



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED

JAN 24 2019

CONSUMER PROTECTION

Alexander T. Walker  
Office: 267-930-4801  
Fax: 267-930-4771  
Email: awalker@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

January 18, 2019

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

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

**Re: Notice of Data Event**

Dear Attorney General MacDonald:

We represent Valley Hope Association (“Valley Hope”), located at 103 S. Wabash Avenue, Norton, Kansas 67654, and write to notify your office of an incident that may affect the security of some personal information relating to twenty-five (25) New Hampshire residents. The investigation into this event is ongoing and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Valley Hope does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

#### **Nature of the Data Event**

On October 10, 2018, Valley Hope became aware of unusual activity relating to an employee’s email account. Valley Hope commenced an investigation, which included working with outside forensic specialists, to determine the full nature and scope of the incident. On November 23, 2018, the investigation determined an unauthorized intruder(s) had logged into the employee email account between October 9 - 10, 2018, resulting in a risk of unauthorized access to the email messages and file attachments stored in that email account. On December 14, 2018, after a thorough review of the impacted email account’s contents, the forensic investigators confirmed those contents potentially included sensitive personal information. Since that time, Valley Hope has been working diligently to identify contact information for affected individuals and provide them notice.

Mullen.law

Attorney General Gordon J. MacDonald  
January 18, 2019  
Page 2

The types of personal information potentially impacted in relation to this incident include the following: name and Social Security number.

### **Notice to New Hampshire Residents**

On January 18, 2018, Valley Hope began mailing written notice of this incident to all affected individuals, which includes twenty-five (25) New Hampshire residents. Written notice to the individuals is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

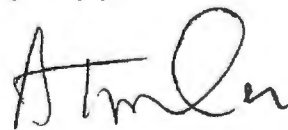
Valley Hope is providing affected individuals access to twelve (12) months of credit monitoring and identity restoration services, through Kroll. Additionally, Valley Hope is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of identity theft and fraud by reviewing account statements and explanation of benefits forms and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Valley Hope is also notifying other state regulators and the three major credit reporting agencies, as well as the U.S. Department of Health and Human Services and prominent media outlets in certain states pursuant to HIPAA requirements, and is posting notice of this incident on its web site homepage.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,



Alexander T. Walker of  
MULLEN COUGHLIN LLC

ATW:mal  
Enclosure

# **EXHIBIT A**



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

## RE: Notice of Data Privacy Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

Valley Hope Association (“Valley Hope”) is writing to make you aware of a recent incident that may affect the privacy of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

**What Happened?** On Oct. 10, 2018, Valley Hope became aware of unusual activity relating to an employee’s email account. We commenced an investigation, which included working with outside forensic specialists, to determine the full nature and scope of the incident. On Nov. 23, 2018, our investigation determined an unauthorized intruder(s) had logged into the employee email account between Oct. 9-10, 2018, resulting in a risk of unauthorized access to the email messages and file attachments stored in that email account. On Dec. 14, 2018, after a thorough review of the impacted email account’s contents, the forensic investigators confirmed they potentially included sensitive personal information. Since that time, we have been working diligently to identify contact information for affected individuals and provide them notice.

**What Information Was Involved?** The patient information present in the impacted emails varied by individual, but the investigation determined that the following types of your information were present in the impacted email account: <<ClientDef1(VARIABLE TEXT FIELD)>><<ClientDef2(VARIABLE TEXT FIELD)>>. Valley Hope wants to stress that ***no diagnosis or treatment information was exposed.***

While this information may have been viewed or acquired by the unauthorized intruder(s), we are not currently aware of any actual or attempted misuse of personal information relating to this incident.

**What We Are Doing.** Valley Hope takes the confidentiality, privacy, and security of information in its care very seriously. Aside from the investigation detailed above, we are taking steps to notify you of this event and provide you with information and access to resources you may use to better protect against potential misuse of personal information, should you feel it appropriate to do so. In addition, we have contacted federal law enforcement authorities.

Valley Hope has created a resource page at <https://valleyhope.org> to help answer further questions and provide guidelines for individuals to help protect themselves from identity theft and what they can do if they believe their personal information has been compromised.

While we have security measures in place to protect information in our care, we are also taking steps to implement additional safeguards and review policies and procedures to further protect the security of information on our systems.

As an added precaution, Valley Hope is providing you with access to 12 months of identity monitoring services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

**What You Can Do.** You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the free identity monitoring services through Kroll.

**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-833-228-5727, Monday through Friday, 8:00 am to 8:00 pm CST.

Please know Valley Hope takes the privacy and security of the personal information in our care very seriously, and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Dan Lara  
Public Affairs Manager

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### **Enroll in Identity Monitoring**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit [my.idmonitoringservice.com](http://my.idmonitoringservice.com) to activate and take advantage of your identity monitoring services.

*You have until April 18, 2019 to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-228-5727. Additional information describing your services is included with this letter.

### **Review Your Credit Report**

Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
(800) 525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
(888) 397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
(800) 680-7289  
[www.transunion.com](http://www.transunion.com)

### **Monitor Your Accounts**

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
P.O. Box 9554  
Allen TX 75013  
(888) 397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
(888) 909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
(800) 685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 9 Rhode Island residents impacted by this incident.



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.