



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

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

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

November 13, 2023

VIA E-MAIL

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

Re: Notice of Data Event

To Whom it May Concern:

We represent Welltok, Inc. (“Welltok”) located at 1515 Arapahoe Street, #700, Denver, Colorado, 80202. 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 notify your office of an event that may affect the security of certain personal information relating to approximately seven (7) Maryland residents. Welltok is reporting this incident on behalf of St. Bernards Healthcare, Inc., who owns the data at issue. By providing this notice, Welltok 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.

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 October 18, 2023, St. Bernards Healthcare, 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 St. Bernards Healthcare, Inc. 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, Social Security number, date of birth, health insurance information, medical record number or patient identification number, provider name, and treatment information/diagnosis.

Notice to Maryland Residents

On or about September 8, 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 November 13, 2023, Welltok provided 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 seven (7) Maryland 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 twenty-four (24) months 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.

Office of the Maryland Attorney General

October 13, 2023

Page 3

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,

A handwritten signature in black ink, appearing to read "Rebecca Jones", written over a light gray rectangular background.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/kzm

EXHIBIT A



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

November 13, 2023



K3274-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ST. BERNARD NOTICE

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Notice of Data [Event/ Breach]

Dear Sample A. Sample:

Welltok, Inc. writes on behalf of St. Bernards Healthcare (“St. Bernards”) to inform you of an event that may affect the security of your personal information. Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for St. Bernards and received your information in connection with these services. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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. We also conducted an examination of our 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. We confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We 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 September 14, 2023, St. Bernards learned the scope of the data present on the impacted server at the time of the event. Since then, we have been coordinating efforts with St. Bernards to review and verify the affected information and provide direct notice to impacted individuals.

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 types of your information may have been impacted: your name and [data elements].

0000001



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 and respond to the event and notify potentially affected 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 twenty-four (24) months of 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.

For More Information. If you have additional questions, or need assistance, please call 800-628-2141, which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and on Saturday and Sunday between the hours of 8:00 a.m. to 5:00 p.m. 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,

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 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 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 800-628-2141 by February 29, 2024. Be prepared to provide engagement number B108165 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 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



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this event.





MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

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 5, 2023

VIA E-MAIL

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

Re: 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 notification to your office of an event that may affect the security of certain personal information relating to approximately twenty-one thousand three hundred twenty-nine (21,329) Maryland residents. Welltok is reporting this incident on behalf of its clients which own the data at issue, a list of whom is attached as ***Exhibit B***. By providing this notice, Welltok 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.

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. 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, date of birth, address, phone number, email address, Social Security number, medical record number and/or patient identification number, provider name, treatment information and/or diagnosis information, prescription information, treatment cost information, health insurance information, and Medicare/Medicaid number.

Notice to Maryland 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 4, 2023, Welltok provided 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 twenty-one thousand three hundred twenty-nine (21,329) Maryland 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,

A handwritten signature in black ink, appearing to read "Rebecca Jones", with a stylized flourish at the end.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/kzm

EXHIBIT A



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

December 4, 2023



K4126-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ADVENTIST ADULT

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Notice of Data [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc. writes on behalf of Adventist HealthCare to inform you of an event that may affect the security of your personal information. Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Adventist HealthCare and received your information in connection with these services. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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. We also conducted an examination of our 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. We confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We 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 October 10, 2023, Adventist HealthCare learned the scope of the data present on the impacted server at the time of the event. Since then, we have been coordinating efforts with Adventist HealthCare to review and verify the affected information and provide direct notice to impacted individuals.

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 types of your information may have been impacted: your name and [data elements].



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 and respond to the event and notify potentially affected 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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141 which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

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 IdentityWorksSM 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 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this event.





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

December 4, 2023

K4130-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 [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc., writes on behalf of Elixir Pharmacy to inform you of an event that may affect the security of your personal information. Welltok operates an online contact-management platform to provide patients with important notices and communications for Elixir Pharmacy and received your information in connection with these services. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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 and conducted an examination of our 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 and confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We subsequently undertook a time-consuming 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 October 18, 2023, Elixir Pharmacy learned the scope of the data present on the impacted server at the time of the event. Since then, we have been coordinating efforts with Elixir Pharmacy to review and verify the affected information and provide direct notice to impacted individuals.

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 types of your information may have impacted: your name and [Extra1].



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 and respond to the event and notify potentially affected 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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141 which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

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 IdentityWorksSM 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 22 Rhode Island residents impacted by this event.





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

December 4, 2023



K4134-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ORTHONEBRASKA ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of Data [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc. writes on behalf of OrthoWest, LLC, dba OrthoNebraska Clinics and Nebraska Orthopaedic Hospital LLC, dba OrthoNebraska Hospital (“OrthoNebraska”) to inform you of an event that may affect the security of your personal information. Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for OrthoNebraska and received your information in connection with these services. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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. We also conducted an examination of our 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. We confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We 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 October 19, 2023, OrthoNebraska learned the scope of the data present on the impacted server at the time of the event. Since then, we have been coordinating efforts with OrthoNebraska to review and verify the affected information and provide direct notice to impacted individuals.

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 types of your information may have been impacted: your name and [data elements].



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 and respond to the event and notify potentially affected 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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141 which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

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 IdentityWorksSM 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you

ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this event.





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

December 1, 2023

K4123-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

PARENT OR GUARDIAN OF
SAMPLE A SAMPLE - L02 MINOR



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



Notice of Data [Event/Breach]

Dear Parent or Guardian of Sample A. Sample:

Welltok, Inc. writes to inform you of a data privacy incident that may have impacted some of your minor dependent's information. Although we have no indication of actual fraud or misuse of your minor dependent's information as a result of the incident, we are providing you with information about the incident, our response to it, and resources available to you to help protect your minor dependent's information, should you feel it appropriate to do so.

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

We continued to investigate this issue using the assistance of third-party cybersecurity specialists and additional information that had been discovered in the intervening period to determine the potential for hidden vulnerabilities on the MOVEit Transfer server and assess the security of data housed on the server. After a full reconstruction of our systems and historical data, our 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. We subsequently undertook a time-consuming 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. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

What Information Was Involved. The information contained in the affected files includes your minor dependent's name and [Extra1]. To date, we are unaware of any actual misuse of this information as a result of the event.



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 and respond to the event and notify potentially affected 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.

While we have no indication of your minor dependent's information being misused in connection with this incident, as an extra precaution, we are offering you access to ## months of complimentary identity protection services through Experian.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor dependent's account statements. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Minor Dependent's Information*. There you will also find more information on the identity protection services we are making available to your minor dependent. While Welltok will cover the cost of these services, you will need to complete the activation process on your minor dependent's behalf. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, or need assistance, please call [Call Center Number], which is available Monday through Friday, 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

Welltok, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR DEPENDENT'S INFORMATION

Enroll in Credit and Identity Monitoring

To help protect your minor dependent's identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

If you believe there was fraudulent use of your minor dependent's 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 minor dependent's 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/minorplus>
- Provide your **activation code: ABCDEFGHI**
- Provide your minor's information when prompted

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:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.

^{**} 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.

ENGAGE#

0000002



K4123-L02

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to review account statements and credit reports for suspicious charges. While minors under the age of eighteen (18) typically do not have credit files, the following information relates to protecting one's credit once established. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) 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 (3) major credit bureaus listed below directly to request a free copy of your credit report.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this event.



EXHIBIT B

Adventist HealthCare

Address: 820 West Diamond Avenue, Suite 600, Gaithersburg, MD 20878

Date of notification from Welltok: September 22, 2023

Date of discovery: October 10, 2023

Data elements impacted: Date of birth, treatment information and/or diagnosis information, prescription information, provider name, medical record number and/or patient identification number, Medicare/Medicaid number, health insurance information, and treatment cost information.

Number of Maryland residents impacted: 20,840

Elixir Rx Solutions

Address: 2181 E Aurora Road, Twinsburg, OH 44087

Date of notification from Welltok: September 22, 2023

Date of discovery: October 18, 2023

Data elements impacted: Date of birth, medical record number and/or patient identification number, prescription information, and health insurance information.

Number of Maryland residents impacted: 248

OrthoNebraska

Address: 2808 South 143rd Plaza Omaha, NE 68144

Date of notification from Welltok: September 22, 2023

Date of discovery: October 19, 2023

Data elements impacted: Address, phone number, email address, date of birth, treatment and/or diagnosis information, provider name, medical record number and/or patient identification number, health insurance information, and treatment cost information.

Number of Maryland residents impacted: 20

OSF HealthCare System

Address: 124 SW Adams Street

Peoria, Illinois 61602

Date of notification from Welltok: September 22, 2023

Date of discovery: October 13, 2023

Data elements impacted: Date of Birth, Social Security number, treatment information and/or diagnosis, provider name, medical record number and/or patient identification number, health insurance information, and treatment cost information.

Number of Maryland residents impacted: 221



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

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 15, 2023

VIA E-MAIL

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

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 its clients who own the data at issue, a list of whom is attached as ***Exhibit B***. By providing this notice, Welltok 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.

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. 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, date of birth, Social Security number, email address, telephone number, treatment/ diagnosis information, prescription information, treatment cost information, dates of service, provider name, medical record number, and health insurance information.

Supplemental Notice to Maryland 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 13, 2023, Welltok provided written notice of this event to potentially impacted individuals on behalf of its clients listed in ***Exhibit B***, which own the data at issue. This mailing includes notice to approximately thirty thousand nine hundred (30,900) Maryland 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

The Office of The Attorney General

December 15, 2023

Page 3

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,

A handwritten signature in black ink, appearing to read "Rebecca Jones", written on a light gray rectangular background.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/kzm

EXHIBIT A



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

December 11, 2023

K4718-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 [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc. is a vendor of one of your health care providers and writes to inform you of an event that may affect the security of your personal information. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we learned that one of our servers, called the MOVEit Transfer server, had been potentially accessed by unknown third parties. The developer of the MOVEit Transfer tool had previously published that there was a vulnerability in the security of this server. In response, we had installed all published patches and security upgrades immediately upon them becoming available. We also examined our systems and networks to determine the potential impact of the published vulnerabilities and confirmed that there was no indication of anyone accessing the information on the MOVEit Transfer server at that time.

Upon learning of the additional concern in July, we moved quickly to launch an additional investigation with the assistance of cybersecurity specialists. We determined on August 11, 2023 that an unknown actor accessed the MOVEit Transfer server on May 30, 2023, and removed certain data from the MOVEit Transfer server during that time. We then undertook a time-consuming and detailed review of the data stored on the server at the time of this incident to understand the contents of that data and to whom it relates. Through that process, we learned that data related to you was present on the MOVEit Transfer server at the time of the event.

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 types of your information may have impacted: [Extra1]

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 and respond to the event and notify potentially affected 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 ## months of 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 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141, which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

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 IdentityWorksSM 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 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity

theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this event.





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

December 11, 2023

K4273-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 [Event/Breach]

Dear Sample A. Sample:

We are writing to inform you of our recent incident at Welltok, Inc. that may affect the security of your personal information. Welltok, Inc. is a wholly owned subsidiary of Virgin Pulse, Inc. and operates a member notification and contact platform. We entered into a contract with West Virginia University Health System (WVUHS) for Camden Clark Medical Center to participate in a pilot program to compile patient and community data and received your information file in connection with these services as part of the agreement. At Welltok, we take the confidentiality of our customers' information very seriously. Although there is no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so. Please understand this is not a breach of any WVUHS application, system, or platform.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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 and conducted an examination of our 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 and confirmed that there was no indication of any compromise at that time. On September 8, 2023, we notified WVUHS of the event.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We subsequently undertook a time-consuming 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. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event and on August 26, 2023, we notified WVUHS that patient data was impacted at the following hospitals: Summersville Regional Medical Center; Reynolds Memorial Hospital; Berkeley Medical Center; Jefferson Medical Center; Potomac Valley Hospital of W.Va., Inc.; United Summit Center; United Hospital Center, Inc.; Wheeling Hospital, Inc.; Barnesville Hospital Association; Harrison Community Hospital, Inc.; St. Joseph's Hospital of Buckhannon, Inc.; Camden-Clark Memorial Hospital Corporation; Braxton County Memorial Hospital, Inc.; Jackson General Hospital; Wetzel County Hospital; Uniontown Hospital; and West Virginia University Hospital, Inc.

0000001



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 types of your information may have been impacted: your name and [Extra1].

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 and respond to the event and notify potentially affected 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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141 , which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. 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,

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 IdentityWorksSM 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 10 Rhode Island resident impacted by this event.





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

December 14, 2023

K4823-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 [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc., operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications used by health plans, pharmacies and employers that encourages healthy lifestyle changes. We are writing to inform you of an event that may affect the security of your personal information. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We 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 and conducted an examination of our 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 and confirmed that there was no indication of any compromise at that time.

Upon being alerted to the alleged issue, we 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 our systems and historical data, our 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. We subsequently undertook a time-consuming 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. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

What Information Was Involved. While Welltok has no evidence that any information has been misused, the following types of information may have impacted: name, date of birth, telephone number, treatment/ diagnosis information, prescription information, provider name, medical record number, and health insurance 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 and respond to the event and notify potentially affected 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.



What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements 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*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. If you have additional questions, or need assistance, please call 1-800-628-2141, which is available Monday through Friday, between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, and Saturday and Sunday, between the hours of 8:00 a.m. and 5:00 p.m. Pacific Time, excluding major U.S. holidays. If you have a speech or hearing impairment and use a TTY, call **800-648-6056**.

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

Sincerely,

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 IdentityWorksSM 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 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file

such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Welltok, Inc.'s address is 1515 Arapahoe St. #700 Denver, CO 80202.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 1345 Rhode Island resident impacted by this event.



EXHIBIT B

White Plains Hospital Medical Center
41 E Post Rd, White Plains, NY 10601
Date of Notification from Welltok: September 22, 2023
Date of discovery: October 11, 2023
Data elements impacted: name, demographic information, dates of service, social security number and diagnosis.
Number of Maryland residents impacted: 3

West Virginia University Medicine
1 Medical Center Drive Morgantown, WV 26506.
Date of Notification from Welltok: September 22, 2023
Date of discovery: October 16, 2023
Data elements impacted: name, MRN/ patient ID, Social Security number, date of birth, health insurance information, provider name, treatment cost information, and treatment information/diagnosis
Number of Maryland residents impacted: 15,394

Centerwell Pharmacy
500 W Main St, Louisville, KY 40202
Date of Notification from Welltok: September 22, 2023
Date of discovery: October 31, 2023
Data elements impacted: name, date of birth, telephone number, treatment/ diagnosis information, prescription information, provider name, medical record number, and health insurance information.
Number of Maryland residents impacted: 4,148

Humana Inc.
500 W Main St, Louisville, KY 40202
Date of Notification from Welltok: September 22, 2023
Date of discovery: October 31, 2023
Data elements impacted: name, date of birth, telephone number, treatment/ diagnosis information, prescription information, provider name, medical record number, health insurance information.
Number of Maryland residents impacted: 11,355