ZwillGen

1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296 3585
Website: www.zwillgen.com

Melissa A. Maalouf
PHONE: (202) 706-5212
FAX: (202) 706-5298

May 19, 2021

VIA EMAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

I am writing to inform you that Bose Corporation, located at The Mountain Road, Framingham, MA 01701, experienced a sophisticated cyber-incident that resulted in the deployment of malware/ransomware across Bose's environment. Bose first detected the malware/ransomware on Bose's U.S. systems on March 7, 2021.

Immediately upon discovering the attack on March 7, Bose initiated incident response protocols, activated its technical team to contain the incident, and hardened its defenses against unauthorized activity. In conjunction with expert third-party forensics providers, Bose further initiated a comprehensive process to investigate the incident. Given the sophistication of the attack, Bose carefully, and methodically, worked with its cyber experts to bring its systems back online in a safe manner. As the systems have been restored, Bose has worked with its forensics experts to determine the data that may have been accessed and/or exfiltrated.

During this investigation, on April 29, 2021, Bose discovered that data from internal administrative human resources files relating to 6 former New Hampshire employees of Bose Corporation was accessed and potentially exfiltrated. The personal information contained in these files include name, Social Security Number, and compensation-related information. The forensics evidence at our disposal demonstrates that the threat actor interacted with a limited set of folders within these files. However, we do not have evidence to confirm that the data contained in these files was successfully exfiltrated, but we are also unable to confirm that it was not.

Bose has engaged experts to monitor the dark web for any indications of leaked data, and has been working with the U.S. Federal Bureau of Investigation. Bose has not received any indication through

its monitoring activities or from impacted employees that the data discussed herein has been unlawfully disseminated, sold, or otherwise disclosed.

Bose has also implemented the following measures:

- Enhanced malware/ransomware protection on endpoints and servers to further enhance our protection against future malware/ransomware attacks.
- Performed detailed forensics analysis on impacted server to analyse the impact of the malware/ransomware.
- Blocked the malicious files used during the attack on endpoints to prevent further spread of the malware or data exfiltration attempt.
- Enhanced monitoring and logging to identify any future actions by the threat actor or similar types of attacks.
- Blocked newly identified malicious sites and IPs linked to this threat actor on external firewalls to prevent potential exfiltration.
- Changed passwords for all end users and privileged users.
- Changed access keys for all service accounts.

Bose is offering impacted New Hampshire individuals with identity protection services for 12 months, free of charge, through IdentityForce (a Sontiq brand) – a global leader in identity theft protection, monitoring and restoration.

Bose has sent notification letters about this incident to the affected individuals on May 19, 2021, and a copy of this notification is attached hereto.

Thank you for your attention to this matter. If you have any questions or concerns, do not hesitate to contact me.

Encl: Sample Notice Letter

Sincerely,

Melissa A. Maalouf

Bose Corporation
Corporate Office
The Mountain
Framingham, MA 01701-9168
US
+1 508 879 7330
bose.com

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you that Bose recently experienced a sophisticated cyber-attack that disrupted some of our systems and may have affected the security of certain information maintained about you by Bose. This notice explains the incident, measures we have taken since, and steps you can take in response.

What Happened?

In early March 2021, Bose experienced a sophisticated cyber-attack that disrupted some of our systems. Based on our investigation and forensic analysis, Bose determined, on April 29, 2021, that the perpetrator of the cyber-attack potentially accessed a small number of internal spreadsheets with administrative information maintained by our Human Resources department. These files contained certain information pertaining to employees and former employees of Bose.

We understand this may be of concern. At this time, through our ongoing monitoring activities and investigative work, we have no evidence that this information has been misused or disseminated by third parties.

What Information Was Involved?

The data elements affected by the cyber-attack include your name, Social Security Number, compensation information, and comparable HR-related information.

What We Are Doing

Bose is committed to protecting the confidentiality of the information we maintain. Upon detection of suspicious activity within our digital network, Bose immediately initiated our incident response protocols, activated our technical team to contain the incident and hardened our defenses against unauthorized activity. We also notified the appropriate authorities of this issue as required under applicable law.

What You Can Do

We are offering you identity protection services for 12 months, free of charge, through IdentityForce (a Sontiq brand) – a global leader in identity theft protection, monitoring and restoration. If you have questions about the specific services being offered, please call IdentityForce's Member Services team at 1-877-694-3367 or review their Frequently Asked Questions page: https://www.identityforce.com/support/member-support.

To sign up for IdentityForce theft protection online, please visit: https://secure.identityforce.com/benefit/boseint

Step 1: Enter your First and Last name
Step 2: Enter your Email Address
Step 3: Enter your Verification Code: **<<Member ID>>**
Step 4: Click Continue button
Step 5: Enter the required information on the Personal Information page

Please note. Sontiq's Privacy Policy (https://www.sontiq.com/privacy-policy/) applies to any data you provide to Sontiq in connection with their services. Sontiq processes this data in the United States. Therefore, please read and agree to Sontiq's Privacy Policy prior to enrolling in the service.

Additionally, we recommend that you remain vigilant about the security of your personal information by monitoring your personal accounts and taking action on any suspicious activity.

For More Information

We deeply regret any inconvenience or concern this incident may cause. If you have any questions regarding this incident, please contact the Bose Employee Relations team at Employee_Relations@bose.com or our Data Protection Officer at dataprotectionofficer@bose.com. For more information on how to combat identity theft, please see the information attached to this notice.

Sincerely,

Allisha Elliott
Chief Human Resources Officer

SUPPLEMENTAL INFORMATION

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-685-1111

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. 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. Contact information for the Federal Trade Commission is as follows:

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

State Attorneys General
Information on how to contact your state attorney general may be found at
www.naag.org/naag/attorneys-general/whos-my-ag.php.

If you are a resident of Connecticut, Maryland, Massachusetts, or Rhode Island, you may contact and obtain information from and/or report identity theft to your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your

consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.