



mwe.com

Edward Zacharias
Attorney at Law
ezacharias@mwe.com
+1 617 535 4018

September 15, 2023

VIA E-MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Data Security Incident

Dear Attorney General Anthony G. Brown:

We write on behalf of Nuance Communications, Inc. (“Nuance”), a leading provider of speech recognition and AI-solutions software to hospitals and healthcare plans. Nuance was recently the victim of a security incident resulting from a zero-day remote code execution vulnerability in Progress Software Corporation’s (“Progress Software”) MOVEit Transfer secure file transfer application. On behalf of Nuance and the Nuance customers listed below, we write to provide you notice of the incident and inform you that Maryland residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On or around May 28, 2023, a cyber threat actor exploited a zero-day remote code execution vulnerability in Progress Software’s MOVEit Transfer application (“MOVEit”) to access the MOVEit instances of Progress Software customers. Nuance used the MOVEit Transfer application to securely exchange files with certain customers, including the organizations listed on Appendix A. Nuance and these customers are among the thousands of organizations around the globe impacted by the Progress Software incident. On May 28 and 29, 2023, the threat actor leveraged the vulnerability to download files from Nuance’s MOVEit instance. On May 31, 2023, Nuance became aware that Progress Software was experiencing a security incident that impacted its MOVEit customers. Nuance immediately followed Progress Software’s and security industry guidance to secure its MOVEit servers and launched an investigation. The incident was limited to Nuance’s MOVEit application. There is no evidence that the threat actor moved laterally to other applications or systems within the Nuance environment. The incident did not affect any Nuance products.

What Information was Impacted? The MOVEit security incident impacted Nuance customer data, including certain personal information. With respect to customers that have authorized Nuance to make

regulatory disclosures on their behalf, the incident impacted the medical or healthcare information of approximately 23 residents of this jurisdiction. The incident did not impact the medical records, radiology images, Social Security Numbers or financial account information of residents of this jurisdiction.

Appendix A lists the impacted Nuance customers that have requested that Nuance provide notice to this office.

Steps Nuance has taken. When Nuance learned that Progress Software was experiencing a security incident, it immediately followed Progress Software's and security industry guidance to secure its MOVEit application, and launched an investigation, which is being conducted with the assistance of Microsoft, outside cybersecurity experts, and McDermott Will & Emery LLP. Nuance also promptly notified the Federal Bureau of Investigation ("FBI") and has worked cooperatively with the FBI's investigation into this cyber attack that affected thousands of organizations globally.

Nuance followed Progress Software's and security industry guidance, including temporarily taking MOVEit servers offline when additional critical vulnerabilities were identified, and promptly installing patches as soon as they were available.

Nuance undertook the significant effort of analyzing the impacted data in order to identify impacted customers and their affected data. Nuance first confirmed that medical and healthcare information was impacted beginning on or around July 10, 2023, and on an ongoing basis thereafter as its investigation progressed. Nuance notified impacted clients on a rolling basis beginning on July 21, 2023, and has been in frequent communications with them to support their response efforts. The last customer identified as having been impacted by the incident was discovered by Nuance on September 5, 2023.

Nuance offered to support its impacted healthcare customers by offering to make any notifications the customers determined were required or appropriate under applicable laws, including the Health Insurance Portability and Accountability Act, as amended ("HIPAA"). At the request and under the authorization of certain impacted clients, Nuance notified the following entities beginning on or around September 8, 2023: the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"); applicable state regulators, including certain Attorneys General; prominent media outlets pursuant to HIPAA; and the consumer reporting agencies.

At the request and under the authorization of certain impacted clients, Nuance will begin notifying impacted individuals on or around September 18, 2023. Impacted individuals will receive written notice pursuant to the enclosed notification letter template. Certain individuals will also receive substitute notice through the Nuance website at <https://www.nuance.com/moveit-support.html>.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter. You may also contact our impacted customers directly at the contacts listed in Appendix A.

Attorney General Brown
September 15, 2023
Page 4

Sincerely,

Edward Zacharias

cc: Jean Liu
Chief Privacy Officer
Nuance Communications, Inc.
jeanliu@microsoft.com

Appendix A: Impacted Nuance Customers Giving Notice to Maryland

Company Name	Company Contact	Impacted Maryland Residents	Impacted Data Types
Athens Orthopedic Clinic	Teresa Tolleson 706-433-4097 ttolleson@athensorthopedicclinic.com	1	Name, details about radiology studies received (description of the study, date of service, provider and facility name, and study identifiers); for some individuals, medical record number (MRN)
Washington Radiology	Michelle Duhe Chief Compliance Officer 469-398-4134 compliance@solismammo.com	22	Name, details about radiology studies received (description of the study, date of service, provider and facility name, and study identifiers); for some individuals, medical record number (MRN)

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

Nuance Communications, Inc. (“Nuance” or “we”) provides solutions to share radiology documentation among your healthcare providers, including <<Consolidated BE- CE_Name_1>>. We place high value on maintaining the privacy and security of the information we maintain for our customers. This letter is to inform you that a third-party vendor we used was recently the victim of a security incident, which impacted some of your personal information. Importantly, we have no evidence that your information has been subject to fraud as a result of this incident. This letter explains the third-party incident, the measures we have taken in response and the steps you can take.

What Happened? We use software made by a third-party company named Progress Software Corporation (“Progress Software”) called MOVEit Transfer, which is widely used by organizations to securely transfer files. On May 31, 2023, Progress Software told us about a previously unknown vulnerability in their software that allowed an unauthorized third party to take information from the MOVEit Transfer software. Upon being told about Progress Software’s incident, we immediately took steps to secure our systems and launched an investigation. Our analysis of the MOVEit Transfer environment found that the unauthorized third party took data between May 28 and May 29, 2023. On <<Var Data 3 -CE discovery_date>>, Nuance confirmed as part of our investigation that, unfortunately, a limited amount of your personal information within audit logs was affected by the Progress Software incident. After gathering all relevant information, we told << Var Data 2- CE Name 2>> about this incident on <<CM dur - CE Notice Date>>.

What Information Was Involved? The personal information involved included your name and details about radiology studies you received, including a description of the study, date of service, provider and facility name, and study identifiers. It may have included your medical record number. Importantly, it did **not** involve or include your medical record or radiology images, Social Security number, or any of your financial information.

What Are We Doing? Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering that Progress Software was experiencing a security incident, we immediately took steps to secure the servers running the MOVEit Transfer application and worked with cybersecurity experts and legal counsel to conduct a comprehensive investigation of the incident and notify affected customers. We also notified law enforcement authorities.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information.

For More Information. Your privacy is of utmost importance to us, and we deeply regret that we were impacted by Progress Software’s security incident and any concern it may cause you. If you have questions, please call our dedicated, toll-free call center at 888-988-0380, Monday through Friday between 8:00 a.m. and 8:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,



Umar Waheed
Chief Information Security Officer
Nuance Communications, Inc.

Group Code:<<CE CODE>

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 916-8800

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

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

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, 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.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Kentucky resident, you can obtain information about steps you may take to avoid identity theft from following sources: the FTC (see contact information above), the major consumer credit reporting agencies (see contact information above), and the Office of the Kentucky Attorney General: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, www.ag.ky.gov, 1-888- 432-9257.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. 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: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.