



Jackson Lewis P.C.
 220 Headquarters Plaza
 East Tower, 7th Floor
 Morristown, NJ 07960-6834
 Tel 973 538-6890
 Fax 973 540-9015
 www.jacksonlewis.com
 Richard J. Cino - Managing Principal

Representing Management Exclusively in Workplace Law and Related Litigation

ALBANY, NY	GREENVILLE, SC	MONMOUTH COUNTY, NJ	RALEIGH, NC
ALBUQUERQUE, NM	HARTFORD, CT	MORRISTOWN, NJ	RAPID CITY, SD
ATLANTA, GA	HONOLULU, HI*	NEW ORLEANS, LA	RICHMOND, VA
AUSTIN, TX	HOUSTON, TX	NEW YORK, NY	SACRAMENTO, CA
BALTIMORE, MD	INDIANAPOLIS, IN	NORFOLK, VA	SALT LAKE CITY, UT
BIRMINGHAM, AL	JACKSONVILLE, FL	OMAHA, NE	SAN DIEGO, CA
BOSTON, MA	KANSAS CITY REGION	ORANGE COUNTY, CA	SAN FRANCISCO, CA
CHICAGO, IL	LAS VEGAS, NV	ORLANDO, FL	SAN JUAN, PR
CINCINNATI, OH	LONG ISLAND, NY	PHILADELPHIA, PA	SEATTLE, WA
CLEVELAND, OH	LOS ANGELES, CA	PHOENIX, AZ	ST. LOUIS, MO
DALLAS, TX	MADISON, WI	PITTSBURGH, PA	TAMPA, FL
DAYTON, OH	MEMPHIS, TN	PORTLAND, OR	WASHINGTON, DC REGION
DENVER, CO	MIAMI, FL	PORTSMOUTH, NH	WHITE PLAINS, NY
DETROIT, MI	MILWAUKEE, WI	PROVIDENCE, RI	
GRAND RAPIDS, MI	MINNEAPOLIS, MN		

*through an affiliation with Jackson Lewis P.C., a Law Corporation

JOSEPH J. LAZZAROTTI
 DIRECT DIAL: (973) 451-6363
 EMAIL: JOSEPH.LAZZAROTTI@JACKSONLEWIS.COM

January 30, 2019

VIA OVERNIGHT MAIL
 Office of Attorney General
 Security Breach Notification
 33 Capitol Street
 Concord, NH 03301

Re: Data Incident Notification⁴

Dear Attorney General:

Please be advised that on January 16, 2019, our client, Sensata Technologies (the “Company”), learned that one of its employees made an internal request for the employee’s IRS Form W-2 for the 2017 tax year. In response to the request, the employee was inadvertently sent on January 2, 2019, IRS Forms W-2 belonging to other Sensata employees. The data elements involved include name, address, Social Security number and employee earnings. We are writing to inform you about the status of the Company’s investigation and significant remediation efforts.

Upon learning of the disclosure of the personal information, the Company promptly commenced an investigation to determine the nature and extent of the incident. The Company’s IT team immediately took steps to review the employee’s email correspondence. The Company interviewed the employee about the incident and took steps to secure the employees’ personal information. This included working with the employee to review the systems that received the email, to assess and confirm that the employee received this information in good faith and in connection with the Company’s business, and to obtain written confirmation by the employee that all of the information had been destroyed or returned, not used for an improper purpose, and not forwarded or shared with anyone else. While the investigation is ongoing, at this stage it appears 2,379 individuals could have been affected, including 3 New Hampshire residents. In light of this incident, the Company plans to begin notifying individuals in the next several days. A draft copy of the notification that will be sent is attached.

As set forth in the attached letter, the Company has taken numerous steps to protect the security of the personal information of all individuals. In addition to continuing its investigation and monitoring this situation, the Company is reexamining its current privacy and data security, policies and procedures to find ways of reducing the risk of future data incidents. In particular, it will be redoubling its efforts at employee training concerning the handling of email attachments to prevent a recurrence of inadvertent communications like this one. The Company deploys data loss prevention software at the site where the incident occurred that will assist in mitigating similar

⁴ Please note that by providing this letter, Sensata is not agreeing to the jurisdiction of this state, or waiving its right to challenge jurisdiction in any subsequent actions.

January 30, 2019

Page 2

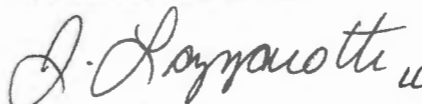
inadvertent communications. Should the Company become aware of any significant developments concerning this situation, such as circumstances that would cause this incident not to be a good faith acquisition by our employee, we will inform you.

In an abundance of caution, the Company is providing affected persons with ID theft resolution and credit monitoring services at no cost. We will be sending enrollment information shortly after the initial notification because we did not want to delay the initial notification.

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

Sincerely,

JACKSON LEWIS P.C.

A handwritten signature in black ink, appearing to read "J. Lazzarotti", with a small flourish at the end.

Joseph J. Lazzarotti

Encl.



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> << NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

NOTICE OF DATA BREACH

Dear <<FirstName>> <<LastName>>,

At Sensata, we take the privacy and security of our employees' personal information very seriously. We regret to inform you that we discovered an incident involving some of your personal information. Based on our investigation to date, summarized below, we do not believe there is a significant risk of harm to you. However, in the abundance of caution, we are sending this advisory to you so that you can take steps to protect yourself and minimize the possibility of misuse of your information. We sincerely apologize for any inconvenience this may cause you and assure you that we have and continue to deploy measures to avoid these kinds of incidents from happening.

What Happened?

On January 16, 2019, we discovered that one of our employees made an internal request for the employee's IRS Form W-2 for the 2017 tax year. In response to the request, the employee was inadvertently sent on January 2, 2019, IRS Forms W-2 belonging to other Sensata employees, including yours.

Based on our investigation to date, we have no reason to believe that your information was shared outside the control of Sensata and its employees.

What Information was Involved?

The personal information that may have been accessed from your form W-2 includes personal information such as name, address, social security number, and employee earnings. We maintain this and other human resources information about you because you are an employee of the Company.

What Are We Doing?

Upon learning of a potential disclosure of personal information, we promptly commenced an investigation to determine the nature and extent of the incident. Our IT team immediately took steps to review the employee's email correspondence. We interviewed the employee about the incident and took steps to secure your personal information. This includes working with the employee to review the systems that received the email and to obtain written confirmation by the employee that all of the information has been destroyed or returned to us, was not used for an improper purpose, and was not forwarded or shared with anyone else.

We prepared the attached sheet which describes steps you can take to protect your identity, credit and personal information. In addition, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until April 30, 2019 to activate your identity monitoring services.

Your membership number for enrollment is: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-560-8630. Additional information describing your services is included with this letter.

Finally, we are reviewing our policies and procedures to determine how we can avoid similar incidents in the future. For example, we will be redoubling our efforts at employee training on the handling of email attachments to prevent a recurrence of inadvertent disclosures like this one.

What Can You Do?

The attached sheet describes steps you can take to protect your identity, credit and personal information. In addition, as noted, while our investigation to date indicates there is not a significant risk of harm to you, we have made credit monitoring and ID theft services available to you at no cost. We recommend you enroll in that service.

For More Information

If you have questions, please call 1-877-560-8630, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Allisha Elliott
Chief Human Resources Officer

Important Identity Theft Information:

Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. When you receive your credit report, look it over with care. If you notice anything suspicious – accounts you did not open, inquiries from creditors that you did not initiate, personal information such as a home address or Social Security number that is not accurate – or you see anything you do not understand, call the credit reporting agency at the number listed in the report. If you find fraudulent or suspicious activity in your credit reports, you should promptly report the matter to the proper law enforcement authorities.

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 national credit reporting agencies listed below.

Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
(888) 685-1111
www.equifax.com

Experian
P.O. Box 4500
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016
(800) 888-4213
www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax: Report Fraud: 1.888.766.0008
Experian: Report Fraud: 1.888.397.3742
TransUnion: Report Fraud: 1.800.916.8800

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three business days after receiving your request 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 personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities 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 three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions If You Are a Victim of Identity Theft

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from: <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: <http://www.ftc.gov/idtheft>; calling 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Additionally, you may obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC.

State-Specific Information

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling 1.515.281.5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may report suspected identity theft to the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling 1.503.378.4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.401.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903. The number of affected individuals who reside in Rhode Island is 353.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.