



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

December 14, 2023

K5088-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 Blue Cross Blue Shield of Massachusetts 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 Blue Cross Blue Shield of Massachusetts 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 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. On October 4, 2023, Blue Cross Blue Shield of Massachusetts 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 Blue Cross Blue Shield of Massachusetts 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, date of birth, 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

0000001



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 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 IdentityWorks<sup>SM</sup> 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](http://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<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** 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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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](http://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](http://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](http://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](http://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 14 Rhode Island residents impacted by this event.





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

January 5, 2024

K5577-L01-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ADULT

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



### Notice of Data [Event/Breach]

Dear Sample A. Sample:

Welltok, Inc. writes to inform you of an event that may affect the security of your personal information. Welltok coordinates the administration of the wellness reward program for your health plan 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 27, 2023, we provided limited information to your health plan regarding the scope of the data present on the impacted server at the time of the event. Since then, we have been coordinating efforts 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 [Extra 1].

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.

**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 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 IdentityWorks<sup>SM</sup> 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](http://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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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](http://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](http://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](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents impacted by this event.





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

January 5, 2024



K6153-L01-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345  
SAMPLE A SAMPLE - L01 KAISER - 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 your health plan 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 your health plan 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, your health plan-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 our healthcare client 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 [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 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 IdentityWorks<sup>SM</sup> 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](http://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:
- 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<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** 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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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](http://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](http://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](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents impacted by this event.

