

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

November 7, 2025

Re: Notice of Data Security Incident

Dear Attorney General Mike Hilgers:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Logis-Tech, LLC (“Logis-Tech”) in connection with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with your data breach notification statute. By providing this notice, Logis-Tech does not waive any rights or defenses regarding the applicability of state law, the applicability of the state data breach notification statute, personal jurisdiction, or any other potentially applicable rights or defenses.

1. Nature of the Incident

On October 31, 2025, Logis-Tech learned that personal information may have been impacted as a result of an attack on the Logis-Tech network discovered on August 6, 2025. Upon discovery of suspicious network activity associated with the attack, Logis-Tech promptly took steps to secure its network and began an investigation to determine the nature and scope of the issue. In so doing, Logis-Tech engaged leading digital forensics specialists to assist through which Logis-Tech determined that certain files were accessed or acquired without authorization. Upon review of those files, Logis-Tech identified certain personal information contained therein and then worked diligently to identify address information sufficient to effectuate notification. Please note that Logis-Tech has no evidence of misuse, or attempted misuse, of any potentially impacted information.

2. Information Involved

The information potentially impacted in connection with the incident for residents of Nebraska may have included name as well as Social Security number.

3. Notification to Affected Individual(s)

On November 7, 2025, a notification letter was sent to one (1) Nebraska resident. The notification letter provides resources and a description of steps that notified individuals can take to help protect their information. The notification letter also offers individuals the opportunity to enroll in complimentary identity protection services,

including credit monitoring, and identity remediation services, as well as a phone number to call, should any individual have questions about the incident. A sample of the notification letter provided is included with this correspondence.

4. Steps Taken Relating to the Incident

Upon discovering the event, Logis-Tech moved quickly to investigate, respond, and identify potentially affected individuals. The Incident was reported to the FBI and Logis-Tech will fully cooperate with any resulting investigation. Logis-Tech is providing access to credit monitoring services for twelve (12) months, through TransUnion, to notified individuals at no cost.

Additionally, Logis-Tech is providing notified 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. Logis-Tech is providing notified 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 and law enforcement to report attempted or actual identity theft and fraud.

Logis-Tech remains dedicated to protecting all information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,



Alyssa Watzman
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

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

<<Name>>
<<Street Address>>
<<City / State / Zip>>

November 07, 2025

Re: Notice of Data Security Incident

Dear <<Name>>:

Logis-Tech, LLC (“Logis-Tech”) is writing to notify you of an incident which may have impacted your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including information regarding the complimentary services we are making available to you.

What Happened? On October 31, 2025, we learned that your personal information may have been impacted as a result of an attack on our network discovered on August 6, 2025. Upon discovery of suspicious network activity, we promptly took steps to secure our network environment and began an investigation to determine the nature and scope of the issue. In so doing, we engaged leading digital forensics specialists to assist through which we learned that certain files were accessed or acquired without authorization. Upon review of these files, we determined that certain personal information was contained therein and then worked diligently to identify address information sufficient to notify potentially impacted individuals. Notably, we are not aware of any actual or attempted misuse of this information.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as <<Elements>>.

What Are We Doing? As soon as we discovered the activity, we took the steps discussed above. In order to reduce the likelihood of a similar incident occurring in the future, we took additional measures to enhance the security of our network environment. In addition, the incident was reported to the FBI and Logis-Tech will fully cooperate with any resulting investigation.

We are also 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, 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: << Code >>. 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.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. It is recommended that you review current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

You can contact TransUnion representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to the TransUnion designated call center at 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays, and they will be happy to provide you with additional information.

Sincerely,

Logis-Tech, LLC

1440 N Edgewood St.
Suite 178
Arlington, VA 22201

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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 above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.