Kennedys

22 Vanderbilt Ave.
Suite 2400
New York, NY 10017

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 646 625 4030

Daniel.Marvin@kennedyslaw.com

July 15, 2026

Via Web Submission

Attorney General Mike Hilgers
Office of the Nebraska Attorney General
Consumer Affairs Response Team
2115 State Capitol Building
Lincoln, NE 68509

Re: **YouLend US LLC – Notice of Security Breach**

Dear Attorney General Hilgers:

We represent YouLend US LLC ("**YouLend**") an organization headquartered in Atlanta, Georgia, and is an embedded financing provider that partners with technology companies, marketplaces, and e-commerce providers to provide financing products for small and medium-sized businesses. We write in accordance with NEB. REV. STAT. ANN. § 87-802 (2016) to report a data event that involved the personal information of 79 residents of Nebraska. Respectfully, please note that in making this submission, YouLend does not waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction. This notice may be supplemented with new information learned after submission.

On June 9, 2026, YouLend discovered suspicious activity within its network environment, which was later confirmed to be ransomware. The threat actor is unknown. Upon discovery, YouLend took immediate action to secure its network environment, which included retaining our law firm. We engaged a cybersecurity forensics firm to assist with the investigation, remediation efforts, and for the provision of rendering legal advice. YouLend also reported the incident to law enforcement. On June 9, 2026, YouLend learned that certain files were taken from its network. YouLend commended a detailed review of the files involved to understand the data potentially involved and to whom it belonged to. YouLend determined on June 9, 2026, that certain individuals were involved in the dataset, and confirmed on July 10, 2026, that 79 Nebraska residents were included.

Kennedys

YouLend notified 79 Nebraska residents via U.S. mail on July 15, 2026. The data involved included first and last names in combination with Social Security number, financial account information and/or payment card information, and Tax ID number. Notified individuals were offered an opportunity to enroll in twelve (12) months of complimentary credit monitoring and identity protection services through CyberScout, a TransUnion company specializing in fraud assistance and remediation services. The services include single bureau credit monitoring, dark web monitoring, access to a $1M insurance reimbursement policy, and fully managed identity theft recovery services. YouLend also set up a professional call center through CyberScout to assist notified individuals with credit monitoring enrollments and to answer inquiries regarding the event. A sample copy of the notification letter is enclosed.

YouLend has taken steps in response to the incident to help mitigate the risk of a similar incident occurring in the future, including reviewing its existing security policies and protections and adopting additional security to safeguard against evolving threats moving forward.

This notice provides your Office with all information necessary to comply with Nebraska law. Should you have any further questions, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Daniel Marvin

Daniel Marvin

Partner for Kennedys

Cc: Lauren Stinger, Esq.

Enclosure: Sample Consumer Notification Letter

Exhibit A

YouLend US LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

YOULEND

[redacted]

July 15, 2026

Re: Notice of Data Privacy Event

Dear [redacted]:

YouLend US LLC writes to notify you of a data privacy event that involved your personal information.

What Happened? On June 9, 2026, we received alerts of a disruption to our computer network. Upon identifying the disruption, we launched an immediate investigation and engaged outside cybersecurity specialists to assist. The investigation determined that our network was accessed without authorization between June 5, 2026 to June 9, 2026, and that certain files containing your personal information, as described below, was acquired.

What Information Was Involved? The personal information included your Name, Date of Birth, Social Security number. We have no evidence of misuse of any personal information for fraud or identity theft.

What We Are Doing. Upon becoming aware of the disruption, we took steps to secure our systems. We also reported the incident to federal law enforcement and other authorities. As an added precaution, we are offering 12 months of complimentary credit monitoring and identity protection services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Instructions for how to enroll in these services are below.

What You Can Do. Once again, we have no evidence of misuse of any personal information for fraud or identity theft. Generally, it is a best practice to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing and monitoring your account statements and free credit reports for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider.

For More Information. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information*," for additional resources. We thank you for your understanding. If you have any other questions, you may contact us at 1-844-671-5730 8:00 am - 8:00 pm ET, Monday through Friday, excluding US Holidays for further assistance.

Sincerely,

YouLend US LLC

STEPS YOU MAY TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score** services at no charge. These services provide you with alerts for **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 identity suspicious activity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified below.

Credit Freeze Instructions: As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	Experian	Equifax
1-800-680-7289 www.transunion.com	1-888-397-3742 www.experian.com	1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.A complaint may be filed with the FTC online at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, or https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico residents, the New Mexico Attorney General may be contacted at the New Mexico Department of Justice, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501; (505) 490-4060; or https://nmdoj.gov/.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Justice Building, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; or https://www.doj.state.or.us/.

For *Rhode Island residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov. The number of Rhode Island residents whose information was involved in this incident is 89.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf. or www.ftc.gov.