Holland & Knight

[redacted]

[redacted]

STATE OF NH
DEPT OF JUSTICE
2015 JAN 13 AM 9:52

January 12, 2015

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

Dear Attorney General Foster:

Pursuant to NH Statutes Section 359-C:20(I)(b), we are writing to notify you of a potential unauthorized use of personal information involving one (1) New Hampshire resident.

On December 10, 2014, Alin Machining Company Inc. (d/b/a Power Plant Services) learned that an independent contractor may have misused personal employee information for a very small group of Power Plant Services personnel between November 7, 2014 and December 4, 2014. The types of information that were the subject of this incident include:

- Name
- Address
- Social Security Number
- Bank Account Number

The company believed that there was an issue when several employees contacted its Human Resources (HR) department regarding suspicious activity on their financial accounts. The company immediately launched an internal investigation to try to determine the cause of the suspicious activity.

During the course of its investigation, the company's HR manager indicated that he had shared his user name and password, providing access to the company's externally housed HR system ("HRIS"), with an independent contractor. At that point, the company's investigation focused on the independent contractor's activities. The company was able to confirm that access to HRIS occurred at unusual times and from unknown IP addresses. Power Plant Services notified and is working with law enforcement—both state and federal—who are currently investigating the matter.

Power Plant Services has determined that there is one (1) New Hampshire resident whose information could have been accessed by the independent contractor. At this time, Power Plant Services knows of 7 employees whose information may have been misused, and those individuals have been contacted separately. Currently, Power Plant Services has no indication that the information of the New Hampshire resident has been misused, but Power Plant Services will be notifying this individual in an abundance of caution. Attached please find a copy of the notice letter that will be mailed to the affected New Hampshire resident on January 13, 2015.

Power Plant Services is taking steps to prevent future incidents of this nature, including reviewing its hiring policies, use of independent contractors, and third-party companies that it utilizes to assist with both. In addition, the company has retained individuals with respect to user access privileges and protection of user IDs and passwords. The company is further reviewing its employee data access process with the goal of implementing more stringent access protocols.

Below is the contact information for [redacted]
Power Plant Services:

[redacted]

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

[redacted]

Alin Machining Co., Inc. d/b/a
Power Plant Services
"The Turnkey Solution"
ISO 9001 Certified

[DATE]

[EMPLOYEE NAME]
[ADDRESS]

RE: Potential Employee Data Breach

Dear [NAME]:

On December 10, 2014, we learned that an independent contractor may have misused personal employee information (including name, address, social security number, and bank account information) for a very small group of Power Plant Services personnel between November 7, 2014 and December 4, 2014, and you have been identified as someone whose information could possibly have been accessed by the independent contractor. At this time, we have no indication that your information has been misused, but we wanted to advise you in an abundance of caution. We have also notified and are working with local and federal law enforcement.

We take the security and privacy of our employee's data very seriously and have suggestions for you to take.

For the future security of your credit card information, we recommend that you remain vigilant by informing your bank and credit card companies of the situation so that they can monitor for suspicious activity. You should also regularly monitor your account activity yourself, and you might consider changing your bank account number, but consult with your bank before doing so. Should you notice any unauthorized transactions, please inform me and the appropriate financial institution immediately. You should also periodically review your credit report and account statements, even if you do not initially find suspicious activity. Of course, you should not provide personal information to others unless you are certain of the requester's identity.

You may also consider opening an account with Credit Karma. This service provides free personal credit monitoring and other additional valuable financial services. Key points to consider when utilizing this service include:

- Review all personal information for accuracy.

- Look for accounts you did not open or for inquiries from creditors that you did not initiate.
- If you see anything that you do not understand, you should call a credit agency.
- Report any suspicious activity on your credit reports to the proper authorities.

Finally, we have included with this letter an explanation of additional steps you may consider taking to further protect yourself.

We sincerely regret that this incident occurred, and we are taking steps to prevent future incidents of this nature. Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Very truly yours,

Antonio H. Caballero
Sr. Human Resources Manager
708-345-8600 x164
tcaballero@ppsvcs.com

IDENTITY THEFT PRECAUTIONS

Free Credit Report

The Fair Credit Reporting Act requires each of the three nationwide consumer reporting agencies (Equifax, Experian and TransUnion) to provide you annually, upon request, with a free copy of your credit report. Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by phone at 1-877-322-8228. You can also request your free credit report by completing the request form available at www.annualcreditreport.com, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major consumer reporting agencies listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

You may also consider placing a free 7-year fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. You can do so by contacting each of the below credit bureaus and supplying the required documentation in writing. PPS can provide you a standard letter template with the requested information and also provide the identity theft police report, if you choose this option.

Equifax
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
Toll-free: 800-525-6285
www.fraudalerts.equifax.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
Toll-free: 800-680-7289
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
Toll-free: 888-397-3742
www.experian.com/fraud/center.html

Further Information

You may obtain additional information about identity theft (including a security freeze) by contacting the above credit bureaus, the Federal Trade Commission (FTC), or your Attorney General's office using the contact information below. In addition, certain state laws advise you to report suspected incidents of identity theft to local law enforcement or to your Attorney General's office.

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