WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

September 28, 2023

[redacted]

Via First Class Mail Return Receipt Requested

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents MiLEND, Inc., a mortgage broker company based in Alpharetta, Georgia, with respect to a cybersecurity incident that was confirmed by MiLEND, Inc. on August 14, 2023 (hereinafter, the "Incident"). MiLEND, Inc. takes the security and privacy of the information within its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve as a notice of the Incident and to inform you of the steps MiLEND, Inc. has taken in response to the Incident. We have also enclosed hereto a sample copy of the notification letters mailed to the potentially impacted individuals, which includes an offer of complimentary credit monitoring services.

1. Nature of the Incident

On or around August 14, 2023, MiLEND, Inc. was notified by its outside MSP provider that its servers were offline and irresponsive. Upon further investigation, MiLEND, Inc. discovered that its computer network had been accessed and encrypted by an unauthorized user. Upon discovery of the Incident, MiLEND, Inc. immediately engaged cybersecurity experts to conduct a thorough forensic investigation to determine the nature and scope of the suspicious activity. The forensic investigation concluded on September 11, 2023.

The forensic investigation confirmed unauthorized activity to MiLEND, Inc.'s computer systems beginning on July 31, 2023 and concluding on August 15, 2023. Upon confirming unauthorized access to its systems, MiLEND, Inc. initiated a review of the compromised servers to determine

whether personally identifiable information may have been maintained within the impacted computer servers for purposes of notifying those individuals whose sensitive personal information may have been impacted by the Incident. Based on its review of the data maintained within the compromised computer systems, MiLEND, Inc. determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: . The exact elements of personal information that may have been exposed as a result of this incident varies per individual.

Based upon the results of its review, MiLEND, Inc. mailed notification letters to the potentially affected individuals along with credit monitoring services and further instructions on how to protect their personal information.

As of this writing, MiLEND, Inc. has not received any reports of related identity theft since the date of the Incident (August 14, 2023) to the present.

2. Number of New Hampshire residents affected.

MiLEND, Inc. discovered that the Incident may have resulted in unauthorized exposure of information pertaining to seven (7) New Hampshire residents. Notification letters to the individuals were mailed on September 28, 2023, by First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

MiLEND, Inc. is committed to ensuring the security and privacy of all personal information within its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MiLEND, Inc. moved quickly to investigate and respond to the Incident. Specifically, MiLEND, Inc. engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MiLEND, Inc. is taking steps to strengthen its security posture to prevent a similar event from occurring again in the future.

MiLEND, Inc. is also offering of complimentary credit monitoring and identity theft restoration services through TransUnion to all potentially affected individuals residing in New Hampshire to help protect their identity. Additionally, MiLEND, Inc. provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact Information

MiLEND, Inc. remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at .

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Richard J. Bortnick

EXHIBIT A

MiLEND, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

milend INC

[redacted]

September 28, 2023

VIA FIRST-CLASS MAIL

Notice of Data Security Incident

Dear [redacted]:

MiLEND, Inc. is writing to inform you of a recent cybersecurity incident that may have involved your personally identifiable information ("PII"). MiLEND, Inc. takes the privacy of personal information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

0000101033G0500

P

What Happened?

On August 14, 2023, MiLEND, Inc. was notified that its computer network had been impacted by a ransomware incident (the "Incident"). Upon discovery of the Incident, MiLEND, Inc. immediately engaged cybersecurity experts to conduct a thorough investigation to determine the nature and scope of the unauthorized activity. The forensic investigation concluded on September 11, 2023 and confirmed unauthorized access to MiLEND Inc.'s network. Upon confirming unauthorized access to its systems, MiLEND, Inc. initiated a review of the compromised servers to determine whether customers' personal information may have been impacted by the incident. While MiLEND, Inc. could not confirm that personal information was accessed by an unauthorized user, out of an abundance of caution, we are providing notification letters to all individuals whose information was potentially impacted by this Incident.

What Information Was Involved?

The investigation determined that personal information stored within MiLEND Inc.'s computer network was potentially subject to unauthorized access. The potentially accessed data contained within the computer system included personally identifiable information such as your:

Please note, at this time, MiLEND, Inc. has not received any reports that personal information has been misused as a result of this Incident.

What We Are Doing

MiLEND, Inc. takes the privacy and security of the personal information within its possession very seriously. We are working with cybersecurity experts to investigate and closely monitor the situation and enhance MiLEND, Inc.'s network security in order to prevent a similar event from occurring in the future.

In order to address any individual concerns and mitigate any exposure or risk of harm 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 for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification 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 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

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/milend** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. You can sign up for the credit monitoring service within ninety (90) days of the date of this letter. Please note that when signing up for credit monitoring services, you may be asked to verify personal information to confirm your identity. Enrollment for credit monitoring services requires an internet connection and e-mail account, and might not be available for individuals under the age of eighteen (18). Enrolling in this service will not affect your credit score.

Although MiLEND, Inc. is not aware of any instances of misuse of any personal information, we recommend that individuals take advantage of the complimentary services that are being offered. We also encourage individuals to remain vigilant and review the enclosed addendum titled "*Additional Important Information*" outlining additional steps you can take to protect your information.

For More Information

Please know that the protection of your personal information is a top priority, and MiLEND, Inc. sincerely apologizes for any concern or inconvenience that this matter may cause you. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call 1- 833-413-3094 during the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday (excluding U.S. national holidays).

MiLEND, Inc. sincerely regrets any inconvenience or concern that this matter may cause and remains dedicated to ensuring the privacy and security of all information within its control.

Sincerely,

MiLEND, Inc.

Additional Important Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Security Freeze: You have the right 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to 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.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island*: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov