POLSINELLI

2100 Southbridge Pkwy, Suite 650, Birmingham, AL 35209

April 1, 2024

VIA FEDERAL EXPRESS
The Honorable John Formella
Consumer Protection Bureau,
Office of the Attorney General
33 Capital Street
Concord, NH 03301

Re: Notice of a Security Incident

Dear Attorney General Formella:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, I am writing to report a security incident on behalf of our client, HALO Branded Solutions ("HALO" or the "Company"). On or around November 22, 2023, HALO Branded Solutions ("HALO" or the "Company") experienced a security incident that resulted in unauthorized access to some of its computer systems. Upon discovering the situation, HALO immediately took these systems offline, notified law enforcement, and engaged external cybersecurity experts to investigate.

The Company's investigation subsequently determined on February 21, 2024 that the threat actor accessed files containing personal information of certain individuals provided to HALO for tax or benefits purposes, including nineteen (19) New Hampshire residents. The information included individuals'

HALO notified affected individuals on March 28, 2024 to inform them of the situation and provide resources to monitor and protect their personal information, including of complimentary credit and identity monitoring services. A copy of the individual notice is enclosed.

HALO has been supporting federal law enforcement's criminal investigation. The Company has been and will continue working with cybersecurity experts to strengthen its cybersecurity defenses, and has retained a third-party service to monitor online forums and marketplaces for any information relating to this event. To date, HALO has found no evidence that any files, including those containing personal information, have been published or misused.

Sincerely,

Todd Panciera, Jr.

Enclosure

HALO
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08669 13-1

[redacted]

March 28, 2024

Re: Notice of Security Incident

Dear [redacted]:

As you may be aware, HALO experienced a security incident in November 2023 that resulted in unauthorized access to some of our computer systems. We have now completed our review of the files contained on these systems, and have identified some personnel records, including your information.

We have been investigating this situation with the help of law enforcement and external cybersecurity experts. To our knowledge, we are not aware of any actual or attempted misuse of personal information as a result of this incident. However, as a precautionary measure, you can enroll in an identity protection solution from Cyberscout at no cost to you. HALO will provide these credit and identity protection services to you for free of charge.

Additional information about the incident, our ongoing response, and the resources that are available to help protect your information can be found below. Please know that we have taken a number of steps to address this situation, and we are committed to doing the right thing for everyone involved.

What Happened? Computer systems within our network were accessed by a sophisticated threat actor using techniques to evade detection by our information security defenses. Upon discovering the situation, we promptly took these systems offline, notified law enforcement, and engaged cybersecurity experts to investigate. Through those efforts, we recently learned that a criminal threat actor had access to computer systems containing your personal information in November 2023 and acquired files containing your personal information. We have recovered the files.

What Are We Doing? We have been working with external cybersecurity experts to investigate what happened, to strengthen our computer network, and to monitor the "dark web" for information relating to our company. These efforts are all ongoing. We are notifying you now that we know what information was involved.

What Information Was Involved? Information provided to HALO Human Resources for tax or benefits purposes, including .

What You Can Do? We are providing an Identity Protection Reference Guide that includes information on general steps you can take to monitor and protect your personal information. You will also find information enclosed on how to enroll in the credit and identity protection services if you are interested in these services.

For More Information. If you have any questions or concerns, please review the FAQs below or reach out to our dedicated support team at 1-833-914-4069, Monday through Friday 8:00 am – 8:00 pm EST, (excluding major U.S. holidays).

Thank you for all you do for HALO.

Sincerely,

Marc S. Simon
CEO

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (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.

If you see anything in your credit report that 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.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

It is only necessary to contact <u>one</u> of these bureaus and use only <u>one</u> of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact <u>each</u> of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no cost to place a security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438- 4338); and TTY: 866-653-4261. The

Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov/.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-866-366-8343 or (410) 576-6491, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

Rhode Island Residents: You can obtain additional information about identity theft prevention and protection from the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. There are approximately 13 Rhode Island residents that may be impacted by this event.

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

We are offering you complimentary access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To activate your membership and start monitoring your credit, please follow the steps below:

- Ensure that you **enroll within 90 days from the date of this letter** (Your code will not work after this date.)
- **Visit** the Cyberscout website to enroll: [redacted]
- Provide your **unique code**: [redacted]

The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. **Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.**

Frequently Asked Questions

- **Q: When did this happen?**
- **A:** HALO IT detected suspicious activity within a portion of its network on November 22, 2023. That is when we started the investigation, but we only recently learned that files copied off our servers contained your personal information.

- **Q: Why am I just learning about this now?**
- **A:** As part of the investigative process, experts hired by HALO conducted a thorough review of the files that were stored on the affected HALO systems to determine what information may have been impacted. These investigations take time. We only recently learned that your information was involved.

- **Q: Has my personal information been misused?**
- **A:** At this time we are not aware of any actual or attempted misuse of personal information.

- **Q: What if I'm already enrolled in another credit monitoring service?**
- **A:** You are still welcome to enroll in the credit monitoring and identity protection service we are offering free of charge.

- **Q: What if someone outside the Company contacts me about this matter?**
- **A:** Please let us know immediately by reaching out to our internal team at