Appendix

On April 6, 2025, Sensata Technologies, Inc. ("Sensata") determined that certain servers in its network were encrypted with ransomware. Sensata immediately implemented its response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations also was engaged. Sensata notified law enforcement and is supporting its investigation.

The evidence showed that there was unauthorized activity in Sensata's network between March 28, 2025 and April 6, 2025. During that time, an unauthorized actor viewed and obtained files from the network. Sensata conducted a careful review of the files and, on May 23, 2025 determined that one or more of them may have contained information concerning 362 Maine residents, including their names, addresses, and one or more of the following data elements: Social Security number, tax identification number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, payment card information, medical information, health insurance information, and/or date of birth.

Today, June 5, 2025, Sensata is mailing notification letters via First-Class mail to the involved Maine residents in accordance with the Health Insurance Portability and Accountability Act (45 CFR §§ 160.103 and 164.400 *et seq*.)[1] and Me. Rev. Stat. Tit. 10, §1348. A copy of the notification letter template is enclosed. Sensata is offering a complimentary, one-year membership to credit monitoring and identity protection services to the residents. Sensata also has established a dedicated, toll-free call center that the residents can call to obtain more information regarding the incident.

To help prevent something like this from happening again, Sensata has taken steps to enhance its existing security measures.

[1] Sensata is a global industrial technology company that manufactures sensors, electrical protection components, and other products. It is not a "covered entity," as defined by HIPAA, but it maintains information related to a group health plan in which its employees and dependents can participate. The plan is covered by HIPAA.

Sensata Technologies

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Sensata Technologies, Inc. recognizes the importance of protecting information. We are writing to inform you that we recently identified and addressed a data security incident that may have involved your information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

Who Are We, and Why Do We Have Your Information?
Sensata Technologies is a global industrial technology company that manufactures sensors, electrical protection components, and other products. We have your information because you are a current or former employee, the dependent of a current or former employee, or for another business-related reason.

What Happened?
On April 6, 2025, we determined that certain servers in our network were encrypted with ransomware. We immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations also was engaged. We notified law enforcement and are supporting its investigation.

The evidence showed that there was unauthorized activity in our network between March 28, 2025 and April 6, 2025. During that time, an unauthorized actor viewed and obtained files from our network. We conducted a careful review of the files and, on May 23, 2025, determined that one or more of them may have contained your information.

What Information Was Involved?
The information may have included your name, address, and one or more of the following data elements: Social Security number, tax identification number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, payment card information, medical information, health insurance information, and/or date of birth.

What We Are Doing.
We are notifying you of this incident and assure you that we take it seriously. We have arranged for you to receive one year of complimentary access to Experian IdentityWorks^{SM} credit monitoring, as discussed below. Additionally, to help prevent something like this from happening again, we have taken additional steps to enhance our existing security measures.

What You Can Do.
You can enroll in the complimentary credit monitoring product we have arranged for you. This product is designed to detect potential misuse of your information and offers identity protection solutions aimed at promptly identifying and resolving any instances of identity theft. Activating this product will not affect your credit score. For more information on identity

theft prevention and Experian IdentityWorks[SM], including instructions on how to activate your one year of access, as well as some additional steps you can take in response, please review the pages that follow this letter.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any questions, please contact us at 855-260-8081, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding holidays.

Sincerely,

Sensata Technologies, Inc.

Enroll in Experian IdentityWorks℠

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 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 12 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 12-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 <<Enrollment Deadline>>**, by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- 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 **<<Enrollment Deadline>>** at (833) 931-7577 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number **<<Engagement #>>** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** 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.

* 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts 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 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- *Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com
- *TransUnion Security Freeze*, PO Box 2000, Chester, PA 19016, www.transunion.com
- *Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Protecting Health Insurance or Medical Information: It is always advisable to review any statements you may receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, contact your insurer or provider immediately.

Sensata Technologies is located at 529 Pleasant Street, Attleboro, Massachusetts 02703, and can be reached at 508-236-3800.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves <<RI#>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.