

Morgan Lewis

Gregory T. Parks

Partner

215.963.5170

gregory.parks@morganlewis.com

VIA EMAIL TO SECURITYBREACH@ATG.WA.GOV

July 7, 2020

State of Washington
Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents the Federal Home Loan Mortgage Corporation ("Freddie Mac") and we are writing to notify you regarding the nature and circumstances of a recent data security incident involving a ransomware attack suffered by one of Freddie Mac's vendors. The data security incident potentially affects personal information of individual borrowers whose mortgage loans were sold to Freddie Mac.

On May 20, 2020, it came to Freddie Mac's attention that, earlier this year on an unknown date, a vendor Freddie Mac hired to perform services on some of its loans experienced a ransomware attack on systems that contained personal information of individual borrowers. At this time, Freddie Mac has no evidence that the personal information of affected borrowers has in fact been accessed or used inappropriately. Freddie Mac has been in communication with the vendor since learning of the incident. Because the incident left the vendor's system inaccessible to the vendor, the vendor did not immediately know the details of the incident or the information affected. Many details are still uncertain.

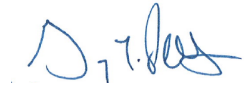
After investigation, Freddie Mac has determined that information on the vendor's systems at the time of the ransomware incident included loan application data of individual borrowers including name, address, social security number, date of birth, credit and bank account information. The vendor has informed Freddie Mac that it has not found any evidence that personal information, which was encrypted as required by Freddie Mac's contract with the vendor, was accessed or taken from its systems by the attackers. Nevertheless, Freddie Mac sent notification letters out to affected borrowers to explain what happened, what information was involved, what Freddie Mac has done and what affected borrowers can do to protect their continued privacy. In addition, Freddie Mac is offering a complimentary two-year subscription to Experian's identity theft and credit monitoring services.

Further information about what Freddie Mac has done and is recommending to the individuals in question can be found in the enclosed notification letter that Freddie Mac sent to 596 Washington residents.

State of Washington
Office of the Attorney General
July 7, 2020
Page 2

If you have any questions, please contact Howard S. Lindenberg, Vice President & Deputy General Counsel, Freddie Mac Legal Division, 8200 Jones Branch Drive, McLean, VA 22102, Howard_Lindenberg@freddiemac.com, (703) 903-2485.

Regards,

A handwritten signature in blue ink, appearing to read "G. T. Parks".

Gregory T. Parks

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 7, 2020

F6293-L01-0000001 P001 T00001 *****MIXED AADC 159
SAMPLE A SAMPLE - L01 ALL OTHER STATES
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Re: Mortgage Loan on property address
Notice of Data Breach

Dear Sample A Sample:

We are writing to notify you of a data security incident suffered by one of our due diligence vendors that we hired to perform services on some of our loans, including yours, and to advise you of some services we are offering to you at no charge to help protect your continued privacy. At this time, we have no reason to believe that your personal information has been accessed or used inappropriately, but we are writing this letter to tell you what happened, what information was involved, what we have done and what you can do to protect your continued privacy.

First, we'd like to explain why we have your personal information. Mortgage lenders often sell mortgage loans after they have made them. Selling the loans replenishes their funds and enables them to maintain a continuous flow of mortgage funding for new loans. In your case, your mortgage loan was sold to us, the Federal Home Loan Mortgage Corporation ("Freddie Mac"). Because you make or have made your mortgage payments to a different company, you probably haven't had direct interactions with Freddie Mac. The company that you make your mortgage payments to (which may be the lender who originally made the loan to you) is responsible for processing your payments and providing you with customer service. The fact that you are receiving this letter from us does not mean that there has been any change in your mortgage or your relationship with that other company.

What Happened?

We recently learned that, earlier this year, a vendor we hired to perform due diligence services on some of our loans, experienced a ransomware attack on its systems. Because the incident left the vendor's system inaccessible to the vendor, the vendor does not know all details of the incident or the information affected.

0000001



What Information Was Involved?

While we have no indication that your personal information was accessed or used inappropriately, we have determined that your information, including your loan application data (e.g., name, address, social security number, date of birth, credit and bank account information), was on the vendor's systems at the time of the incident. The vendor has informed us that it has not found any evidence that your personal information, which was encrypted as required by our contract with them, was accessed or taken from its systems by the attackers. However, given the nature and circumstances of the attack, we decided, as a precautionary measure, to make credit monitoring available to you at no cost.

What We Are Doing

To help protect your identity, we are offering a complimentary two-year subscription to Experian® IdentityWorksSM, a credit monitoring and identity theft protection service provided by Experian®. If you would like to accept our offer, please follow the steps below:

- Ensure that you enroll by: October 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: ABCDEFGHI

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 **877-890-9332** by **October 31, 2020**. Please be prepared to provide engagement number DB21040 as proof of eligibility for the identity restoration services by Experian.

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require you to sign up for Experian IdentityWorks. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do

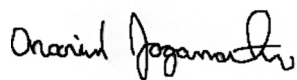
The attached Reference Guide describes additional steps that you can take to protect against potential threats to your privacy and information security. We encourage you to read and follow these steps.

For More Information

Freddie Mac is here to help you if you have any further questions or concerns. If you have questions or concerns, please call 1.800.373.3343 and select option #2, Monday through Friday, 8:30 a.m. to 7:00 p.m., Eastern Time.

Please know that Freddie Mac takes this matter very seriously and we apologize for any concern and inconvenience this may cause you.

Sincerely,



Aravind Jagannathan

Vice President, Single-Family Chief Data Officer

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don’t recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have 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> or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com

TransUnion Fraud Victim Assistance Division www.transunion.com
P.O. Box 2000
Chester, Pennsylvania 19016

The credit bureaus may require that you provide proper identification prior to honoring your request. In order 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 (5) 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 either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov



For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office	NYS Department of State's Division of
Bureau of Internet and Technology	Consumer Protection
(212) 416-8433	(800) 697-1220
https://ag.ny.gov/internet/resource-center	https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.