11/28/2017

Via Certified Mail Return Receipt Requested

Mr. Gordon MacDonald, Attorney General
State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: PII Breach Incident Notification

Dear Attorney General MacDonald:

Pursuant to New Hampshire Statutes, Section 359-C:20, we are writing to notify you of a data breach incident involving three (3) New Hampshire residents.

Nature of the Incident

On Tuesday, November 21, 2017 at or around 4:52 and 4:53 PM, an employee located at our New Hampshire office inadvertently sent three (3) emails containing the personally identifiable information (PII) of three (3) employees, who are also New Hampshire residents, to an unintended email recipient.

The PII that may have been obtained by the unintended email recipient as a result of this breach includes the employees' names and their social security numbers.

Steps Taken in Response to the Incident

Upon notice of the incident, our Human Resources and Compliance Departments were immediately notified on November 22, 2017 at or around 9:27 AM..

On November 22, 2017, the Compliance Department attempted to contact the unintended recipient to first determine whether or not they indeed received the emails and secondly, to notify them to delete all emails and any attachments; however the email address of the unintended recipient is one that appears to not be in use. As such, we were unable to determine whether or not the recipient indeed obtained any personal information via that email address.

On November 22, 2017, the Human Resources Department sent notifications electronically to the three (3) New Hampshire employees informing them of the breach incident. Included in each

notice were suggested steps that these employees can take to monitor their personal information. In addition, we included contact information and/or appropriate internet links for credit reporting agencies and the Federal Trade Commission. Lastly, we provided contact information for the individual at our agency who can answer their questions and address any concerns regarding this breach incident. A sample copy of that electronic notice is enclosed.

To date, we have not seen any evidence suggesting that the personal information has been accessed or misused in anyway, and we do not have any reason to believe that this will occur. Regardless, we will continue to monitor this incident and follow up with the affected three (3) New Hampshire employees.

Company Contact Information:

Ms. Krista M. Strazza, Director of Compliance
Coordinated Transportation Solutions
35 Nutmeg Drive, Suite 120
Trumbull, CT 06611
(203) 736-8810, Ext. 10009
kstrazza@ctstransit.com

Sincerely,

Ms. Krista M. Strazza, Director of Compliance
Coordinated Transportation Solutions

Enc.

NOTICE OF DATA BREACH

Dear [EMPLOYEE NAME],

We are contacting you about a data breach that has occurred at CTS.

On Tuesday, November 21, 2017 at or around 4:52 and 4:53 PM, an individual from our office inadvertently scanned an email with your personal benefits enrollment information to an unintended single recipient.

We are currently acting to recall the scanned email from this unintended recipient, and recall the message. We will keep you updated if we are successful, and the outcome of all our efforts on this matter.

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

Equifax: equifax.com (link is external) or 1-800-525-6285
Experian: experian.com (link is external) or 1-888-397-3742
TransUnion: transunion.com (link is external) or 1-800-680-7289

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call local law enforcement. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends

on state law. Find your state Attorney General's office at naag.org (link is external) to learn more.

If you determine there are any problems with your personal information being utilized, please notify me and Krista Strazza right away and we can discuss assisting you with services to prevent and monitor these concerns.

Best regards

Thanks,
Pat

Patricia Wheeler
Director, Talent Acquisition and Human Resources
Coordinated Transportation Solutions, Inc.
35 Nutmeg Drive Suite 120
Trumbull, CT 06611-5431

pwheeler@ctstransit.com
203-736-8810 ext.10140
203-375-0510 (fax)
www.ctstransit.com