CHIESA SHAHINIAN & GIANTOMASI PC

105 Eisenhower Parkway, Roseland, NJ 07068
csglaw.com

MICHELLE A. SCHAAP
mschaap@csglaw.com
(O) 973.530.2026
(F) 973.530.1501

January 23, 2026

via Electronic Mail
Attorney General John M. Formella
Office of the Attorney General Consumer Protection Bureau
1 Granite Place
South Concord, NH 03301
Tel: 603-271-3643
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Security Incident

To Whom It May Concern:

This firm serves as legal counsel to JURA Inc., a company located at 20 Craig Rd, Montvale, NJ 07645 (the "Company"). This letter serves as notice pursuant to N.H. RSA §§ 359-C:20(I)(b) regarding a security incident suffered by the Company (the "Security Incident"), which the Company believes impacted one (1) New Hampshire resident. The Company submitted a formal notice of the Security Incident to the affected individual via U.S. mail on or about January 21, 2026. A copy of the notice is appended to this letter.

NATURE OF THE SECURITY INCIDENT

On December 23, 2025, the Company detected unusual activity on the Company's computer network and confirmed the presence of an unauthorized entity in the Company's environment. After retaining this firm and performing a forensic investigation, the Company determined that an unknown threat actor had bypassed the Company's firewall on or about December 13, 2025. After bypassing the firewall, the unknown threat actor proceeded to access and exfiltrate certain personnel files containing the sensitive personal information of JURA's employees and contract hires.

At this time, the categories of personally identifiable information of the single New Hampshire resident believed compromised during the Security Incident include full name, address, Social Security Number, payment information, and other personal information incidental to compensation.

Importantly, however, there is neither evidence to date nor reason to believe that the Security Incident has resulted in or will result in identity theft, fraud, or financial losses to consumers.

STEPS TAKEN OR PLANNED TO TAKE RELATING TO THE INCIDENT

Shortly after confirmation of the Security Incident on December 23, 2025, the Company immediately responded by hiring this firm and engaging forensic consultants to assess the scope of the Security Incident and conduct a forensic investigation. In addition to updating its written information security plan, the Company has taken and plans to take further remedial and proactive measures,

including remediation of the vulnerability in the Company's firewall; implementation of advanced security tools on servers and workstations; deployment of additional protection software on the Company's systems and servers; and hardening all Company systems and servers.

Additionally, the Company is providing all potentially affected individuals with Experian IdentityWorks, a complimentary identify theft protection and credit monitoring service product, for a period of twenty-four (24) months.

OTHER NOTIFICATION AND CONTACT INFORMATION

Please reach me at 973-530-2026 or mschaap@csglaw.com if you have any questions or need further information.

Respectfully yours,

Michelle A. Schaap, Esq.

Michelle A. Schaap

MAS:fxw
Enc. (Sample Personnel Notice issued to the Impacted Individual)

January 21, 2026

[**NAME OF INDIVIDUAL**]
[**ADDRESS**]
[**CITY, STATE, ZIP CODE**]

NOTICE OF DATA INCIDENT

Dear [**NAME OF INDIVIDUAL**]:

At JURA Inc. ("**JURA**"), we value our workforce. In the course of our day-to-day operations at JURA, we recently identified unauthorized access to our computer network, resulting in the exposure of your sensitive personal information (the "**Security Incident**").

While we are taking appropriate steps in response to the Security Incident, we nevertheless recognize that notice of the Security Incident may be unsettling. We take the well-being and privacy of our workforce very seriously, and we want you to have the information you need to respond appropriately. To that end, we want you to know what happened, what information was involved, what we did and are doing in response to this Security Incident, and what you can do to help protect yourself against possible misuse of the information.

What Happened

On December 23, 2025, our third party managed service provider detected unusual activity on our computer network and confirmed the presence of an unauthorized entity in our computer environment. After performing an investigation, we determined that, on or about December 13, 2025, an unknown threat actor had bypassed our firewall as the result of an unknown vulnerability. After bypassing the firewall, the unknown threat actor proceeded to access and exfiltrate certain personnel files containing the sensitive personal information of JURA's employees and contractors.

We engaged legal counsel and forensic experts to further investigate the Security Incident. This month, in conjunction with legal counsel and our external forensic resource, we confirmed the scope of the Security Incident, including the persons and information compromised.

What Information Was Involved

At this time, based on our investigation, we believe that the categories of personally identifiable information involved and to have been compromised in this Security Incident were first names, last names, Social Security Numbers, dates of birth, addresses, and other personal information incidental to compensation.

What We Are Doing

Shortly after confirmation of the Security Incident on December 23, 2025, we immediately responded by engaging forensic consultants to assess the scope of the Security Incident and conduct a forensic investigation. We have taken and plan to take further remedial and proactive measures, including remediation of the vulnerability in our firewall; implementation of advanced security tools on servers and workstations; deployment of additional protection software on our systems and servers; and hardening all company systems and servers.

The Security Incident is being reported to law enforcement and applicable state agencies. To date, we have not received any reports regarding any unauthorized use of personal information beyond the Security Incident.

[redacted]

What You Can Do

Should you receive a call, email, or other communication from someone who claims to have your personal information pursuant to the Security Incident:

- do not engage with the caller/correspondent;
- do not offer details about the Security Incident or what may have occurred;
- listen carefully and immediately following such communication, make notes; and
- as soon as possible, share such information with me.

Importantly, we have contracted with Experian, at our sole expense, to provide all potentially affected individuals with IdentityWorks, a complimentary identify theft protection and credit monitoring service product, for a period of twenty-four (24) months. The attachment provides additional details about how to register for the product.

We recommend you remain vigilant and continue to monitor and review all your financial and personal account statements and credit reports. We further recommend that you immediately notify your local police department and your applicable financial institution(s) to advise them to be watchful for any suspicious or otherwise unusual activity associated with your financial or personal account(s).

We've also attached to this letter certain resources with additional information for your reference, including the toll-free numbers, the addresses, and direct websites of several relevant regulatory agencies and resources. Additionally, we have included the toll-free numbers, the addresses, and website addresses for the FTC and the three consumer credit reporting agencies. Please note that an individual can obtain information from the FTC and consumer reporting agencies about fraud alerts and security freezes, free of charge. We also describe more proactive measures you can take to protect yourself and your information.

Other Important Information

If you have any questions regarding this information, please contact me at [redacted] or [redacted].

Respectfully,

Alicia LaPierre
Human Resources Manager

[redacted]

DETAILS REGARDING YOUR 24-MONTH
EXPERIAN IDENTITYWORKS MEMBERSHIP

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** April 30, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/1bcredit/
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by April 30, 2026 at (833) 931-7577 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

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.
- **Security Freeze:** A freeze prevents unauthorized access to your Experian credit file, giving you peace of mind and protection against fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident.

If you have further questions or concerns, or would like an alternative to enrolling online, please call (833) 931-7577 toll-free Monday through Friday from 8 am to 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

Resource Pages

- **Local Police Reporting**

File a report with your local police department.

- **Passwords, Passcodes**

Change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. If you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to "recycle" or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, it is highly recommended to enable this for those accounts.

- **Social Security Administration**

Block Electronic Access: If you know your Social Security information has been compromised, you can request to Block Electronic Access. This is done by calling the Social Security Administration National 800 number (Toll Free 1-800-772-1213 or 1-800-325-0778). Once requested, any automated telephone and electronic access to your Social Security record is blocked. Note: No one, including you, will be able to see or change your personal information on the internet or through the Social Security Administration's automated telephone service. If you have requested that the Social Security Administration block access to your record and later change your mind, you can contact the Social Security Administration and ask to have the block removed. You will need to prove your identity when you call the Social Security Administration. See also: https://www.ssa.gov/pubs/EN-05-10220.pdf.

- **IRS**

Complete IRS Form 14039. The form can be found at: https://www.irs.gov/newsroom/tips- for-taxpayers-victims-about-identity-theft-and-tax-returns-2014.You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

We encourage you to monitor your financial accounts, including the account you use for direct deposit, and ask your account manager for additional services or resources that your bank may offer to protect your accounts. 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.

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security. To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Theft of your social security number should also be reported to the FTC at https://www.identitytheft.gov/. Alternatively, you may submit your request by marking it as "Confidential" and sending it via postal mail:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

- **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 http://www.annualcreditreport.com, calling toll-free 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 can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit

report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report, general inquiries, placing a fraud alert on your credit report, or requesting a credit freeze is provided below:

Experian	TransUnion	Equifax
1-888-EXPERIAN (397-3742)	1-800-680-7289	1-800-525-6285
P.O. Box 9532	Fraud Victim Assistance Division	P.O. Box 740241
Allen, TX 75013	PO Box 2000	Atlanta, GA 30374-0241
www.experian.com	Chester, PA 19016	www.equifax.com
	www.transunion.com	

- **Fraud Alert**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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 http://www.annualcreditreport.com.

- **Credit Freezes**

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived during such time
5. Proof of current address such as current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specific period of time.

To remove the security freeze, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic

means, or three business days after receiving your request by mail, to remove the security freeze.

Additional resources may be available from your state. Please see the below listing for your state. Note that not all states have additional sites.

Alabama:https://www.revenue.alabama.gov/faqs/if-i-am-a-victim-of-identity-theft-what-should-i-do/
Arizona: https://www.azag.gov/consumer/data-breach/identity-theft
California: https://oag.ca.gov/idtheft/facts/victim-checklist
Colorado: https://stopfraudcolorado.gov/fraud-center/identity-theft.html
Florida:https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Identity-Theft/Identity-Theft. For additional information, please call the Florida Attorney General's Identity Theft Victim Services toll-free telephone number at 1-866-9-NO-SCAM.
Georgia:https://www.bing.com/search?q=Identity+Theft+%7C+Georgia+Attorney+General%27s+Consumer+Protection+Division&cvid=c06989e6c5754d17a4c38386ef72028b&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQ6QcY_FXSAQgzODE0ajBqNKgCALACAA&FORM=ANAB01&PC=U531. See also https://dds.georgia.gov/georgia-licenseid/existing-licenseid/how-do-i-replace-license
Illinois: https://www.illinoisattorneygeneral.gov/consumers/hotline.html
Massachusetts: https://www.mass.gov/protecting-yourself-if-your-identity-is-stolen. For additional information, please call the Massachusetts Attorney General's Consumer Advocacy & Response Division, Consumer Hotline at (617) 727-8400.
Maine:https://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml#:~:text=Resources%3A,respond%20as%20soon%20as%20possible
Michigan: https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/id-theft-telemarketing/data-breaches
Minnesota:https://dps.mn.gov/divisions/ojp/help-for-crime-victims/Pages/Identity%20Theft.aspx and also https://www.revenue.state.mn.us/mndor-pp/6466?type=html.
Mississippi: https://www.its.ms.gov/services/identity-theft.
Nevada: Nevada Identity Theft Program, 1-775-684-1100.
New Hampshire: https://www.doj.nh.gov/citizens/consumer-protection-antitrust-bureau/consumer-protection-hotline.
New Jersey: https://www.nj.gov/njsp/tech/identity.html
New York: https://ag.ny.gov/consumer-frauds-bureau/identity-theft
North Carolina: https://ncdoj.gov/protecting-consumers/identity-theft/. In addition to the resources that we provided to you already, please note that you can also contact North Carolina resources about preventing identity theft as follows:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

Ohio: https://www.ohioattorneygeneral.gov/identitytheft#. For additional information, please visit https://www.ohioattorneygeneral.gov/FAQ/Responding-to-Identity-Theft-FAQs.
Oklahoma: https://oklahoma.gov/okdhs/library/idresources.html
Pennsylvania: https://www.attorneygeneral.gov/protect-yourself/identity-theft/
South Carolina: https://consumer.sc.gov/identity-theft-unit/id-theft.
Tennessee: https://www.tn.gov/content/dam/tn/safety/documents/IdentityTheftVicrimToolkit.pdf.
Texas: https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/identity-theft-resources.
Virginia: https://www.oag.state.va.us/programs-outreach/identity-theft. See also: https://www.dmv.virginia.gov/licenses-ids/license/applying/identity-theft .
Washington: https://www.atg.wa.gov/data-breach-resources.