APPENDIX

Benefits Partner, LLC dba Salus Group ("Salus Group") is independent insurance agency that provides insurance brokerage and consulting services.

The subject security incident involved unauthorized access to one employee's email account. Upon first identifying suspicious activity in an employee's account, Salus immediately disabled the account, reset the employee's password, and began an investigation with the assistance of a third-party forensic firm. The investigation determined there was unauthorized access to the account for a period of time on October 9, 2024. The investigation was unable to determine which emails, if any, were viewed by the unauthorized person. Accordingly, Salus conducted a comprehensive review of the contents of the email account. This review included identifying emails and attachments with personal information and cataloging the information. Salus received preliminary results of this review on January 8, 2025. Salus then took steps to determine its relationship with each identified individual; from whom it received the information; and the purpose for which it was received. Salus began notifying applicable data owners (*i.e.*, employer group health plans and insurance carrier partners) on or around March 27, 2025.

Through the review, Salus identified emails and/or attachments containing approximately 1,315 Washington residents' information. The information involved varies by individual, but generally includes names, Social Security numbers, drivers' license numbers, financial account information, and/or health insurance information.

On April 7, 2025, Salus began mailing notification letters via USPS First-Class mail to the Washington residents. A sample copy of the notification letter is enclosed. Salus is offering individuals a complimentary membership to credit monitoring and identity theft protection services through Kroll. Salus has also established a dedicated, toll-free call center to help answer any questions individuals may have.

To help prevent a similar incident from occurring in the future, Salus has made security enhancements to its email environment.

SALUS GROUP

<<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(Notice of Data Breach)>>

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

Benefits Partner, LLC dba Salus Group is an independent insurance agency that provides insurance brokerage and consulting services. We are committed to protecting the confidentiality and security of the information we maintain. Regrettably, we are writing to inform you of an incident involving some of your information, which we received from your current or former employer and/or insurance carrier in connection with the services we provide. This notice describes the incident, outlines the measures we have taken in response, and provides steps you can take to further protect your information.

What Happened? On October 9, 2024, we identified suspicious activity in one employee's email account. We immediately disabled the account, reset the employee's password, and began an investigation with assistance from a third-party forensic firm. Through the investigation, we determined that there was unauthorized access to the account for a period of time on October 9, 2024. The investigation was unable to determine which emails, if any, were viewed by the unauthorized person. Accordingly, we conducted a comprehensive review of the contents of the email account. We completed our analysis of the data involved in late February 2025 and began informing employers and insurance carriers of the incident on or around March 27, 2025.

What Information Was Involved? Through our review, we identified emails and/or attachments containing some of your information, including your <<b2b_text_2(data elements)>>.

What We Are Doing. As a precaution, we wanted to notify you of this incident and assure you we take this matter very seriously. We have arranged for you to receive a <<Monitoring Term Length (Months)>> month complimentary membership to identity monitoring services through Kroll. The identity monitoring services we are making available include credit monitoring, fraud consultation, and identity theft restoration. Additionally, to help prevent a similar incident from occurring in the future, we implemented additional security controls in our email environment and are providing employees with further training on how to identify and avoid suspicious emails.

What You Can Do. It is always a good idea to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. 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 pages that follow this letter.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For More Information. We regret that this incident occurred and apologize for any inconvenience. If you have questions, please call (866) 408-1493, Monday through Friday, between 9:00 a.m. and 6:30 p.m., Eastern Time, excluding major U.S. Holidays.

Sincerely,

Salus Group

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 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.identitytheft.gov

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.

Benefits Partner, LLC can be reached by mail at 38233 Mound Rd., Building F, Sterling Heights, MI 48310 or by phone at (866) 991-9907.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.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.

Massachusetts: Under Massachusetts 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, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

New York: 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.

North Carolina: You may contact and obtain information from your state attorney general at: *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: Approximately 41 Rhode Island residents are receiving notice of this incident. Under 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, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

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). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, 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.