BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

October 27, 2021

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Primary Residential Mortgage, Inc. ("PRMI") to notify you of a security incident involving 1,712 Washington residents. PRMI is a private residential mortgage lender headquartered in Salt Lake City, Utah.

On August 8, 2021, PRMI identified and addressed a data security incident involving unauthorized access to some of its computer systems. Upon discovering the incident, PRMI took immediate action, and brought certain servers offline to secure the environment. PRMI also initiated a thorough investigation, notified law enforcement and engaged third-party cybersecurity firms to assist and further enhance the security of PRMI systems.

The investigation determined that an unauthorized party accessed or acquired certain data that was stored on PRMI's systems during the incident. The data was reviewed, and, on September 27, 2021, determined that some of the data included the personal information of some individuals affiliated with PRMI including a limited number of borrowers' and employees' personal information. The type of information identified includes the individuals' names, Social Security numbers, driver's license numbers and state or government identification numbers.

On October 22, 2021, PRMI will begin mailing notification letters to the 1,712 Washington residents pursuant to Wash. Rev. Code § 19.255.010.[1] A copy of the notification letter is attached.

[1] This report does not waive PRMI's objection that Washington personal jurisdiction over it related to any claims that may arise from this incident.

PRMI has established a dedicated, toll-free call center where individuals may obtain more information regarding the incident and is offering affected individuals complimentary identity protection services.

To help prevent something like this from happening again, PRMI has implemented additional security and controls to its computer systems.

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

Sincerely,

M. Scott Koller

M. Scott Koller
Partner

Enclosure

PRMI | Primary Residential Mortgage, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-989-3937
Or Visit:
https://response.idx.us/prmi
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

October 27, 2021

Dear <<FirstName>> <<LastName>>:

We are writing to inform you of an incident that may have involved some of your information. This letter explains the incident, measures we have taken, and provides some steps you may consider taking in response.

What Happened?
On August 8, 2021, we identified and addressed a data security incident involving unauthorized access to some of our systems. Upon discovering the incident, we took immediate action, and brought certain servers offline to secure the environment. We also initiated a thorough investigation, notified law enforcement, and third-party cybersecurity firms were engaged to assist.

What Information Was Involved?
Our investigation determined that an unauthorized party accessed or acquired certain data that was stored on our systems during the incident. On September 27, 2021, we determined that some of the data included the personal information of some individuals affiliated with PRMI, including a limited number of borrowers and employees. The type of information identified includes individuals' names, Social Security numbers, driver's license numbers and state or government identification numbers.

What Are We Doing?
In response to the incident, we have taken steps to help prevent a similar incident in the future including implementing additional security safeguards. In an abundance of caution, we are offering you a complimentary one-year membership to credit monitoring and identity theft protection services through IDX. IDX identity protection services includes 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Please note the deadline to enroll is January 27, 2021.

What You Can Do.
We encourage you to sign up for the complimentary credit monitoring service and to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity over the next 12 to 24 months. If you see any unauthorized activity, immediately alert the financial institution and consumer reporting agencies. For more information on IDX, including instructions on how to activate your complimentary membership as well as some additional steps you can take to help protect yourself, please see the pages following this letter.

For More Information.
If you have any questions, please call 1-833-989-3937, Monday through Friday, 7:00 a.m. to 7:00 p.m. Mountain Time.

Sincerely,

Charlie Brown

Charlie Brown
Director of Enterprise Risk Management

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/prmi and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-989-3937 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 over the next 12 to 24 months. 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 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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, 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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Primary Residential Mortgage, Inc., 1480 N 2200 W Salt Lake City, UT 84116, 1-800-255-2792.

Maryland: 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

New York: You may contact and obtain information from these state agencies: *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; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 1,266 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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 above. You also have a right to place a security freeze on your credit report, as described above.

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). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, 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.