

Appendix

Robin Van Vliet dba Van Vliet Wellness & Insurance Solutions (“Van Vliet”). Van Vliet is an employee benefits insurance broker located in Mill Valley, California.

Upon completing its investigation into the nature and extent of a suspected data security incident, Van Vliet determined that an email phishing attack may have resulted in unauthorized access to emails and attachments in an employee’s email account.

Although no evidence was found during the investigation that indicated that any emails in the employee’s account were in fact viewed or acquired, Van Vliet could not rule out that possibility. Subsequently, Van Vliet conducted a review of the emails and attachments in the email account. The investigation, which Van Vliet concluded on August 13, 2021, determined that an employee’s email account was subject to unauthorized access as a result of the phishing incident on May 5, 2021 and may have contained residents’ names, Social Security numbers, and/or and health insurance information.

On August 27, 2021, Van Vliet provided written notification to the health plans whose members’ information may have been involved in this incident and offered to provide notice to those members and applicable regulatory agencies on their behalf. Between August 27, 2021 and September 13, 2021, the various health plans responded affirmatively to the notification offer.

On September 24, 2021, Van Vliet mailed a notification letter via United States Postal Service First-Class mail to one Maine resident, in accordance with Me. Rev. Stat. Tit. 10, §1348 and 45 C.F.R. § 164.404. Van Vliet is offering the resident a complimentary one-year membership to credit monitoring and identity theft protection services through Kroll. A copy of the notification letter is enclosed.¹ Van Vliet also has established a dedicated, toll-free incident response line to answer questions that individuals may have.

To help prevent a similar incident from occurring in the future, Van Vliet has enhanced its existing security measures.

¹Van Vliet is not licensed with the Maine Bureau of Insurance. This report is not, and does not constitute, a waiver of Van Vliet’s objection that Maine lacks personal jurisdiction over Van Vliet regarding any claims related to this data security incident.



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

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

<<b2b_text_1(SubjectLine)>>

Dear <<first_name>> <<last_name>>:

Robin Van Vliet dba Van Vliet Wellness & Insurance Solutions (“Ms. Van Vliet”) is the employee benefits insurance broker for <<b2b_text_3(EmployerName)>> and helps your employer to administer enrollment for your health insurance plans. We are committed to protecting the security and confidentiality of all the information we maintain. We are writing to inform you about an incident involving some of your health plan information. This notice explains the incident, measures we have taken, and some steps you can take in response. To date, we do not have any evidence that indicates that your information was actually accessed or misused, but we are notifying you of this incident out of an abundance of caution.

What Happened?

On August 27, 2021, we notified your health plan of an email phishing attack that targeted Ms. Van Vliet and may have resulted in unauthorized access to emails and attachments in their email account. Upon learning of the incident, Ms. Van Vliet immediately secured the email account, reset the password to the account, and launched an investigation. The investigation determined that the email account was accessed by an unauthorized party on May 5, 2021 as a result of the phishing attack.

What Information Was Involved?

Although we did not find any evidence that indicates that any emails or attachments in the account were actually viewed or acquired, we could not definitively rule out that possibility. Subsequently, we conducted a review of the emails and attachments in the email account. Based on this review, we determined that emails or attachments in the email account contained information about you, including your name in combination with your <<b2b_text_2(DataElements)>>.

What You Can Do.

As a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please visit the below website and see the additional information provided with this letter.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **December 23, 2021** to activate your identity monitoring services.

Membership Number: <<MembershipNumber (s_n)>>

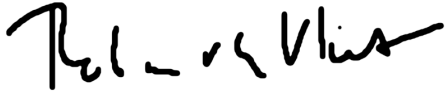
What We Are Doing.

We regret any inconvenience or concern this may cause you. We recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately. To help prevent a similar incident from occurring in the future, we are enhancing our existing security measures.

For More Information.

If you have any questions, please call [1-800-444-4444](tel:1-800-444-4444), Monday through Friday, **8:00 a.m. to 5:30 p.m.**, Pacific Time, excluding major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Robin Van Vliet". The signature is stylized and cursive.

Robin Van Vliet
NIPR# 7091111



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

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

Fraud Alerts: There are two types of general 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 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. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* 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

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. *How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

California Residents: You can obtain additional information from the California Office of Privacy Protection (www.privacy.ca.gov) on protection against identity theft.

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

Maryland: You may contact and obtain information from your state attorney general at: *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