## Appendix

On March 17, 2022, Orange Silicon Valley, LLC (OSV), a nonsubsidiary affiliate of Orange Business Services U.S., Inc. ("OBS"), learned that an unauthorized individual accessed several OSV servers on January 4, 2022, by exploiting a vulnerability in a third-party firewall device. Upon discovery, the firewall device was removed from the network and an investigation was commenced to determine what happened and what information may have been accessed by the unauthorized individual. That investigation was unable to determine the specific files accessed by the unauthorized party. However, on May 20, 2022, OSV learned that one of the accessed servers contained information about employees of OBS, and on or around June 8, 2022, OBS learned that the same server contained information about employees of certain OBS affiliates. Therefore, OBS is notifying any current or former OBS or OBS-affiliate employee whose personal information was stored on the server that was accessed. OSV notified OBS about the security incident and the potential impact on information about OBS employees on May 23, 2022, which was the next business day after OSV learned that one of the accessed servers contained information about employees of OBS. The accessed server stored certain information relating to participants in the employee benefit programs sponsored by OBS and include the name, date of birth and Social Security number of nine Maine residents.

Today, OBS began mailing notification letters to the Maine residents via U.S. mail. A copy of the notification letter is enclosed. OBS is providing individuals a one-year complimentary membership to identity monitoring services through IDX and is providing a toll-free phone number for potentially affected individuals to call with any question they may have about the incident.

To help prevent something like this from happening in the future, OBS has confirmed with OSV that they have discontinued the use of the subject firewall, have removed from their servers any data relating to employees of OBS or OBS affiliates and that they have implemented additional measures to enhance their security protocols.

orange™ Business Services
400 Carillon Parkway
Suite 225
St Petersburg, FL 33716

To Enroll, Please Call:
1-833-423-2920
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

August 3, 2022

**Notice of Data Breach**

Dear <<First Name>> <<Last Name>>:

Orange Business Services U.S., Inc. (OBS) is writing to inform you of a security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and additional steps you may consider in response.

***What Happened?*** On March 17, 2022, Orange Silicon Valley (OSV), a nonsubsidiary affiliate of OBS, learned that an unauthorized individual accessed several OSV servers on January 4, 2022, by exploiting a vulnerability in a third-party firewall device. Upon discovery, the firewall device was removed from the network and an investigation was commenced to determine what happened and what information may have been accessed by the unauthorized individual. That investigation was unable to determine the specific files accessed by the unauthorized party. However, on May 20, 2022, OSV learned that one of the accessed servers contained information about employees of OBS, and on or around June 8, 2020, OBS learned that the same server contained information about employees of certain OBS affiliates. Therefore, we are notifying any current or former OBS or OBS-affiliate employee whose personal information was stored on the server that was accessed. OSV notified OBS about the security incident and the potential impact on information about OBS employees on May 23, 2022, which was the next business day after OSV learned that one of the accessed servers contained information about employees of OBS.

***What Information Was Involved?*** The accessed server stored certain information relating to your participation in employee benefit programs sponsored by OBS and may include your name, date of birth, and Social Security number.

***What Are We Doing?*** To help prevent something like this from happening in the future, we have confirmed with OSV that they have discontinued the use of the subject firewall, have removed from their servers any data relating to employees of OBS or OBS affiliates and that they have implemented additional measures to enhance their security protocols. As a precaution, we are offering you a complimentary <<12/24>> month membership in identity theft protection services through IDX. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

***What You Can Do?*** We encourage you to remain vigilant against the possibility of fraud and identity theft by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact the relevant financial institution immediately. You may also enroll in the free credit monitoring that we are providing. For more information on free identity protection services, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the pages that follow this letter. Please note the deadline to enroll is November 3, 2022.

We regret this incident occurred and apologize for any inconvenience. If you have any questions, please call our dedicated call center at 1-833-423-2920, Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Sincerely,

**Jenny Adams**
Head of Human Resources, North America

**ENROLLMENT INSTRUCTIONS**

**1**. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-833-423-2920 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

**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 and Credit or Security Freezes:**

***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**

**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

**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, 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:** This incident involves 7 individuals in Rhode Island. 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