Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 22, 2023

VIA E-MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Supplemental Notice of Data Event

To Whom it May Concern:

We represent Welltok, Inc. ("Welltok") located at 1515 Arapahoe St. #700, Denver, CO, 80202. Welltok operates a voluntary online wellness program used by healthcare providers and employers that encourages healthy lifestyle changes. Additionally, Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications. We are writing to supplement our previous notifications to your office. Welltok is reporting this incident on behalf of United Healthcare Services, Inc. who owns the data at issue. By providing this notice, Welltok does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 26, 2023, Welltok was alerted to an earlier alleged compromise of its MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. Welltok had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool. Welltok also conducted an examination of its systems and networks using all information available to determine the potential impact of the published vulnerabilities presence on the MOVEit Transfer server and the security of data housed on the server. Welltok confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, Welltok moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of its systems and historical data, the investigation determined on August 11, 2023, that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. Welltok subsequently undertook an exhaustive and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. On December 4, 2023, United Healthcare Services, Inc. learned the scope of the data present on the impacted server at the time of the event. Since then, Welltok has been coordinating efforts with the impacted data owner(s) to review and verify the affected information and provide direct notice to impacted individuals.

The information that could have been subject to unauthorized access includes name addresses, dates of birth, member and/or Medicaid ID numbers, and health insurance coverage type.

Supplemental Notice to Washington Residents

On or about September 22, 2023, Welltok provided notice of this event to affected clients with an offer to provide notification services to potentially impacted individuals on their behalf and at their direction. On or about December 22, 2023, Welltok began providing written notice of this event to potentially impacted individuals on behalf of its clients, which own the data at issue. This mailing includes notice to approximately nine thousand nine hundred thirty-eight (9,938) Washington residents.

Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Welltok moved quickly to investigate and respond to the event, assess the security of its systems, and notify potentially affected individuals. Welltok is providing access to credit monitoring services for twelve (12) to twenty-four (24) months, depending on state law requirements, through Experian, to individuals whose personal information was potentially impacted by this event, at no cost to these individuals.

Additionally, Welltok is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Welltok is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade

Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/kzm

EXHIBIT A

Welltok

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

December 22, 2023

K5504-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

Notice of Data Breach

Dear Sample A. Sample:

Welltok writes to inform you of an event that may affect the security of your health information. Welltok provides a variety of wellness-related communication services on behalf of UnitedHealthcare and received your information in connection with same. We are providing you with information about the incident, our response to it, and resources available to you to help protect your data, should you feel it appropriate to do so.

What Happened. On May 31, 2023, Progress Software announced it discovered a previously unknown ("zero-day") vulnerability in the MOVEit transfer tool software that could allow an unauthorized party to access files. On July 26, 2023, Welltok learned that its MOVEit Transfer server may have been impacted by exploitation of the vulnerability and initiated an investigation with the assistance of third-party cybersecurity specialists. On August 11, 2023, Welltok determined that an unknown actor exploited the software vulnerability between May 30, 2023 – May 31, 2023, accessed the MOVEit Transfer server, and exfiltrated certain data during that time. Welltok continued to work with third-party forensics specialists to reconstruct and analyze the impacted data to understand the contents of the data and to whom that data relates. On December 4, 2023, we discovered that your information was impacted as a result of the incident.

What Information Was Involved. While we have no evidence that any of your information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following information may have impacted: your name, address, phone number, Member ID, DOB/Age, Medicaid ID, plan type. This incident did not involve disclosure of your Social Security number, driver's license number, or any financial account information.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate, respond, and notify potentially affected customers and individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event.

As an added precaution, we are providing you with access to 24-months of free credit monitoring and identity protection services provided by Experian. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements, medical claims, and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information* where you will find more information on the credit monitoring and identity restoration services we are making available to you.

We suggest that you retain this notice in case of any future problems with your accounts.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141 (TTY 1-800-648-6056), which is available Monday through Friday, between the hours of 6am and 8pm Pacific Time, and Saturday and Sunday 8am to 5pm Pacific Time, excluding major U.S. holidays.

We apologize for any inconvenience to you and remain dedicated to protecting the information in our care.

Sincerely,

Ian O'Neill
Global Head of Legal
Welltok, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for ## 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 ## 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 ##-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** February 29, 2024 (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 1-800-628-2141 by February 29, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-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 ExtendCARE™:** 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.

Reference Guide

1. Review Your Account Statements

As a precaution to protect against misuse of your health information, we recommend that you remain vigilant and regularly monitor the explanation of benefits statements that you receive from [us/your plan], and your bank and credit card statements, credit reports, to check for any unfamiliar activity. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact your plan at the number on your member ID card. If you do not regularly receive explanation of benefits statements, you may request that your plan send you these statements following the provision of any health care services in your name or plan number by contacting your plan at the number on your member ID card. If you notice any suspicious activity on either your bank or credit card statement, please immediately contact your financial institution and/or credit card company, or relevant institution.

2. Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

Upon receiving your credit report, review them carefully. Look for any accounts you did not open. Look in the "inquires" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for inaccuracies in information (such as home address and Social Security number).

If you see anything that you do not understand, call the credit bureau at the telephone number of the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

3. Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and FTC.
If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides an interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.
Step 2: Place a fraud alert and get your credit reports.
Step 3: Report identity theft to the FTC.
Step 4: You may choose to file a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at https://www.identitytheft.gov/#/Steps, or you can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft at https://consumer.ftc.gov/features/identity-theft.

4. Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be a victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging your file with a fraud alert at all three bureaus.

Credit Agency[1]	Mailing Address	Phone Number	Website
Equifax	P.O. Box 105069 Atlanta, GA 30348-5069	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

5. Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file, at no cost to you, 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 security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) phone number, current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

You can request a security freeze for free by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-800-916-8800	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about security breach response and steps you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office
Director of Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319
Phone: 1-515-281-5926
Website: www.iowaattorneygeneral.gov

For Maryland Residents. You can contact the Maryland Attorney General at:
Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202
Phone: 1-410-576-6491
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For Residents of Massachusetts. You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico Residents. New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.
You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.
The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:
(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
(2) proper identification to verify your identity; and
(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.
A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.
A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.
If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York Residents. You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
Phone: 1-800-771-7755
Website: www.ag.ny.gov

For North Carolina Residents. You can obtain information about preventing and avoiding identity theft from the North Carolina Attorney General at:
North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000
Website: https://ncdoj.gov/
Identity Theft Link: https://ncdoj.gov/protecting-consumers/protecting-your-identity/

For Oregon Residents. State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Department of Justice at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
Phone: 1-877-877-9392
Website: www.doj.state.or.us

For Rhode Island Residents. You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
Phone: 1-401-274-4400
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#