BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

December 18, 2019

VIA EMAIL (*SECURITYBREACH@ATG.WA.GOV)*
Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Dear Sir or Madam:

We are writing on behalf of our client, Vimly Benefit Solutions, Inc. ("Vimly"). Vimly is the third-party administrative manager for the Northwest Fire Fighters Trust ("Trust"). We are writing you to notify you of a security incident involving 3,655 Washington residents who are participants in the Trust and whose protected health information may have been impacted by a recent event at Vimly. Vimly is a business associate of the Trust under the Health Insurance Portability and Accountability Act ("HIPAA").

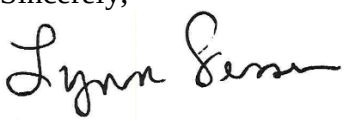
On August 19, 2019, Vimly discovered that an unauthorized individual may have gained access to some Vimly employees' email accounts containing information relating to participants of the Trusts, beginning on August 16, 2019. Vimly immediately took steps to secure the email accounts and began an investigation. A leading cybersecurity firm was engaged to assist in the investigation. The investigation was unable to definitely determine what information, if any, the unauthorized individual may have viewed or accessed in the email accounts. Vimly advised the Trusts of this incident on October 18, 2019. Vimly is offering one year of complimentary credit monitoring, fraud consultation, and identity theft protection service through Kroll to Trust participants whose Social Security number was contained in the email accounts. Vimly has also established a dedicated call center where Trust participants may obtain more information regarding the incident.

On December 18, 2019, Vimly began mailing notification letters to the Washington residents potentially affected by this incident in substantially the same form as the enclosed letter. This notification to the Attorney General is done in compliance with Wash. Rev. Code § 19.255.010. Vimly is offering one year of complimentary credit monitoring, fraud consultation, and identity theft protection service through Kroll to Trust participants whose Social Security number was contained in the email accounts. Vimly has also established a dedicated call center where Trust participants may obtain more information regarding the incident.

To help prevent something like this from happening in the future, Vimly continues to aggressively pursue measures to protect and secure the confidential information in its possession, including pursuing HITRUST certification as evidence of its commitment to security and privacy, as well as reviewing its email protocols and continuously enhancing its security.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Lynn Sessions

Enclosure

NORTHWEST FIRE FIGHTERS BENEFITS TRUST
Administered by Vimly Benefit Solutions, Inc.
P.O. Box 6, Mukilteo, WA 98275
(360) 943-3030

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

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

Re: Potential Disclosure of HIPAA Protected Information (PHI)

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

As we communicated to you previously, Vimly Benefit Solutions ("Vimly") recently experienced a data security incident. Since this incident may have resulted in the inadvertent disclosure of some of your protected health information (PHI), you are receiving this notice.[1]

Information Disclosed:

As we previously advised, a third-party firm conducted an investigation to determine whether any participants in the Trust had their PHI accessed, acquired, used, or disclosed as a result of the Event. This investigation was unable to determine if any information was, in fact, viewed or accessed as a result of the Event. A detailed analysis of the content of the email accounts followed the investigation, and some of your information may have been contained in one of the affected email accounts, including your name, date of birth, benefit enrollment information, social security number and/or address.

Mitigation:

We are not aware of any fraud or misuse of your PHI as a result of this incident. To help relieve concerns and restore confidence following this incident, we have secured the services of a company called Kroll to provide identity monitoring at no cost to you for one year. 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, Fraud Consultation, and Identity Theft Restoration for a period of one year.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
*You have until **<<Date>>** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

We also wanted to advise you that Vimly has assured us that it continues to aggressively pursue measures to protect and secure your personal information, including pursuing "HITRUST" certification as evidence of its commitment to security and privacy, as well as reviewing its email protocols and continuously enhancing its security.[2]

[1] You might receive multiple copies of this same notice if members of your household (including spouses and children) are covered by the Trust. This is required by law. The Board apologizes for any inconvenience this might cause you.

[2]The HITRUST Common Security Framework (CSF) is a comprehensive and certifiable security framework used by healthcare organizations and their business associates to efficiently approach regulatory compliance and risk management. HITRUST unifies recognized standards and regulatory requirements from NIST, HIPAA/HITECH, ISO 27001, PCI DSS, FTC, COBIT, and can be completed according to SOC 2 criteria, making it the most widely adopted security framework in the U.S. healthcare industry.

Contact Information

We regret that this situation has occurred. Should you have any questions, please call 1-???-???-????, from 6:00 a.m. to 3:30 p.m. Pacific Time. The Board is committed to its participants' well-being, including protecting your personal information, and we want to assure you we will continue to do our best to ensure that the Trust's vendors have the most up-to-date policies and procedures to protect your privacy.

Sincerely,

Greg Markley,
Chairman of the Northwest Fire
Fighters Benefits Trust

ADDITIONAL STEPS YOU CAN TAKE

We remind you 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,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO 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

If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from 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, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *Office of the Massachusetts Attorney General,* One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- *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.

If you are a resident of West Virginia, 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 one (1) year. 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,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO 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 hour 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 hour 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.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You’ve been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

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.

[1] Kroll’s activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.