BakerHostetler

STATE OF NH
DEPT OF JUSTICE
2016 MAR 22 AM 9:49

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 21, 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, Convey Health Solutions, Inc. ("Convey"), on March 7, 2016, learned that a targeted "phishing" email message had been sent from outside the company to a Convey employee. Upon learning this, Convey immediately began an internal investigation. The investigation revealed that the phishing email targeted a Convey employee in HR on March 7, 2016, requesting copies of 2015 Forms W-2, and unfortunately the email was not recognized as a scam. The information disclosed by Convey to the sender of the phishing email was the actual W-2 information, including the names, addresses, Social Security numbers, and earnings for certain employees during the 2015 tax year. The IRS and federal law enforcement have been notified of this incident and Convey is cooperating with their investigation.

Convey provided an email notification of this incident to its current affected employees on March 15, 2016, and will begin mailing notification letters to the home addresses of affected current and former employees by March 21, 2016. Convey is offering affected current and former employees two years of credit monitoring and identity theft protection services through Experian. Convey also is providing call center support for those affected.

Convey is notifying one (1) New Hampshire resident in substantially the same form as the letter attached hereto.[1] Notification is being provided in the most expedient time possible 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, Convey 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

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

CONVEY™
HEALTH SOLUTIONS

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

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

<<Date>>

Dear <<FirstName>> <<LastName>>:

Convey Health Solutions ("Convey") is committed to maintaining the privacy and security of our employees' personal information. Regrettably, we are writing to inform you of an incident involving some of that information.

On March 7, 2016, we learned that a targeted "spear phishing" email message had been sent to a Convey employee that same day. Spear 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. The email our employee received was designed to appear as though it had been sent to the employee by a Convey executive, from the Convey executive's email account, requesting copies of 2015 Forms W-2, including names, addresses, Social Security numbers, and salary information. Believing the email to be legitimate, the employee authorized the reply to the message on the day the email was received, and the 2015 Forms W-2, which included your personal information, were attached to the response.

The IRS and federal law enforcement have been notified of this incident, and we are cooperating with their ongoing investigation. The IRS has indicated to us that they will monitor affected employees' accounts for this year, in an effort to prevent fraudulent tax refunds from being paid out.

We recognize this issue can be frustrating, and we are taking steps to help protect you and to safeguard the personal information we receive and maintain going forward. We are offering a complimentary two-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. ProtectMyID Elite is completely free, and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on ProtectMyID Elite and instructions on how to activate your complimentary two-year membership, please see the next page of this letter.**

We regret any concern this may cause you. To help prevent something like this from happening again, we are reinforcing our information security training program with an emphasis on the detection and avoidance of phishing email scams and identifying opportunities to increase security within our information technology systems. Should you have further questions regarding this incident, you may call 1-855-219-2587, Monday through Friday, 8:30 a.m. to 5:00 p.m. Eastern Standard Time, excluding holidays.

Sincerely,

Steven M. Mead
Senior Vice President of Finance

ACTIVATE PROTECTMYID NOW IN THREE EASY STEPS

1. ENSURE **That You Enroll By: June 30, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Website to enroll: www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide engagement #: **PC100048**.

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 3-Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded, or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity 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; and 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.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

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 877-441-6943.

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
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
(800) 685-1111

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary, 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.

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, D.C. 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.