



June 27, 2022

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

RECEIVED
JUL 01 2022
CONSUMER PROTECTION

Nations Lending Corporation is writing to notify you of data security incident involving 15 New Hampshire residents.

IDENTIFICATION OF PARTIES

Nations Lending Corporation is a mortgage lender with its principal place of business located at 4 Summit Park Drive, Suite 200, Independence, OH 44131. The party that experienced the incident subject to this notification is Kaye Smith, Inc. (“Kaye-Smith”) a print and mail company used as a vendor for some loan transactions by Nations Lending. Kaye-Smith has its corporate office located at 4101 Oakdale Ave., SW, Renton, Washington 98057.

NATURE OF THE DATA SECURITY INCIDENT

Sometime in late May 2022, Kaye-Smith was victim of a ransomware attack which froze the data in their systems and made it inaccessible. Kaye-Smith has been restoring its systems and data, but they have not excluded the possibility that the individuals whose malware caused the incident were able to access electronically stored information from the system. Nations Lending received initial notification of an incident from Kaye-Smith on June 3, 2022 and launched its own inquiry to attempt to determine which of our customers’ information might be at risk. At the time of this notification, Nations Lending is not aware of any resulting identity theft, fraud, or financial losses to its customers because of this incident.

NUMBER OF RESIDENTS AFFECTED AND POTENTIALLY AFFECTED INFORMATION

As known at the time of this notification, 15 individuals residing in New Hampshire had personal information that was subject to the incident. Information from the initial disclosure package of the customers’ loan, including documents bearing the customer’s name, address, Social Security number, email, and information about the customer’s assets was involved. The affected individuals will be mailed a notice of the data breach around July 11, 2022. A copy of the notice is attached.

STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Nations Lending has suspended any further transactions with Kaye-Smith and moved print/mail activities in-house while we evaluate other options. Before we resume any business transactions with Kaye-Smith, they would have to pass a complete cybersecurity evaluation and demonstrate that their systems and personnel are hardened against any further attacks. Nations Lending did not report this incident to law enforcement and does not have any information regarding any reporting by Kaye-Smith. Nations Lending does maintain a Written Information Security Plan, but we are not implementing any changes as our systems were not compromised by the attack. Review of Kaye-Smith’ WISP will be conducted prior to resuming any use of their services.

CREDIT MONITORING

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to the customer for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Customers can enroll in the free credit monitoring services until January 21, 2023, and all customers affected can enroll in this service.

Sincerely,

R. Christopher Baker
General Counsel

216-393-6901
christopher.baker@nationslending.com

Enclosure:



<<MemberFirstName>> <<MemberLastName>>

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

<<Address1>>

<<Address2>>

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

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

At the end of May a printing company used as a vendor for mailing some disclosures for loan transactions by Nations Lending was victim of a ransomware attack which froze the data in their systems and made it inaccessible. The company has been restoring its systems, but they have not ruled out the possibility that the individuals whose malware caused the incident were able to access information from the system. Nations Lending received notice from the company early in June and launched its own inquiry to attempt to determine which of our customers' information might be at risk. Your transaction data may have been one of those affected by this attack.

What information was involved?

Information from the initial disclosure package for your loan, including documents bearing your name, address, Social Security number, email, and financial information about your assets.

What we are doing.

We suspended any further transactions with the vendor and switched to processing these print services internally while we evaluate other service providers. Before we resume any business transactions with any print vendor, they will have to pass a complete cybersecurity evaluation and demonstrate that their systems and personnel are hardened against attacks.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by 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.

For more information.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Nations Lending Corporation

Customer Service Department

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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 or call toll free at **1-877-322-8228**.

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 ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont 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).

Fraud Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit 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 5 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, and display your name, current mailing address, and the date of issue.

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 minimize the risks of 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 Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

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

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Three 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.