PHILIPS

Sent via Fedex Delivery

May 24, 2018

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

Pursuant to N.H. Rev. Stat. §§ 359-C:19 et seq. (C:20, -C:21), we are writing to notify you of an unauthorized access of personal information involving two New Hampshire residents.

The incident which occurred in May 2018 was caused by an unknown actor sending an email to the employees' work email account which requested the employee to click on a link and reveal their personnel account log-in credentials ("phishing incident"). Once done, the unknown actor was able to access the employee's personnel profile information and change the employee's direct deposit instructions to a different financial institution. The personal information that was the subject of the phishing incident included name and financial account information in electronic format.

On May 18, 2018 the two New Hampshire residents affected were sent, pursuant to the New Hampshire statute, a notice letter via FedEx from Philips North America LLC.

Philips takes the security of its systems and the privacy of its employee, customer and consumer data very seriously. As soon as Philips became aware of the incident, it assembled a team and began investigating. Philips has now taken several steps to address this incident as well as combat future incidents.

In particular, Philips has confirmed and reviewed the following administrative, physical and technical measures to ensure similar incidents do not occur. Philips mandates two information security training modules for all employees, which cover information security fundamentals and phishing awareness. The following technical security measures have been instituted: Philips has implemented dual factor authentication, plus an additional authentication requirement for employees to approve any changes to employee personnel accounts. Philips is now reaching out to employees through test phishing emails, email alerts, posters, and through the use of its internal electronic boards to quickly provide notice and education to employees to be vigilant to such email attacks. We do not have information on whether any affected employee reported this incident to law enforcement; however, Philips has advised its employees of their right to contact law enforcement. Additionally, Philips makes available as a benefit to all employees credit monitoring and identity theft remediation services and has specifically notified the affected employees of the steps to take to access this benefit.

If you have any questions, please feel free to reach out to Ellen Giblin, Privacy Officer at 3000 Minuteman Road, Andover, MA 01810 or via e-mail at ellen.giblin@philips.com or by phone at 978-659-4368.

Best regards,

Mary Hofford

Mary Ammon Hofford
Legal Counsel – Privacy NAM
PHILIPS NORTH AMERICA LLC
mary.hofford@philips.com
724-610-8643 (mobile)

Enclosure: Sample Notice Letter

[Insert Date]

Dear [Insert Employee Name],

Re: Notice of Phishing Attack Incident

Philips takes the security of its systems and the privacy of its employee data seriously. Please be assured that we are taking appropriate actions and measures to investigate recurrent phishing attacks on our email systems.

Recently, you were contacted by Philips People Services NA regarding misdirection or the possibility of misdirection of the direct deposit of your paycheck which resulted from an email phishing attack that occurred in May 2018. Philips is reviewing and implementing next steps to protect against these types of attacks as well as further monitoring and protecting the security of our systems. Please remain vigilant of your personal information by reviewing your account statements and monitoring your credit reports offered below.

To protect our employees, Philips offers access to identity theft protection as part of your life insurance benefit from Sun Life Financial in partnership with Assist America. The program for identity theft protection is free to you through the **SecurAssist** program, explained in detail below.

The **SecurAssist** program offers you the following benefits:

- 24x7 telephone support and step-by-step guidance by anti-fraud experts,
- a case worker assigned to you to help you notify the credit bureaus and file paperwork to correct your credit reports,
- help canceling stolen cards and reissuing new cards, and
- help notifying financial institutions and government agencies.

You may also:

- securely store information from credit cards, bank cards, and documents in one safe, centralized location. If any information ever becomes lost or stolen, retrieval is easy and the resolution process can begin.
- register for identity fraud protection surveillance of up to 10 credit or debit cards.
  - Registered cards are monitored using sophisticated real-time early warning technology that monitors underground chat rooms across cyberspace, where thieves are selling and trading stolen personal information.
  - You receive early warning of potential threats and you are notified if your identity has been misused.

Next Steps

SecurAssist Enrollment:

To take advantage of the SecurAssist program for identity theft protection, please follow the information listed below to begin your enrollment.

Identity Theft Protection

If you are the victim of financial or medical identity fraud, or if you'd like to store your card information in one central location, call:

877-409-9597 — 01-AA-SUL-100101 **Membership number**

To proactively protect your credit cards, register them for Identity Fraud Protection surveillance:

www.securassist.com/sunlife — 18327 **Access code**

Additionally, a copy of the brochure further describing your benefits offered through Sun Life Financial which includes Identity Theft Protection as well as Emergency Travel Assistance is enclosed.

Credit Reporting Agencies

If you choose not to utilize the SecurAssist program, you can contact the credit reporting agencies directly at the phone numbers or e-mail addresses listed below:

Equifax
800-349-5191 or equifax.com
TransUnion
800-680-7289 or 888-909-8872 or transunion.com
Experian
888-397-3742 or experian.com

You may also contact the **Federal Trade Commission.**

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.

If you have any further questions about the benefits offered to you, please contact your Philips People Services NA representative at 888-367-7223 Option 5 or for any questions concerning your privacy, please feel free to contact Ellen Giblin, Privacy Officer at ellen.giblin@philips.com.

Best regards,

Bethany Clear
Sr. Manager, HR OPS NA
Attn: PPS Contact Center
511 Union Street
Nashville, TN 37219
629-215-7380