

EXHIBIT 1

By providing this notice, Texollini Inc. (“Texollini”) does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 18, 2026, Texollini became aware of suspicious activity and encryption of certain data on within its technical environment. Texollini promptly took measures to secure its network, to mitigate risk of further activity and launched an investigation with the help of third-party forensic specialists to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to the Texollini network between February 16, 2026, and February 18, 2026, during which time certain files were copied and taken from the network.

Texollini underwent a thorough and time-consuming effort to review the files potentially copies to determine whether the files contained any sensitive information. This process was resource intensive and involved multiple steps to ensure the accuracy and completeness of the review. On April 28, 2026, Texollini completed its review and determined that personal information was impacted by this event.

The information that could have been subject to unauthorized access for the Nebraska resident includes name, Social Security number, driver’s license number, and financial account information.

Notice to Nebraska Resident

On May 29, 2026, Texollini provided written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Texollini moved quickly to investigate and respond to the incident, assess the security of Texollini systems, and identify potentially affected individuals. Texollini is also working to implement additional safeguards and training for its employees. Texollini is providing access to credit monitoring services for twelve (12) months through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

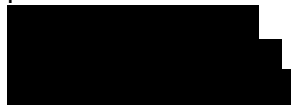
Additionally, Texollini is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Texollini is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

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



P



May 29, 2026

NOTICE OF DATA BREACH

Dear [REDACTED]:

Texollini, Inc., ("Texollini") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? Texollini recently learned of anomalous activity within our environment. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that our environment was subject to unauthorized access from February 16, 2026 to February 18, 2026, and certain files were accessed by the unauthorized actor. Upon completion of the forensic investigation, we conducted an internal review of those files to determine whether they contained any sensitive information. We completed this review on April 28, 2026, at which time we determined sensitive information was contained within the impacted files.

What Information Was Involved? Texollini determined that the following information related to you was located within one of the accessed files: your full name, Social Security number, driver's license number, U.S. Alien Registration number, and financial account information..

What We Are Doing. We take the security of information in our care and our systems very seriously. As soon as we became aware of the activity, we launched an investigation with the support of third-party forensic specialists to confirm the security of our network. We have since taken steps to strengthen our environment, including implementation of additional safeguards and enhanced monitoring.

In an abundance of caution, Texollini is providing you with access to 12 months of credit monitoring and identity protection services through TransUnion at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Further Protect Your Information*. Please note that you must complete the enrollment process for yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Further Protect Your Information*, which includes additional information on what you can do to protect your information against misuse, should you feel it necessary to do so.

000010102G0500

P

For More Information. Texollini understands you may have questions about this event not addressed in the letter. To ensure your questions are answered in a timely manner, please call 1-800-405-6108 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. You may also contact us at PrivacyEvent@Texollini.com.

Sincerely,

Texollini, Inc.

Steps You Can Take To Further Protect Your Information

Enroll in Monitoring Services

In response to the 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 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, 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]. 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, (1-877) 322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

00001020280000

P

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
(1-888) 298-0045	(1-888) 397-3742	(1-833) 799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; (1-877) ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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