



Randy V. Sabett
T: +1 202 728 7090
rsabett@cooley.com

September 01, 2023

VIA EMAIL

Office of the Attorney General
ldtheft@oag.state.md.us
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

On behalf of Nextiva Inc. ("Nextiva"), a Voice over Internet Protocol (VoIP) phone service provider, I write to inform you of an incident involving unauthorized access to certain personal information of four (4) Maryland residents. Attached please find a copy of the letter Nextiva is sending to the affected individuals with information about this incident and the steps the affected individuals may take to protect themselves.

Between January 14 and 15, 2020, Nextiva investigated reports of phishing emails that caused the company to investigate the possibility that accounts had been compromised. Nextiva began analyzing Office 365 (O365) email logs and application permissions for potentially suspicious access. Nextiva identified a small number of users who had fallen victim to a phishing attack that granted "Email Client" access to their mailboxes between November 19 and December 9, 2019. Nextiva identified other users that had fallen victim to other phishing attacks who had unauthorized logins to their O365 accounts. Of the affected users, the company's forensic investigation revealed that nine users potentially had emails exposed. However, no evidence of actual exposure or exploitation of data has been identified. Emails for those users were then analyzed for any potential personal information that may have been in the emails. Nextiva's forensic investigation determined that the individuals' financial account numbers (without a password or routing number) and social security number may have been exposed.

Nextiva responded by removing permissions for the O365 app, preventing all users from granting app access permissions, and enforcing multifactor authentication (MFA) on all O365 logins. Nextiva switched to Okta federated identity with enforced MFA. Notably, the breach occurred during the global pandemic and Nextiva's investigation (and subsequent notification efforts) were significantly hampered.

Nextiva will notify the four Maryland residents of the incident via mail on or around September 01, 2023. All notified individuals will be offered two years of free credit monitoring and identity theft protection services through Experian.

Enclosed please find a sample notice letter to the Maryland residents.

Should you have any questions, please contact me at rsabett@cooley.com or at 202-728-7090.



September 01, 2023
Page Two

Best regards,

A handwritten signature in blue ink, appearing to read "RS", is positioned above the name.

Randy V. Sabett

Encl.

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589



September 1, 2023

J8631-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to notify you of a data breach involving your personal information. You are receiving this notice because your personal information may have been affected by this incident. Please read this notice carefully to learn more about the incident and what you can do to protect yourself.

What Happened?

In January 2020, we became aware of unauthorized access to a small number of Nextiva user email accounts. Based on our subsequent investigation, we further determined that a bad actor had gained access to emails containing personal information.

What Information Was Involved?

Through our investigation, we determined that bad actors may have been able to access your name, address, social security number, driver license number, passport number, or health information.

What We Are Doing

We took steps to address these incidents including, among other things, initiating an internal investigation, engaging (a) a world-class cybersecurity services provider to perform a thorough forensic examination of our systems and data and (b) a data analysis company to isolate and identify personal information that may have been exposed in this incident.

What You Can Do

We encourage you to carefully review the Additional Information appendix to this letter, as it contains information about the steps you can take to protect yourself against fraud and identity theft. We are offering all affected individuals two (2) years of complimentary credit monitoring and identity protection services. Please review the enrollment instructions provided below for activating these services. Please note that you must activate these services prior to the enrollment deadline provided with the enrollment instructions.

For More Information

If you have any further questions regarding this incident, please reach out to us privacy@nextiva.com.

Sincerely,

Nextiva



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by November 30, 2023. Be prepared to provide engagement number **B098189** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL INFORMATION

- **Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft. The FTC can be reached at: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For Massachusetts Residents: By law, you have a right to obtain a police report filed relating to these incidents (if any), and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You also have the right to request a security freeze, as described below. You may contact and obtain information from the Massachusetts 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.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

- **Security Freezes and Fraud Alerts:** 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and



enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the following national credit reporting agencies:

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241, Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:

P.O. Box 740256, Atlanta, GA 30374

Experian

(www.experian.com)

General Contact:

P.O. Box 2104, Allen, TX
75013

888-397-3742

**Fraud Alerts and Security
Freezes:**

P.O. Box 9556, Allen, TX
75013

TransUnion

(www.transunion.com)

**General Contact, Fraud Alerts
and Security Freezes:**

P.O. Box 2000, Chester, PA
19022

800-916-8800