cons.

May 13, 2015

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capital Street
Concord, NH 03301

Re: OSRAM SYLVANIA - Notice of Security Breach

Dear Mr. Attorney General:

I am writing to inform you that a vendor of OSRAM SYLVANIA Inc. had a security breach that may have resulted in unauthorized access to a computer account containing personal information of a former employee of OSRAM SYLVANIA who resides in New Hampshire.

Description of the Incident

OSRAM SYLVANIA contracted with Equifax, Inc. for various human resources services, including payroll and unemployment services. Equifax first notified OSRAM SYLVANIA of unauthorized access of an individual account by e-mail on April 10, 2015, however, the e-mail did not include information about the identity of the potentially affected individual. The e-mail also stated Equifax was continuing its investigation and working with law enforcement. OSRAM SYLVANIA made a follow-up inquiry with Equifax, and received a more detailed explanation in a letter dated April 30, 2015 (received on May 5, 2015).

The letter reported that on April 9, 2015, as a result of an internal investigation prompted by suspicious activity, Equifax determined that an employee had potentially misused access privileges to reset the accounts for two former employees of OSRAM SYLVANIA and accessed personal information associated with those accounts. The account resets occurred in January and February 2015. The personal information may have included names, home address, employee identification number, social security number, financial information, and employment information including hire date, termination date, total time, and last pay date. Equifax reported that it had no indication that the account of the New Hampshire resident had been inappropriately accessed other than the account reset. After further investigation OSRAM SYLVANIA could not determine whether there had been any unauthorized access of the New Hampshire resident's account and decided to notify the affected individuals as well as your office.

Notice to New Hampshire Resident

OSRAM SYLVANIA sent the New Hampshire resident written notice of this incident on May 13, 2015, in the form of the attached letter.

OSRAM SYLVANIA
100 Endicott Street
Danvers, MA 01923
☎ (978) 777-1900

www.sylvania.com

Other Steps Taken

Equifax informed OSRAM SYLVANIA that it terminated the employee and is cooperating with law enforcement. Equifax has also taken steps to prevent any further inappropriate access including performing an account reset that requires the affected individuals to contact Equifax to reestablish account access, and daily, targeted network monitoring of the affected accounts for suspicious activity. Equifax is offering each employee access to two free years of credit monitoring services. OSRAM SYLVANIA is reviewing its data breach notification protocols and vendor security practices.

Should you have any questions concerning this incident, please contact me at [redacted]

[redacted]

Enclosure

[LETTER DATE]

[NAME]
[ADDRESS

Dear [FIRST NAME],

I am writing to inform you of a security incident involving one of our vendors that may have resulted in unauthorized access to your personal information.

OSRAM SYLVANIA Inc. contracted with Equifax, Inc. to handle various human resource processes on our behalf, including payroll and unemployment services.

On May 5, 2015, we received a letter from Equifax's Security team notifying us that they determined that an employee may have misused their access privileges to reset your account on [DATE], and may have accessed personal information within your account. The personal information may have included your name, address, employee identification number, social security number, financial information and employment information including hire date, termination date, total time and last pay date.

Equifax has provided us with assurances that they have investigated the matter and there is no indication that your account has been inappropriately accessed by anyone else. Equifax terminated the employee and is cooperating with law enforcement. Equifax has also taken steps to prevent any further inappropriate access, including performing an account reset that requires you to contact Equifax and reestablish your account access and performing daily monitoring of your account for suspicious activity. I wanted to inform you of this incident as soon as possible so that you can take appropriate measures, such as those set forth below, to further protect your personal information.

Equifax will provide you with a free two-year subscription to Equifax's identity theft protection service, ID Patrol. This service includes comprehensive credit file monitoring and automated alerts of any key changes to your credit reports, a one million dollar Identity Fraud Expense Coverage, and access to your credit report. The attached materials describe the ID Patrol service and include instructions on how to enroll with your personal activation code (ID Patrol Activation Code: ####). Please note that you must complete the enrollment process by [ENROLLMENT DEADLINE].

Here are some additional steps you can take to protect your personal information:

- Closely monitor your financial accounts and promptly contact your financial institution if you see any unauthorized activity.

- Monitor your credit report at all three of the national consumer credit reporting agencies. You can order a free copy of your credit report by:

OSRAM SYLVANIA
100 Endicott Street
Danvers, MA 01923
☎ (978) 750-2757
www.sylvania.com

- Visiting www.annualcreditreport.com;
- Calling 877-322-8228; or
- Completing the Annual Credit Report Form on the Federal Trade Commission website at *http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf.*

Here is the contact information for all three national credit-reporting agencies:

Equifax	Experian	TransUnion
Phone: 800-685-1111 P.O. Box 740241 Atlanta, GA 30374 www.equifax.com	Phone: 888-397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	Phone: 800-916-8800 P.O. Box 2000 Chester, PA 19022 www.transunion.com

- Consider placing a fraud alert message on your Equifax credit file. By placing this alert on your Equifax credit file, any company that requests your credit file will receive a message warning them that you may have been a victim of fraud. Moreover, companies that receive this alert may request proof of your identity. This step will help protect you from accounts being opened or used by anyone other than yourself. If you would like to place a fraud alert message on your Equifax credit file, please call 1-877-478-7625. Once you contact Equifax to place a fraud alert, Equifax will notify Experian and TransUnion on your behalf to request that they place a fraud alert on your file as well.

- If you detect any incident of fraud or identity theft, promptly report the incident to local law enforcement and the Federal Trade Commission (www.consumer.ftc.gov; 877-438-4338; 600 Pennsylvania Avenue, NW, Washington, DC 20580). You can also obtain information from these sources about additional methods to prevent identity theft, and you can obtain more information regarding fraud alerts and security freezes from the Federal Trade Commission and consumer reporting agencies.

We take the protection of our employees' information very seriously and we apologize for any inconvenience this may cause you. If you have any questions regarding this notification, please feel free to contact me at (978) 750-2757.

Sincerely,

Ben Kradin, Esq. CIPM, CIPP/US
Corporate Manager of Information Security & Data Privacy

Enclosure