Jennifer S. Stegmaier
312.821.6167
jennifer.stegmaier@wilsonelser.com

May 11, 2026

Via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Cybersecurity Incident Involving Lamb-Star Engineering, LLC

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Lamb-Star Engineering, LLC ("Lamb-Star"), located at 3801 Parkwood Boulevard, Suite 550, Frisco, Texas 75034, with respect to a recent data security incident that may have resulted in unauthorized access to some individuals' personal information ("Incident"). Lamb-Star takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that Lamb-Star has taken in response to the Incident. We have also enclosed hereto a sample of the notification letter that to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On or about January 20, 2026, Lamb-Star detected suspicious activity on its system. Upon discovery of this incident, Lamb-Star immediately disconnected the affected systems and remote access to the network. Lamb-Star promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about March 4, 2026, and determined that there was unauthorized access to Lamb-Star's network and that certain data was accessed without authorization on January 20, 2026.

Based on these findings, Lamb-Star began reviewing the affected files to identify the specific individuals and the types of information that may have been compromised. This process was necessary to provide accurate information and notice to potentially impacted individuals. Lamb-Star completed its list of individuals to notify on or about April 29, 2026.

2. Number of State residents affected.

Lamb Star identified 4 residents of Maine potentially affected by this Incident. Notification letters were mailed to these individuals on May 11, 2026, by United States Postal Service 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.

Data privacy and security are among Lamb-Star's highest priorities, and it is committed to doing everything it can to protect the privacy and security of personal information in its care. Upon discovery of the incident, Lamb-Star moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts. Specifically, Lamb-Star promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident.

In addition, Lamb-Star has also taken additional technical and administrative steps to further enhance the security of its systems and customer data to mitigate the risk of future harm. Specifically, Lamb-Star has fully rebuilt all servers, patched identified and unidentified vulnerabilities, applied necessary security updates, strengthened access control systems, implemented enhanced monitoring and detection methods, reset all user and service account passwords, initiated new password managers, updated and implemented new security policies, updated and enhanced backup policies and infrastructure, enhanced backup methods, timelines, and repositories, enhanced user cybersecurity training and attack simulations.

Lamb-Star has no knowledge of any instances of identity theft or fraud resulting from this incident. However, as a precautionary measure, Lamb-Star is offering credit monitoring and identity theft protection services through Kroll, a data breach and recovery services expert, to all affected individuals at no cost. Kroll's identity protection services include 12 months of credit and fully managed identity theft recovery services. With this protection, Kroll will help them resolve issues if their identity is compromised.

4. Contact information

Lamb-Star remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 312.821.6167 or jennifer.stegmaier@wilsonelser.com.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Jennifer S. Stegmaier

EXHIBIT A

Sample Individual Notice Letter

Lamb-Star Engineering, LLC

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



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

<<b2b_text_1 (Re: Notice of Data Security Incident involving Lamb-Star Engineering, LLC/ Re: Notice of Data Breach involving Lamb-Star Engineering, LLC)>>

Dear <<First_name>> <<Last_name>>,

Lamb-Star Engineering, LLC ("Lamb-Star"), located at 3801 Parkwood Boulevard, Suite 550, Frisco, Texas 75034, is writing to inform you of a data security incident that may have involved your personal information. We take the protection of your personal information very seriously and are sending you this notice to tell you what happened, what information was involved, what we have done in response, what you can do in response to this incident, and what resources are available to help protect against the potential misuse of sensitive personal information, if you feel it is appropriate.

What Happened?

On or about January 20, 2026, Lamb-Star detected suspicious activity on its system. Upon discovery of this incident, Lamb-Star immediately disconnected the affected systems and remote access to the network. Lamb-Star promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about March 4, 2026, and determined that there was unauthorized access to Lamb-Star's network and that certain data was accessed without authorization on January 20, 2026.

Based on these findings, Lamb-Star began reviewing the affected files to identify the specific individuals and the types of information that may have been compromised. This process was necessary to provide accurate information and notice to potentially impacted individuals. Lamb-Star completed its list of individuals to notify on or about April 29, 2026. We determined that some of your personal information may have been affected by the incident.

What Information was Involved?

The personal information that may have been subject to unauthorized access includes: <<b2b_text_2 (data elements)>><<b2b_text_3 (data elementscontinued)>>. Please note the information impacted varies for each potentially impacted individual.

What We Are Doing.

Data privacy and security are among Lamb-Star's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the incident, Lamb-Star moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts. Specifically, Lamb-Star promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident.

In addition, Lamb-Star has also taken additional technical and administrative steps to further enhance the security of its systems and customer data to mitigate the risk of future harm. Specifically, Lamb-Star has fully rebuilt all servers, patched identified and unidentified vulnerabilities, applied necessary security updates, strengthened access control systems, implemented enhanced monitoring and detection methods, reset all user and service account passwords, initiated new password managers, updated and implemented new security policies, updated and enhanced backup policies and infrastructure, enhanced backup methods, timelines, and repositories, enhanced user cybersecurity training and attack simulations.

Lamb-Star has no knowledge of any instances of identity theft or fraud resulting from this incident. However, as a precautionary measure, Lamb-Star is offering identity monitoring services through Kroll, a data breach and recovery services expert. Kroll's identity monitoring services include: <<ServiceTerminMonths>> months of credit and fully managed identity theft recovery services. With this protection, Kroll will help you resolve issues if your identity is compromised.

What You Can Do.

We encourage you to enroll in the complimentary identity monitoring that we are offering to you at no cost. Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. You can find more information on steps to help protect yourself against identity theft identity theft in the enclosed *Additional Resources to Help Protect Your Information* sheet.

If your Social Security number is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these actions:

- Obtain an Identity Protection PIN (IP PIN) to prevent tax-related identity theft. The IP PIN is a 6-digit code that authenticates your identity, preventing the filing of fraudulent returns in your name. You can apply for a PIN online at IRS.gov.
- Respond immediately to any IRS notice: call the number provided.
- If your e-filed return is rejected because of a duplicate filing under your Social Security number, or if the IRS instructs you to do so, visit irs.gov/victimassistance to complete Form 14039, Identity Theft Affidavit, attach it to the back of your completed paper tax return and mail to the IRS location based upon the state you reside. You also have the option to submit the Form 14039 online and mail your paper return separately.
- Visit IdentityTheft.gov for steps you should take right away to protect yourself and your financial accounts.

How do I enroll for the free services?

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

For More Information.

If you have any questions or concerns not addressed in this letter, please call (844) 403-4632 (toll free) Monday through Friday, during the hours of 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Lamb-Star sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Lamb-Star Engineering, LLC

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative, you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state, and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.