

March 27, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown,

Butzel Long represents Sierra Lobo, Inc. ("SLI"), an engineering services company located in Ohio. I am writing to provide notification of a security incident in accordance with Maryland's data breach notification statute.

I. Nature of Security Incident

On February 23, 2024, SLI noticed unusual IT activity and immediately shut down its servers. SLI engaged cybersecurity forensic experts and legal counsel to assist with the investigation and remediation of the incident. Based upon the forensic investigation, it is believed this cybersecurity incident commenced through the exploitation of a vulnerability in SLI's remote access tool, ScreenConnect. It is estimated that approximately two hundred and thirteen (213) Maryland residents were affected by this cybersecurity incident. Despite the immediate application of a patch addressing the identified vulnerability, subsequent investigations suggest that the system remained compromised, indicating that the initial breach occurred prior to the patch application. SLI believes that this vulnerability was the likely point of entry, enabling unauthorized access to our network. Working diligently with forensic experts and cybersecurity counsel, SLI discovered that on March 14, 2024, the unauthorized access resulted in the disclosure of data contained on SLI's servers. SLI believes that this access included the personal information of SLI's current and former employees, which may have included full names and one or more of the following: address, date of birth, driver's license number, full or partial Social Security Number and passport details. As a result, personal information may have

been exposed to others. Please be assured that SLI has taken every step necessary to contain and address this incident.

II. Notification of Affected Individuals

On March 28, 2024, SLI will begin providing written notices of this incident to two hundred and thirteen (213) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A.

III. Steps Taken to Address the Incident

SLI has taken additional steps to strengthen the security of the environment and to ensure that future incidents are unsuccessful, including implement the recommendations of the forensics experts. In addition, the FBI and the US Cybersecurity and Infrastructure Security Agency (CISA), were notified of the incident on February 23, 2024, and are assisting us with our investigation. The incident was also reported to the FBI's Internet Crime Complaint Center (IC3) on February 29, 2024.

SLI and the forensic team have taken extensive mitigation actions including system restoration from trusted backups, implementation of Multi-Factor Authentication (MFA), and a comprehensive review and enhancement of our security posture to address and fortify against such vulnerabilities. Additionally, SLI's IT team has subscribed to the CISA daily email which outlines current vulnerabilities and threats. Password requirements have been strengthened. Finally, additional tools are being deployed to provide defense in depth with a target completion by the end of April. Additionally, we changed password complexity and flushed all passwords, renewed all Kerberos certificate twice and enhanced firewall protections (including geolocation).

To help protect user identities, SLI is offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides users with superior identity detection and resolution of identity theft. SLI has also provided steps for users to activate their memberships.

Users may contact Experian **immediately** regarding any fraud issues, and have access to the following features once enrolled in Experian® IdentityWorksSM: Credit reporting, credit monitoring and fraud detection, identity restoration, theft insurance for unauthorized electronic transfers.

MD Attorney General Anthony Brown
March 27, 2024



VI. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (248) 258-2603 or geroux@butzel.com

Very truly yours,



Debra Geroux

MD Attorney General Anthony Brown
March 27, 2024



EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 28, 2024

L0854-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



Notice of Data Breach

Dear Sample A. Sample,

We are contacting you regarding a data security incident that we discovered on March 14, 2024, that involved certain personal information of Sierra Lobo's employees, including demographic information and other personal information as more fully described below. As a result, your personal information may have been exposed to others. Please be assured that we have taken every step necessary to address the incident. Under Massachusetts law, you have the right to obtain any police report filed regarding 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.

What Happened

On February 23, 2024, we noticed unusual IT activity and immediately shut down its servers. SLI engage cybersecurity forensic experts and legal counsel to assist with the investigation and remediation of the incident. Based upon the forensic investigation, it is believed this cybersecurity incident commenced through the exploitation of a vulnerability in our remote access tool, ScreenConnect. Despite the immediate application of a patch addressing the identified vulnerability, subsequent investigations suggest that the system remained compromised, indicating that the initial breach occurred prior to the patch application. We believe that this vulnerability was the likely point of entry, enabling unauthorized access to our network. Working diligently with our forensic experts and cybersecurity counsel, we discovered on March 14, 2024, that this unauthorized access resulted in the disclosure of data contained on our servers. We believe that this access included the personal information of SLI's current and former employees, which may have included full names and one or more of the following: address, date of birth, driver's license number, full or partial Social Security Number and passport details. As a result, your personal information may have been exposed to others. Please be assured that we have taken every step necessary to contain and address this incident.

SLI has taken additional steps to strengthen the security of the environment and to ensure that future incidents are unsuccessful, including implement the recommendations of the forensics experts. In addition, the FBI and the US Cybersecurity and Infrastructure Security Agency (CISA), were notified of the incident, and are assisting us with our investigation.



What We Are Doing to protect your information:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: July 1, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-3700, Monday through Friday 8am to 8pm CST, closed Saturday and Sunday (excluding major U.S. holidays) by **July 1, 2024**. Be prepared to provide engagement number **B119355** as proof of eligibility for the identity restoration services by Experian. For additional information, please review the attached **Information About Identity Theft Protections**.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-3700. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 833-931-3700.

Sincerely,

April Reeves
Sierra Lobo, Inc.
Corporate Human Resources Manager

Enclosure: Information About Identity Theft Protections

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an 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 by contacting one or more of the three nationwide consumer reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, GA 30374, 1-800-685-1111, www.equifax.com

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

TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For District of Columbia Residents: You may contact the DC Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of District of Columbia

400 6th Street NW, Washington, DC 20001. (202) 727-3400, oag@dc.gov

For Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa

Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164
www.iowaattorneygeneral.gov

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain any 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 North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For Oregon Residents: You may report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice

1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400
<http://www.doj.state.or.us>

For Rhode Island Residents: You have the right to obtain a police report and request a security freeze as described below. You also may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

0000001



Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three nationwide consumer reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Security Freezes: You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
-

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the consumer reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.