JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

Direct Dial: (212) 545-4063
Email Address: damon.silver@jacksonlewis.com

June 2, 2026

VIA EMAIL (DOJ-CPB@doj.nh.gov)
Office of the New Hampshire Attorney General
Attn: Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

To whom it may concern:

We are writing to notify your office that our client, Yorozu Automotive Tennessee, Inc. ("Yorozu" or the "Organization"), was the subject of a cyberattack ("the Incident"). Yorozu immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on its information systems, and the identities of those the Incident may have affected.

Through its extensive investigation, the Organization identified certain files that may have been subject to unauthorized access. The Organization then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those files to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about December 19, 2025, the Organization determined that, during the period from October 9-13, 2024, the threat actor(s) may have accessed PII stored on the Organization's systems, including information related to two (2) residents of New Hampshire. The categories of impacted information included names, dates of birth, social security numbers, driver's license numbers, passport numbers, financial account information, medical information and/or health insurance information. The Organization found no evidence that this information was misused.

Out of an abundance of caution, and in accordance with applicable law, the Organization will provide notice to the affected New Hampshire residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. Additionally, the Organization has arranged for them to enroll in free credit monitoring and related services for 12 months.

[1] Please note that the Organization is not, by providing this letter, agreeing to the jurisdiction of the State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

The Organization treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, the Organization has taken a number of steps to further secure its systems. Specifically, it has, among other things, strengthened its security posture by updating all passwords, enabling multi-factor authentication across email networks, firewalls, VPNs, and administrative servers, and enhancing access controls and system monitoring. Yorozu also continues to regularly assess and strengthen its security policies.

If you require any additional information on this matter, please contact me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ Damon W. Silver

Damon W. Silver

cc: Melissa Pascualini (Jackson Lewis P.C.)

4904-8155-5366, v. 1

4904-8155-5366, v. 1

EXHIBIT “A”

YOROZU

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: September 2, 2026
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

June 2, 2026

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to notify you that Yorozu Automotive Tennessee, Inc. ("Yorozu") was impacted by a ransomware attack (the "Incident"). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident.

Through our extensive investigation, we identified certain files that were potentially subject to unauthorized access. We then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those files to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about December 19, 2025, we determined that, during the period from October 9-13, 2024, the threat actor(s) may have accessed PII that related to you. We found no evidence that this information was misused.

What Information Was Involved

The impacted files may have contained your name, along with your address, date of birth, social security number, driver's license number, government ID number, financial account information, health insurance information, medical information, or biometric information.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<1 year/ 2 years>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have, among other things, strengthened our security posture by updating all passwords, enabling multi-factor authentication across email networks, firewalls, VPNs, and administrative servers, and enhancing access controls and system monitoring. We continue to regularly assess and strengthen our security policies.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN] or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is September 2, 2026.

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please call our dedicated assistance line at [TFN] Monday through Friday, from 8:00 a.m. to 8:00 p.m. Central Time, except holidays.

Sincerely,

/s/*Phillip Williams*
Phillip Williams
Human Resources Director
Yorozu Automotive Tennessee, Inc.

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- ***All U.S. Residents***: The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338) or https://consumer.ftc.gov/features/identity-theft. The mailing address for the FTC is:

  Federal Trade Commission
  Consumer Response Center
  600 Pennsylvania Avenue, NW
  Washington, DC 20580

- ***Iowa Residents***: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.
- ***New Mexico Residents***: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here**.** Identity theft victims and active-duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; and by contacting Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- ***New York Residents***: Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.
- ***North Carolina Residents***: North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Oregon Residents***: Oregon Attorney General's Office, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.
- **Texas Residents**: The Office of the Attorney General of Texas, PO Box 12548, Austin, TX 78711-2548, 800-621-0508, www.texasattorneygeneral.gov.