OLENDERFELDMAN LLP
ATTORNEYS AT LAW

Writer's contact information:
908-624-6293
Aaron I. Messing, Esq., CIPP
amessing@olenderfeldman.com
RESPOND TO NEW JERSEY

June 19, 2015

VIA FEDERAL EXPRESS
Attorney General Joseph Foster
Office of the Attorney General
Attn: Security Breach Notification
33 Capital Street
Concord, NH 03301

RE: COA Network - Potential Data Breach

Dear Attorney General Foster:

Please be advised that this firm is counsel to COA Network, Inc. ("COA"), a New Jersey business which provides virtual telephone systems and content management systems to customers throughout the country. This letter is to notify you that on June 5, 2015, COA's IT department detected a pattern of irregular activity affecting our computer systems. We believe this activity was caused by a hacker attempting to access our secure customer account pages using a "brute force" attack, with the ultimate purpose of gaining access to those pages and the customer information contained therein. As soon as COA detected the attack, it immediately took action to increase the security of all customer account pages and correct all security vulnerabilities. As a result, the attack has been halted and we believe that all customer information is now secure. Unfortunately, we believe that the hacker may have gained access to some of our customer's electronically-stored information, which may have included names, email addresses, physical addresses, and payment card numbers and expiration dates.

At this time, we do not have any specific evidence that any customer information belonging to New Hampshire residents has been used by the hacker or otherwise compromised. However, as a precautionary measure, we are treating all customer information contained within COA's systems as being potentially compromised. This includes the information of twenty-three (23) COA customers who identified themselves as New Hampshire residents.

In response to the attack, COA has taken several additional steps to protect customer information beyond enhancing its internal security measures. First, we are working with the payment card companies to prevent any fraudulent activity. Additionally, we are in contact with federal law enforcement officials, who are further investigating the breach incident.

On or about Monday, June 22 we will be notifying all potentially-affected COA customers in New Hampshire about the breach incident and our efforts to remediate the attack. These notifications will contain information on (i) the importance of monitoring payment card accounts and credit reports; (ii) what to do in the event a customer believes they have been the victim of fraud or identity theft; (iii) how to contact credit reporting bureaus to obtain a credit report and place fraud alerts and account freezes on those reports; and (iv) contact information for reporting any incidents of identity fraud to the Federal Trade Commission. A sample of the letter being sent to New Hampshire residents is attached hereto.

We and our client are available to answer any questions or concerns you may have in connection with the potential data breach. Please feel free to contact me directly.

Sincerely,

/s/ Aaron I. Messing

AARON I. MESSING

Enclosures
AIM/fa

June 19, 2015

RE: COA Network - Potential Data Breach

Dear Customer:

COA Network takes the protection of the privacy and security of your data very seriously. On June 5, 2015, our IT department detected a pattern of irregular activity affecting our computer systems. We believe this activity was caused by a hacker attempting to access our secure customer account pages using a "brute force" attack with the ultimate purpose of gaining access to those pages and the customer information contained therein. As soon as we detected the attack, we immediately took action to increase the security of all customer account pages and correct all security vulnerabilities. As a result, the attack has been halted and we believe that your information is now secure. Unfortunately, we believe that the hacker may have gained access to some of our customer's information, which may have included names, email addresses, physical addresses, and payment card numbers and expiration dates.

At this time, we do not have any specific evidence that any of your information has been used by the hacker or otherwise compromised. However, your information was contained in the system which the hacker accessed. Therefore, as a precautionary measure, we are treating all customer information, including yours, as being potentially compromised.

In response to the attack, we have taken several additional steps to protect you and your information beyond enhancing our internal security measures. First, we are working with the payment card companies to prevent any fraudulent activity. Additionally, we are in contact with law enforcement officials, who are further investigating the breach incident.

As a precaution, we recommend that you review your account for any suspicious activity. If you believe that your payment card may have been used for unauthorized charges, you should immediately contact your bank or payment card issuer. Typically, customers are not responsible for any fraudulent charges on their credits cards that are reported in a timely fashion. If you detect any incident of identity theft or fraud, you should promptly report the incident to law enforcement or your state's Attorney General. If you find that your information has been misused, the Federal Trade Commission (FTC) encourages you to file a complaint with the Commission and take these additional steps: (i) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (ii) file and keep a copy of a local police report as evidence of the identity theft crime.

We also recommend that you regularly monitor your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus, regardless of whether you suspect unauthorized activity on your account. To obtain a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

remedy the situation and secure your information. As always, we thank you for being a customer of COA Network.

Very truly yours,

Paul Champaneria
Chief Executive Officer
COA Network

In addition, you can contact any of the three major credit reporting bureaus listed below to request a copy of your credit report. You also may request that the credit reporting bureaus place a "fraud alert" on your file at no charge. A fraud alert requires creditors to take additional steps to verify your identity prior to granting credit in your name for a 90-day period. Please note, however, that these additional verification steps may delay an approval of credit. You may contact the credit reporting bureaus by using the contact information below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can also ask the credit reporting bureaus to place a "security freeze" on your credit report that prohibits them from releasing information from your credit report without your prior written authorization. For more guidance on how you can prevent, respond to, or report identity theft, you may contact the FTC at:

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

Finally, we are available to answer any questions or concerns you may have in connection with the potential data breach. Please feel free to contact COA Network directly at 1-800-454-5930 if you have any questions or concerns. We apologize for any inconvenience this may cause you. Please know that we have been working extremely hard since discovering the attack to remedy the situation and secure your information. As always, we thank you for being a customer of COA Network.

Very truly yours,

Paul Champaneria
Chief Executive Officer
COA Network