

December 15, 2023

VIA E-MAIL (attorneygeneral@doj.nh.gov)

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Nationstar Mortgage LLC (dba Mr. Cooper) Data Security Incident

To the New Hampshire Attorney General's Office:

We are contacting you on behalf of our client, Nationstar Mortgage LLC (dba Mr. Cooper)¹, about a data security incident that involved the personal information of approximately 77,568 residents of New Hampshire. We will begin mailing notification letters to those individuals on or about December 15, 2023, substantially in the same form as the letter attached here. Please note that by submitting this notice, Mr. Cooper does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

What Happened

On October 31, 2023, Mr. Cooper detected suspicious activity in certain network systems. Immediately upon detection, Mr. Cooper initiated response protocols, launched an investigation with the assistance of cybersecurity experts to determine the nature and scope of the incident, and contacted law enforcement. Mr. Cooper also made the decision to shut down its systems to contain the incident and in an effort to protect customers' information.

Through the investigation, Mr. Cooper determined that there was unauthorized access to certain systems between October 30, 2023 and November 1, 2023. During this period, Mr. Cooper identified that files containing personal information were obtained by an unauthorized party. The personal information in the impacted files included . For a very limited subset of individuals,

were also contained in the impacted files.

¹ Mr. Cooper's sister brands also include RightPath Servicing, Rushmore Servicing, and Champion Mortgage.

December 15, 2023

Page 2

Steps to Protect Your State Residents

Mr. Cooper is providing all current and former customers with access to credit monitoring services at no charge for a period of . These services provide individuals with same-day alerts when changes occur to their credit file for 24 months from the date of enrollment. Mr. Cooper is also providing individuals with proactive fraud assistance to help with any questions individuals may have. The services are provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

In addition to the complimentary identity theft protection and credit monitoring services, Mr. Cooper is also providing all current and former customers with (i) information on how to place a fraud alert and security freeze on one's credit file; (ii) the contact details for the national consumer reporting agencies; (iii) information on how to obtain a free credit report; (iv) a reminder to remain vigilant for incidents of fraud and identity theft; and (v) a reminder to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Lastly, Mr. Cooper is also notifying regulators as required.

Upon learning of this security incident, Mr. Cooper immediately took steps to identify and remediate the incident, including locking down its systems, changing account passwords, and restoring its systems. Mr. Cooper initiated a detailed review to identify personal information contained in the impacted files. Mr. Cooper is monitoring the dark web, and to date, has not seen any evidence that the data related to this incident has been further shared, published, or otherwise misused. Mr. Cooper is also further enhancing the security of its systems.

Contact Information

If you have any further questions regarding this incident, please do not hesitate to contact me either by telephone at

Sincerely,

Michelle A. Reed

Mr. Cooper
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

December , 2023

Notice of Data Breach

Dear

Nationstar Mortgage LLC (dba Mr. Cooper) writes to inform you of a data security incident at Mr. Cooper that may have involved some of your personal information. If you are not familiar with the Mr. Cooper brand:

- Your mortgage may have been previously acquired or serviced by Nationstar Mortgage LLC or Centex Home Equity;
- Your mortgage is or was serviced by a sister brand¹;
- Mr. Cooper may be or previously was the servicing partner of your mortgage company; or
- You previously applied for a home loan with us.

Although we have no evidence at this time that your information has been misused for identity theft or fraud as a result of this incident, we are contacting you to explain the circumstances of this event, and to provide information about the service we will provide to help you protect yourself.

What Happened?

On October 31, 2023, Mr. Cooper detected suspicious activity in certain network systems. Immediately upon detection, we initiated response protocols, launched an investigation with the assistance of cybersecurity experts to determine the nature and scope of the incident, and contacted law enforcement. We also made the decision to shut down our systems to contain the incident and in an effort to protect our customers' information. Through our investigation, we determined that there was unauthorized access to certain of our systems between October 30, 2023 and November 1, 2023. During this period, we identified that files containing personal information were obtained by an unauthorized party.

What information was Involved?

The personal information in the impacted files included your

What We Are Doing.

We take the security of the data entrusted to us very seriously. Upon learning of this incident, we immediately took steps to identify and remediate it, including locking down our systems, changing account passwords, and restoring our systems. We initiated a detailed review to identify personal

¹ Sister brands include: RightPath Servicing, Rushmore Servicing, Greenlight Financial Services, and Champion Mortgage

information contained in the impacted files as part of the incident. We are monitoring the dark web and have not seen any evidence that the data related to this incident has been further shared, published, or otherwise misused. We are also further enhancing the security of our systems to help prevent incidents like this from happening in the future.

To help relieve concerns following this incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts when changes occur to your credit file for 24 months from the date of enrollment. This alert is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do.

We encourage you to enroll in free identity protection services by logging on to www.mytrueidentity.com and following the instructions provided. When prompted, please provide the following unique code to receive services: . Please note that we are unable to independently take this step for you. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity. **You will need to reference the enrollment code provided in this letter when enrolling, so please do not discard this letter.**

In addition to enrolling in the complimentary identity protection and credit monitoring services described above, we encourage you to review the enclosed "Recommended Steps to Help Protect Yourself," which describes other steps you can take to help protect your personal information. These steps include recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information.

If you have any questions or would like to learn additional information about this incident, call the Mr. Cooper Cyber Incident Response Line, supported by TransUnion at 1-833-960-4745, available Monday through Friday 8:00am to 8:00pm ET. We deeply regret that this incident has occurred and sincerely apologize for any concerns or inconvenience that it may cause.

Sincerely,

Jay Jones Jr.
Executive Vice President of Servicing, Mr. Cooper

Recommended Steps to Help Protect Yourself

Contact information for the three nationwide credit reporting agencies is:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-866-349-5191
- **Experian**, PO Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-916-8800

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/contact-us
888-378-4329

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
experian.com/freeze
888-397-3742

TransUnion Consumer Solutions

P.O. Box 160
Woodlyn, PA 19094
freeze.transunion.com
800-916-8800

More information can also be obtained by contacting the Federal Trade Commission listed below.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For California residents: This notification was not delayed by law enforcement. Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Colorado, Georgia, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For Connecticut residents: The Attorney General may be contacted at: Office of the Attorney General, 55 Elm Street, Hartford, CT 06106; www.ct.gov/ag; 1-860-808-5318.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Kentucky residents: You may contact the Office of the Attorney General of Kentucky at 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland residents: The Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD, 21202; www.marylandattorneygeneral.gov; 1-888-743-0023; consumer hotline (410) 528-8662.

For Massachusetts residents: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. There is no charge to place a security freeze on your credit report.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. The Attorney General may be contacted at: Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301-4096; 503-378-6002.

For Rhode Island residents: The Attorney General may be contacted at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. This incident affected approximately 47,818 Rhode Island residents.

For Vermont residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For Washington, DC residents: You may contact the Attorney General at: Office of the Attorney General, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; <https://oag.dc.gov/>; 1-202-727-3400 to receive additional information about steps to take to avoid identity theft.