Additionally, First Home is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and credit freeze on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements, resetting online account passwords, and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the incident, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/mzb
Attachment

EXHIBIT A



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: <<b2b_Text_2[Notice of Security Incident/Notice of Data Breach]>>

Dear <<First_Name>> <<Last_Name>>,

First Home Mortgage Corporation ("First Home") is writing to inform you about an incident that potentially impacted your personal information. We have no indication that your information has been subject to actual or attempted misuse. Out of an abundance of caution, we are providing you this notice that contains information about the incident, our response to it, and the resources available to assist you with safeguarding your information, should you feel it is necessary. First Home values and respects the privacy of your information and prioritizes the confidentiality and security of the information within its care.

What Happened? On or about November 30, 2021, First Home discovered suspicious activity involving an employee's business email account. Upon discovery, we took steps to secure the account and launched an investigation into the nature and scope of the incident with the assistance of third-party cybersecurity specialists. That investigation determined that an unauthorized actor accessed the email account and may have accessed or downloaded email messages. We then performed a lengthy and labor-intensive process to determine whether the accessible account contained protected personal information and to whom that information belonged. On February 9, 2022, we determined that your information was in the email account at the time of the incident and may have been impacted by the incident, which is why you are receiving this notice.

What Information Was Involved? The information potentially impacted by this incident includes your <<b2b_Text_1(DataElements)>>.

What Are We Doing? First Home takes the confidentiality and security of information in its care very seriously. Once we were notified of the incident, we promptly investigated and took steps to secure our email environment. We undertook a thorough review of our existing policies and procedures in an effort to reduce the likelihood of a similar future incident. As an added precaution, we are providing you, free of charge, with access to identity monitoring services through Kroll for 24 months. Information on these services and instructions on how to activate may be found in the enclosed **Steps You Can Take to Help Protect Your Information**.

First Home will report this incident to the credit reporting agencies and applicable regulatory authorities as required by law.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, reset online account passwords, and to monitor your credit reports for suspicious activity and/or errors. We also encourage you to review the enclosed **Steps You Can Take to Help Protect Your Information** section of this letter, which shares additional resources available to you and instructions on how to activate the identity monitoring services we are offering. Please note, you will need to activate yourself in these services as we are unable to do so on your behalf.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please call our dedicated assistance line at 1-888-888-8888, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays. Please have your membership number ready.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

First Home Mortgage Corporation

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber(S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a general practice, we encourage individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are forty-four (44) Rhode Island residents impacted by this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.