



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street Suite C-402
Brooklyn, NY 11201
dcmcmillan@constangy.com

October 17, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 410-576-6491
Email: Idtheft@oag.state.md.us

Re: Ora, LLC - Notice of Data Security Event

Dear Attorney General Brown:

We represent Ora, LLC (“Ora”) located at 138 Haverhill Street Suite 102 Andover, Massachusetts 01810, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately eight (8) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ora does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of Incident

On May 10, 2024, Ora received information suggesting that certain data stored within its network may have been downloaded without authorization by unknown actors. Ora immediately commenced an investigation, aided by independent cybersecurity experts to determine what happened and whether any sensitive data was affected. Ora’s investigation confirmed the unauthorized actors gained access to a limited portion of Ora’s digital network may have accessed and / or downloaded certain files in the process. Ora has undertaken a comprehensive review of the impacted files to determine precisely what data may have been available. On August 26, 2024, Ora confirmed that certain personal information may have been involved in this incident.

The impacted information may include the residents’ names along with their Social Security number, and driver’s license number.

2. Number of Maryland Residents Affected

On or about October 17, 2024, Ora provided written notice of this incident to approximately eight (8) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Steps Taken Relating to the Incident

As soon as Ora discovered the incident, it took the steps described above. Ora has also taken steps to further bolster the security of its network and reduce the likelihood of a similar incident occurring in the

future. In addition, Ora is offering affected individuals complimentary credit monitoring and identity protection services. Ora has also provided guidance on steps individuals can take to protect personal information.

4. Contact Information

Ora takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 718.614.8371 or dmcmillan@constangy.com.

Sincerely yours,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan of

CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter

Exhibit A



<<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 (Re: Notice of [Data Breach/Potential Security Incident])>>

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

Ora, LLC ("Ora") is writing to inform you of a data security incident that may have involved your personal information. At Ora, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident out of an abundance of caution, providing you with steps you can take to help protect your personal information, and offering you the opportunity to activate complimentary identity monitoring services.

What Happened? On May 10, 2024, we received information suggesting that an unknown cybercriminal had claimed to have downloaded certain data from our network. We immediately commenced an investigation, aided by independent cybersecurity experts to determine whether these claims had any credibility and, if so, whether any sensitive data was potentially affected. Our investigation did not uncover any evidence that the bad actor's claims of data theft were legitimate. Nonetheless, out of an abundance of caution, we undertook a comprehensive review of the files that were purportedly downloaded in order to identify any personal information that may have been involved. We completed our analysis on August 26, 2024 and confirmed that your personal information was included in the files that the bad actor claimed to have downloaded.

What Information Was Involved? The potentially affected information includes your name along with your <<b2b_text_2 (exposed data elements)>>. We emphasize that Ora has no evidence your information was taken by the bad actor. This notification is being provided because your information was included in the files the bad actor *claimed* to have downloaded.

What We Are Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- 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 about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to activate the complimentary identity monitoring services we are offering. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: Kroll representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at <<phone number>>.

We thank you for your understanding deeply regret any worry or inconvenience that this may cause.

Very truly yours,

Ora, LLC

138 Haverhill Street

Suite 102

Andover, Massachusetts 01810

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION



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.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>