

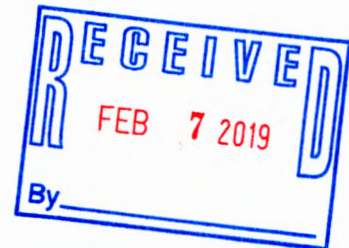
January 30, 2019

WRITER'S DIRECT NUMBER: (317) 236-2391
DIRECT FAX: (317) 592-4736
EMAIL: Stephen.Reynolds@icemiller.com

CONFIDENTIAL

Via Certified Mail

Consumer Protection Bureau
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110



RE: Written Notification of an Information Security Incident

Dear Attorney General:

On behalf of my client, Defenders, Inc. ("Defenders"), I am hereby submitting written notification of an Information Security Incident, in compliance with N.H. Rev. Stat. §§ 359-C:20(I)(b).

We discovered that a very limited number of Defenders' employee email accounts were compromised by an unauthorized third party in or around August 2018. Some of those email accounts were then used to try to direct a "phishing" scheme towards Defenders' employees. As soon as we learned of suspicious activity, we began an investigation. Defenders also hired a leading computer security and forensics firm to assist with the investigation. Among other things, we forced a system wide log out for all employees, required all employees to reset their passwords and engaged leading digital forensics firms to assist us in identifying the scope of the incident and to enhance our security controls to prevent a similar incident in the future. On September 4, 2018, the investigation determined that unauthorized access had occurred and the time period that the unauthorized access affected the few Defenders' employee email accounts. Further investigation determined what information was potentially accessed. The information that may have been accessed included first and last name, and social security number. Following a thorough investigation into the limited number of compromised email accounts, we discovered that personal information was in one of the compromised email accounts. We have no evidence to suggest that the information was actually viewed or collected by any unauthorized third party. However, we are unable to rule out the remote possibility that their personal information was

Consumer Protection Bureau
Office of the New Hampshire Attorney General
January 30, 2019
Page 2

accessed. Therefore, out of an abundance of caution, we are providing consumers with notice in the unlikely event that their information was compromised.

At this time, we believe the security incident may have involved unauthorized access to the information of eight (8) New Hampshire residents. A copy of the notice that will be sent to the eight (8) New Hampshire residents on January 31, 2019 is attached hereto.

If you require further information about this matter, please contact me by telephone at (317) 236-2391 or via email at stephen.reynolds@icemiller.com.

Very truly yours,

ICE MILLER LLP



Stephen E. Reynolds

Attachments: Copy of Notice



DEFENDERS, Inc.
 3750 Priority Way South Drive
 Indianapolis, IN 46240

January 29, 2019

##E3980-L01-0000046 0001 00000001 *****MIXED AADC 159
 SAMPLE A SAMPLE - #6022444



APT ABC
 123 ANY ST
 ANYTOWN, US 12345-6789



NOTICE OF DATA BREACH

Dear Sample A Sample,

We are writing to inform you of a security incident which may have involved some of your personal information. We take the privacy and security of your personal information seriously and for this reason want you to understand what we are doing to address this issue and what steps you can take to protect yourself.

What Happened

We discovered in September 2018 that a very limited number of DEFENDERS' employee email accounts were compromised by an unauthorized third party in or around August 2018. Some of those email accounts were then used to try to direct a "phishing" scheme towards DEFENDERS' employees. Upon discovery we launched further internal investigations in an attempt to determine the full scope of the incident.

What Information Was Involved

Following a thorough investigation into the limited number of compromised email accounts, we discovered that your information was in one of the compromised email accounts. The information that may have been accessed included your first and last name and social security number. We have no evidence to suggest that your information was actually viewed or collected by any unauthorized third party. However, we are unable to rule out the remote possibility that your information was accessed. Therefore, out of an abundance of caution, we are providing you with this notice in the unlikely event your information was compromised.

What We Are Doing

As soon as we learned of suspicious activity, we began an investigation. Among other things, we forced a system log out of all employees, required them to reset their passwords and engaged leading digital forensics firms to assist us in identifying the scope of the incident and to enhance our security controls to prevent a similar incident in the future.

0000046



E3980-L01

What You Can Do

We encourage you to remain vigilant in monitoring your account statements and transactions for incidents of fraud and identity theft, and to promptly report such incidents. While we have no reason to believe that your information was accessed by a malicious party or has been used to engage in identity theft, to help protect your identity, we are offering a complimentary one year membership of Experian's® IdentityWorksSM, at no cost to you. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: April 30, 2019 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/3bplus>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide Engagement Number **DB10210** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-Month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- ◆ **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- ◆ **Credit Monitoring**: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- ◆ **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- ◆ **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- ◆ **Up to \$1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.**

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

For More Information

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. If you want to learn more about the steps you can take to protect against identify theft or fraud, please review the enclosed "Reference Guide" materials. If you have any questions about this security incident, please call 877-890-9332 toll free during weekdays from 9:00am to 9:00pm ET and weekends from 11:00am to 8:00pm ET. The toll free number has been created specifically to answer your questions about the incident and to assist your enrollment in identity repair and credit monitoring services.

Sincerely,

DEFENDERS, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000046



Reference Guide

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "Inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

Security Freezes

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number 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.

As of September 21, 2018, you have the right to request a credit freeze from a consumer reporting agency, free of charge. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze
1-800-685-1111
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-888-909-8872
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than one business day after receiving a request by phone or secure electronic means, and no later than three business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Right to Obtain a Police Report

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of California

Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft.

000046



E3980-L01

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General Consumer Protection Division,
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For Residents of New Mexico

You have a right to place a security freeze on your credit report or submit a declaration of removal with a consumer reporting agency pursuant to the Fair Credit Reporting and Identity Security Act. Please see above for more information on security freezes.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division,
Mail Service Center 9001, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For Residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, Office of the Attorney General,
1162 Court Street NE, Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us

For Residents of Kentucky

You may also obtain information about preventing and avoiding identity theft from the Kentucky Attorney General's Office:

Office of the Attorney General of Kentucky,
700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 1-502-696-5300, www.ag.ky.gov.

For Residents of Iowa

You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division,
1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.

As a resident of Iowa, beginning July 1, 2018, consumer reporting agencies are prohibited from charging you a fee for placing, removing, suspending or reinstating a security freeze.

A security freeze prevents potential creditors and other third parties from accessing credit reports without your approval. Typically, businesses will not open credit card or loan accounts without checking your credit history. You must contact each of the credit reporting agencies individually online or by postal mail.

There is **no cost** to place or lift a security freeze. For more information, see detailed instructions entitled "Placing a Security Freeze on Your Credit Report to Protect Yourself from Identity Theft" at the Iowa Attorney General website at <https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/security-freeze-identity-theft/>.