



RECEIVED

SEP 10 2018

CONSUMER PROTECTION

September 6, 2018

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General MacDonald:

As required under New Hampshire law, we are writing to notify you of a breach of security involving 14 New Hampshire residents.

On August 30, 2018 an email regarding health benefits was sent to the employees of KYOCERA Document Solutions New England, Inc. ("KDA-NE") which contained sensitive employee information. The breach involved the inadvertent inclusion of names, social security numbers, and hire dates of a majority of the KDA-NE employees.

There was a total of 14 individuals residing in New Hampshire whose personal information was the subject of the incident. We are sending notice to all KDA-NE employees residing in New Hampshire on or around September 12, 2018 via mail. A sample copy of the notice to New Hampshire residents is attached.

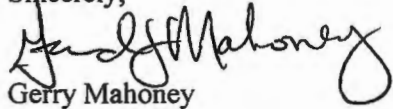
The breach was identified immediately after it occurred on August 30, 2018 and the email was recalled within minutes of being sent. KDA-NE has taken a number of additional actions to limit harm to the affected individuals. KDA-NE immediately began working with KDA headquarters to mitigate the propagation of the email and erased the email from our systems. On August 31, 2018, KDA-NE began working with Microsoft's Professional Services Group to use forensic tools to search and destroy the email off of their servers. This action was completed at 10pm, Wednesday, September 5, 2018. KDA-NE's IT Team has gone to KDA-NE employee work stations in Connecticut, Maine, Massachusetts and Vermont to remove the email from all computers and personal devices, and also called in service technicians to do the same to their computers and other devices. Other remote offices of KDA-NE have been advised how to remove the email from the system. KDA-NE requested that employees who received the email delete it from all devices, and agree not to save, print, or forward it in any way. The IT Team is using forensic tools provided by Microsoft to determine whether any of those actions have occurred. Those employees who have forwarded the email to a personal account have been spoken to, and advised to permanently delete the email. A search was run the morning of Tuesday, September 4, 2018, which resulted in a finding that no further transfers or forwards have occurred to any email accounts. Moreover, based on the results of that search, no evidence of the email in question remained in KDA-NE's servers.

To further confirm that employees' information was not dispersed, we are requesting each KDA-NE employee complete, sign and have notarized an Affidavit to certify that the employee has not opened or used the information contained in the offending email in any way.

KDA-NE provided the contact information on the three major credit reporting bureaus to the employees to protect themselves from potential harm resulting from this breach and suggested they order and monitor their credit reports. KDA-NE purchased a program through Experian for all KDA-NE employees to place a fraud alert on their credit report, and provided additional information if they wish to obtain 12 months of free credit monitoring through Experian, the cost of which will be paid by KDA-NE.

For further assistance, additional information, or questions, please call Brian Fox at 781-404-5307, or email at [brian.fox@kda-ne.com](mailto:brian.fox@kda-ne.com) or send a letter to KYOCERA Document Solutions America, Inc., attention Brian Fox at One Jewel Drive, Wilmington, MA 01887.

Sincerely,

A handwritten signature in black ink, appearing to read "Gerry Mahoney". The signature is written in a cursive style with a large, looping "G" and "M".

Gerry Mahoney  
President

SEPTEMBER \_\_, 2018

SUBJECT: BREACH NOTIFICATION

Dear Employee:

As we advised you on Friday, August 31, 2018 ("Initial Notice"), KYOCERA Document Solutions New England, Inc. ("KDA-NE") became aware that a breach of your (and other of your colleagues') sensitive identifying information had occurred. This breach occurred when an email regarding Open Enrollment was sent to all KDA-NE employees in error on the morning of August 30, 2018.

First, let me again say that we are profoundly sorry that this occurred. We apologize to you for this unfortunate incident. Secondly, let me describe what our investigation has uncovered, and those actions we have taken to address this situation and prevent any future breach. We have also included information in this letter regarding actions you may take to further protect your own information.

The breach involved the inadvertent inclusion of names, social security numbers, and hire dates of a majority of the KDA-NE employees. The breach was identified immediately after it occurred on August 30, 2018.

Upon learning of this disclosure, KDA-NE has taken a number of actions to limit harm to you and the other affected individuals. As explained in the Initial Notice, this included recalling the email within minutes of it being sent. KDA-NE also immediately began working with KDA HQ to mitigate the propagation of the email and began taking major steps to erase the email from our systems. On Friday, August 31<sup>st</sup>, KDA-NE began working with Microsoft's Professional Services Group to use forensic tools to search and destroy the email off of our servers. This action was completed at 10pm, Wednesday September 5, 2018. Our IT Team has gone to KDA-NE employee work stations in Maine, Connecticut, Massachusetts and Vermont to remove the email from all personal devices, and also called in service technicians to do the same to their devices. Other remote offices have been advised how to remove the email from the system.

We requested that employees who receive the email delete it from all devices, and agree not to save, print, or forward it in any way. The IT Team is using forensic tools provided by Microsoft to determine whether any of those actions have occurred. Those employees who forwarded the email to a personal account have been spoken to, and advised to permanently delete the email. A search was run the morning of Tuesday, September 4, 2018, which resulted in a finding that no further transfers or forwards have occurred to any email accounts. Moreover, based on the results of that search, no evidence of the email in question remained in KDA-NE's servers.

To further confirm that your and the other impacted employees' information was not disseminated, we are requesting each KDA-NE employee review, sign and have notarized, the attached Affidavit to certify that the employee has not opened or used the information contained in the Open Enrollment email in any way. In the next few days, we will provide a date and time

when a notary will be present in your offices to facilitate the signing and/or suggestions of how to get the Affidavit notarized if you are in a remote location. Once executed, please provide the original to your office manager who will gather all affidavits and send them to KDA Legal. If you have any questions regarding the Affidavit, please do not hesitate to contact Gerry Mahoney or Brian Fox. The security of our employees' information is of utmost importance to us, and we sincerely appreciate your cooperation in providing us the Affidavit.

In addition to the actions we have taken regarding this specific incident, we are working on a number of items to prevent any future violations of this type. For instance we have changed our internal email approval setting so that any deliveries to the "All Employees" distribution groups must first be approved by the President or Controller prior to release. We are reviewing other preventative measures, including utilizing email encryption, but note that because our main focus in the last few days has been to remedy the current breach, we have not been able to implement these changes. We will continue to update you as we put them into place.

While we have no reason to believe the information disclosed will be used for fraudulent purposes, as a result of this unfortunate incident, you may want to consider taking the following steps to protect yourself from potential harm resulting from the breach:

- There are three major credit reporting bureaus. Their contact information is listed below. We have already purchased a program through Experian for all KDA-NE employees, not just those affected, to place a fraud alert on your credit report if you choose to participate. This can help prevent an identity thief from opening additional accounts in your name. As soon as Experian confirms your fraud alert, the other two bureaus will be notified automatically of the fraud alert.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	Fraud Victim Assistance Division
Atlanta, GA 30374	Allen, TX 75103	P. O. Box 6790
1-888-766-0008	1-888-397-3742	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	1-800-680-7289
		www.transunion.com

- If you wish to obtain twelve months of free credit monitoring through Experian, the cost of which will be borne by KDA-NE, please contact Brian Fox at [Brian.Fox@kda-ne.com](mailto:Brian.Fox@kda-ne.com) on or before December 31, 2018 to make arrangements to enroll. If you wish to learn more about the program, please see the attached information provided by Experian and/or contact Experian directly.
- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. You are entitled to receive a free credit report annually from each of the three credit bureaus free of charge. We recommend that you space out your requests so that you receive one free credit report every four months. For example, request a report from Experian

immediately, a report from Equifax four months from now and a report from TransUnion four months later. Examine each report closely and look for signs of fraud such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure that an imposter has not opened an account with your personal information.

Again, we very much regret this situation occurred and apologize for any concern this may cause you personally.

For further assistance, additional information, or questions, please call Brian Fox at 800-847-3526 or 781-404-5307, or email at [Brian.Fox@kda-ne.com](mailto:Brian.Fox@kda-ne.com), or send a letter to Brian Fox, Controller, Kyocera Document Solutions-New England, Inc., One Jewel Drive, Wilmington, MA 01887.

Sincerely,

Brian Fox, Controller

Enclosures

cc: Gerry Mahoney, President