BakerHostetler

STATE OF NH
DEPT OF JUSTICE
2016 MAR 10 AM 9:21

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

March 9, 2016

VIA OVERNIGHT DELIVERY

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

Our client, Seagate US LLC ("Seagate"), on March 1, 2016, learned that a targeted "phishing" email message had been sent from outside the company to Seagate employees. Upon learning this, Seagate immediately began an internal investigation. The investigation revealed that the phishing email targeted Seagate employees in HR and Payroll on February 29, 2016, requesting copies of all 2015 Forms W-2, and unfortunately the email was not recognized as a scam. The information disclosed by Seagate to the sender of the phishing email was the actual W-2 information, including the names, addresses, Social Security numbers, and earnings for anyone who was a Seagate or Seagate affiliate employee and was issued a W-2 for the 2015 tax year. The IRS and federal law enforcement have been notified of this incident and Seagate is cooperating with their investigation.

Although, at this time, we know of no reports of identity theft or other fraud related to this incident, Seagate provided an email notification of this incident to its current U.S. employees on March 4, 2016, and will begin mailing notification letters to the home addresses of affected current and former employees by March 9, 2016. Seagate is offering affected current and former employees at least two years of credit monitoring and identity theft protection services through Experian. Seagate also is providing call center support for those affected.

Seagate is notifying seven (7) New Hampshire residents in substantially the same form as the letter attached hereto.[1] Notification is being provided in the most expedient time possible

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

and without unreasonable delay pursuant to the investigation described above, which was necessary to determine the scope of the incident and identify the individuals potentially affected. *See* N.H. REV. STAT. ANN. § 359-C:20(I)(a).

To prevent this from happening again, Seagate is analyzing where process changes are needed and supplementing the training in this area that has been conducted for all employees with additional training.

Please do not hesitate to contact me if you any have questions regarding this matter.

Sincerely,

Theodore J. Kobus III

Enclosure

cc: Mark D. Honeycutt, Senior Attorney, Legal Department

SEAGATE

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>><<Last Name>>
<<Street Address>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

Seagate Technology is committed to maintaining the privacy and security of our employees' personal information. Regrettably, we are writing to inform you of an incident involving the unauthorized disclosure of this information.

On March 1, 2016, we learned that a targeted "phishing" email message had been sent from outside the company to Seagate employees. Phishing emails are an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. In this case, the phishing email targeted Seagate employees in HR and Payroll, requesting copies of all 2015 Forms W-2, and unfortunately the email was not recognized as a scam. The information disclosed was the actual W-2 information, including the names, addresses, Social Security numbers, and earnings for anyone who was a Seagate or Seagate affiliate employee and was issued a W-2 for the 2015 tax year.

The IRS and federal law enforcement have been notified of this incident. The IRS has reported that several other companies have been targeted by this type of scheme. The IRS has also indicated to us that they will add extra scrutiny to affected employees' accounts for this year, in an effort to prevent fraudulent tax refunds from being paid out.

Seagate is offering you at least a two-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your two-year membership, please see the additional information provided with this letter. We strongly recommend that you follow these instructions to activate your membership as soon as possible.

We deeply regret that this incident has occurred and that the privacy and security of your personal information was not protected as it should have been. At the company level, we are aggressively analyzing where process changes are needed, and will take the appropriate actions. We will supplement the phishing training conducted for all employees with additional training and further information in the near future.

Should you have any questions, we have arranged a dedicated call center run by a third party, Epiq, to assist with questions about how to protect your identity following this incident. Please call Epiq at 1-844-754-5542, from 9:00 a.m. to 9:00 p.m. Eastern Standard Time, Monday through Friday.

Sincerely,

Regan J. MacPherson
Vice President and Interim General Counsel

Enclosures: Activate ProtectMyID Now in Three Easy Steps
Information About Preventing Identity Theft

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: June 13, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: <<Acct code>>**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC99735**

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/redeem
or call 877-371-7902 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(800) 680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
(877) 438-4338

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.