



RECEIVED

MAR 06 2026

CONSUMER PROTECTION

March 2, 2026

New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Sir/Madam:

On behalf of US Mortgage Corporation, a mortgage company based in New York, I am writing to inform your office about a security event that affected 4 New Hampshire residents. The event involved unauthorized activity on our network. We promptly began working with cybersecurity experts to investigate and identify the impacted data. On March 5, 2026, we are providing substitute notice and mailing written notice to affected individuals.

On May 14, 2025, US Mortgage detected a cybersecurity event involving unauthorized activity in portions of the company's computer network. We promptly engaged outside counsel who then notified law enforcement and retained cybersecurity experts to conduct a privileged forensic investigation.

As the investigation progressed, we engaged in restoration and remediation efforts. For example, we restored files from backups and further bolstered our security through measures such as: resetting passwords, rebuilding the affected systems in a new clean environment, and adopting additional technical safeguards. Those enhancements built on our existing security infrastructure, which included measures such as firewalls, multifactor authentication, and secure backups.

The investigation determined that this was a ransomware event with unauthorized activity starting on May 13, 2025, and ending on May 14, 2025. The cybersecurity experts also identified the impacted files, and we engaged a data-review firm to assess those files. The data-review firm provided their results on October 23, 2025. Based on our counsel's

CORPORATE OFFICE: 201 OLD COUNTRY ROAD • SUITE 140 • MELVILLE, NY 11747 • TEL: (631) 580-2600 • NMLS# 3901

Licensed Mortgage Banker-NYS Department of Financial Services-Licensed Nationwide except HI State Banking Departments/Regulators.

WWW.USMORTGAGE.COM

| Page 1 of 2



review of the data-mining results, we have reason to believe this event impacted the following types of personal information: name, contact information, government identification numbers (such as a driver's license or Social Security number), financial account information, and limited medical or insurance information. Upon receiving the report in October, we worked with our counsel to assess notification obligations and locate current addresses for impacted individuals. We completed that process on February 11, 2026, and we are mailing notices on March 5, 2026.

We have included templates of the notices we are providing to the impacted individuals. Those notices include complimentary credit monitoring, via Experian IdentityWorks, for any individual with a Social Security or driver's license number impacted by the event.

If you have any questions, please contact Josh Hansen (our outside counsel for this event) at (303) 285-5306 or jahansen@shb.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Scott A. Milner', is written over a light blue horizontal line.

Scott A. Milner
President



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

US Mortgage Corporation is writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened and what we are doing in response.

What Happened?

On May 14, 2025, we detected suspicious activity in a limited portion of our computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In July 2025, the investigation found that an unauthorized third party gained access to a portion of our computer network from May 13 to May 14, 2025. The investigation identified the files impacted by the event, and then we began working with a data-review firm to analyze those files' contents. We received the data-review results in October 2025. Many of those results did not contain contact information, so we have been working since October to ensure we have accurate contact information for notifying impacted individuals.

What Information Was Involved?

We determined that the impacted files contained some of your personal information, which includes your: <<Breached Elements>>.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance on the next page.

For More Information.

Should you have any questions, you can contact us at (877) 421-8688 Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,
US Mortgage Corporation

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit: www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted <<Rhode Island Count>> Rhode Island residents.