Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

November 1, 2023

By Electronic Mail: *attorneygeneral@doj.nh.gov*

The Honorable John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident

Dear Attorney General Formella:

We write on behalf of Okta, Inc. ("Okta"), with headquarters located at 100 First Street, San Francisco, CA 94105, to provide you with notice regarding a data security incident experienced by Okta's third-party vendor, Rightway Healthcare, Inc. ("Rightway"), that has impacted the personal information of New Hampshire residents. Rightway is a vendor used by Okta to provide its employees and their dependents with support in finding healthcare providers and rates.

On October 5, 2023, Rightway informed Okta that as a result of a targeted SIM swap attack on one of its employees, an unauthorized actor gained access to an eligibility census file maintained by Rightway in its provision of services to Okta. Rightway has indicated that the impacted file was accessed on September 23, 2023. Upon discovering the incident, Okta promptly launched an investigation and reviewed the affected file to determine the extent of impact to Okta's current and former employees, and their dependents. On October 12, 2023, the investigation revealed that the impacted file contained the following types of personal information of 16 New Hampshire residents: .

Okta regularly reviews and updates the measures it takes to protect personal information. Upon discovering this incident, Okta launched an investigation and worked with Rightway to assist Rightway in confirming that there was no further impact to Rightway systems or the personal information maintained by Rightway on Okta's behalf.

Okta will notify affected New Hampshire residents via first class mail on November 2, 2023, offering of complementary IdentityWorks credit monitoring, identity restoration, and fraud detection services through Experian. Enclosed is a sample notification letter being sent to affected individuals.

If you should have any questions, or if we can provide further assistance to the New Hampshire residents affected by this incident, please feel free to contact me.

Sincerely,

Bret Cohen

okta

[DATE]

[First Name] [Last Name]
[Mailing Address]
[City, State, ZIP]

RE: Notice of Data Breach

Dear [Name],

We write to share important information with you about a recent data security incident experienced by our third-party vendor, Rightway Healthcare, Inc. ("Rightway"), that may have impacted your personal information. Rightway is a vendor used by Okta, Inc. ("Okta") to provide support to our employees and their dependents in finding healthcare providers and rates. We are providing you with this notice so that you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? On October 12, 2023, Rightway informed Okta that an unauthorized actor gained access to an eligibility census file maintained by Rightway in its provision of services to Okta. Upon discovering the incident, we promptly launched an investigation and reviewed the affected file to determine the extent of the impact to our current and former employees, and their dependents. The investigation revealed that your personal information was contained in the impacted file. Rightway has indicated that the unauthorized activity occurred on September 23, 2023.

What Information Was Involved? The types of personal information contained in the impacted eligibility census file included your . We have no evidence to suggest that your personal information has been misused against you.

What We Are Doing. Okta regularly reviews and updates the measures it takes to protect your personal information. While we have no evidence that your personal information has been misused, as an added precaution, we are making available to you access to 24 months of complementary credit monitoring, identity restoration, and fraud detection services, through a product called IdentityWorks, offered by Experian.

What You Can Do. We encourage you to enroll in the free IdentityWorks services by visiting http://www.experianidworks.com/3bcredit or calling . To enroll, you must provide the following activation code [Activation Code]. This code is unique for your use and should not be shared. Please note that the deadline to enroll is [Date]. You may also consult the resources included on the enclosed form, which provides additional information about protecting your personal information.

For More Information: For general questions about the incident, please contact our dedicated call center at [Telephone Number] [Call Center Hours].

We would like to reiterate that the security of your personal information is among our highest priorities. We sincerely regret any inconvenience caused to you by this incident.

Sincerely,

Ronald Anderson

Ronald Anderson
Director and Legal Counsel - Cybersecurity
Okta, Inc.

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

It is necessary to contact only ONE of these bureaus and use only ONE 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 will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

If you are a resident of the District of Columbia, Iowa, Maryland, North Carolina, New York, Rhode Island, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below to obtain information about preventing and avoiding identity theft and fraud. All other state residents can find information on how to contact your state attorney general at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP
(382.4357)/
https://www.consumer.ftc.gov/identity-theft-and-online-security

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 /
https://justice.oregon.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755/
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400/
https://ncdoj.gov/protecting-consumers/identity-theft/

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400/oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023/
www.marylandattorneygeneral.gov

Consumer Protection Division Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926/
www.iowaattorneygeneral.gov

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400/
https://riag.ri.gov/