

November 10, 2023

By E-Mail to IDTheft@oag.state.md.us

**Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202**

Re: Notice of a Data Security Incident

To the Office of the Attorney General:

I write on behalf of my client, Spectrum Brands Inc. (“the Company”), to inform you that the Company’s vendor, Welltok Inc. (“Welltok”), experienced a data security incident that affected the personal information of some of the Company’s current and former employees. Welltok provides a wellness-related mobile application and service, and Welltok handles personal information to provide those services.

I. Nature of the Security Incident

Welltok and reportedly hundreds of companies and state agencies use a third-party file transfer and storage software tool called MOVEit to transfer and store data to conduct their business. On May 31, 2023, the provider of MOVEit, Progress Software Corp., publicly disclosed a security vulnerability of the software. Welltok is a user of this software. Welltok stated that it quickly addressed the vulnerability by applying available patching and undertaking other recommended mitigation steps. Further, Welltok stated it promptly launched an internal investigation with the assistance of third-party cybersecurity specialists to determine the potential impact of the vulnerabilities on the security of data they transmitted and stored with the software.

According to Welltok, on August 31, 2023, Welltok’s investigation determined that an unknown actor exploited the MOVEit vulnerability between May 30, 2023 and May 31, 2023, and accessed and exfiltrated certain data transmitted and maintained by the software during that time. Welltok stated that it subsequently undertook a time-consuming and detailed review of the data stored by the software tool during that time period to identify the contents of the affected data and to whom that data relates. On October 18, 2023, Welltok notified the Company that Welltok had confirmed that personal information maintained on behalf of the Company was affected by the MOVEit incident.

II. Number of Residents Affected and Notified

The affected data contained the personal information of eight Maryland residents. The personal information included full name, address, telephone number, and email address for all affected individuals.

For most of the affected individuals, the personal information also included social security numbers, date of birth, and insurance plan name and coverage level.

Notices to Maryland residents were sent via first class mail on November 13, 2023.

III. Steps Welltok and the Company have Taken to Address the Incident

Welltok stated that upon learning of the MOVEit vulnerability Welltok moved quickly to implement protective measures to protect against further unauthorized access (including installing software patches, implementing other mitigation steps recommended by the software provider, and updating internal technical measures and security procedures to further strengthen their information security program) and to investigate the impact and scope of the incident. Welltok also notified law enforcement and the consumer reporting agencies of the security breach. Upon confirmation that personal information associated with the Company's current and former employees was affected, Welltok and the Company have worked together to promptly notify affected individuals and ensure that each affected individual has access to 24 months of credit monitoring services from Experian at no cost to the individual. The notification also encourages affected individuals to continue to be vigilant about monitoring their credit report information and financial accounts to protect against fraudulent activity. Enclosed is a copy of the notification letter to individuals.

After the Company discovered the MOVEit vulnerability, the Company evaluated its own use of the MOVEit software tool and confirmed that employees are not given permission to use the software. After receiving notice from Welltok that the Company's current and former employee personal information was affected, the Company followed its incident response policies and procedures. The Company took steps for Welltok to confirm it had implemented appropriate security safeguards to mitigate the MOVEit vulnerability to prevent further exploitation and to confirm that an incident involving Welltok would not also affect the Company's environment. The Company is also evaluating whether to continue providing the Welltok services to its employees or to replace Welltok with a different vendor.

Please contact me if you have any questions.

Sincerely,



Wendell Bartnick
Reed Smith LLP

Cc: Sheek Shah, Reed Smith LLP

Enclosure



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

November 13, 2023

K3138-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 NON-MA
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of Data Incident

Dear Sample A. Sample:

Welltok, Inc. (“we” and “our”), the provider of CaféWell, writes on behalf of Spectrum Brands, Inc. to inform you of a security incident that involves your personal information. Welltok received your personal information to operate CaféWell, an employee wellness benefit which can be used to assist with healthy lifestyle changes. Welltok used file transfer and storage software called MOVEit that had a security incident that impacted hundreds of companies and state agencies.

Based on our investigation, we have no indication of actual fraud or misuse of your information, but your personal information was involved in the security incident. This letter provides 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. You can learn more about the incident by calling the dedicated assistance line provided below or visiting the CaféWell or Welltok website.

What Happened. On May 31, 2023, the provider of MOVEit publicly disclosed the security vulnerability of the software. As a user of that software, we moved quickly to apply available patching and undertook recommended mitigation steps. We promptly launched an internal investigation with the assistance of third-party cybersecurity specialists to determine the potential impact of the vulnerabilities on the security of data we transmitted and stored with the software. On August 11, 2023, our investigation determined that an unknown actor exploited the software vulnerabilities between May 30 and May 31, 2023 and accessed and acquired certain data we transmitted and stored with the software during that time. We conducted a time-consuming and detailed review of the data transmitted and stored by the software on those days to understand the data and individuals impacted. On October 18, 2023, we learned that data related to you was affected by the security incident.

What Information Was Involved? While we have no evidence that any of your personal information has been misused, we are notifying you and providing information and resources to help protect your personal information. The following types of information about you was impacted by the security incident: your name, address, telephone number, email address, [Extra1]. Health information was not involved in this security incident. This letter lists the impacted types of personal information specific to you, and it may be different from information you read on our website or in the media about this security incident.

What We Are Doing. We take this event and the security of personal information very seriously. Upon learning of this event, we moved quickly to institute protective measures to protect against further unauthorized access (including installing software patches and implementing other mitigation steps recommended by the software provider), investigate and respond to the security incident, and notify affected individuals. We also notified law enforcement of the security incident. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event.



As an added precaution, we are providing you with access to 24 months of 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 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.
1515 Arapahoe St#700
Denver, CO 80202
844-936-1689

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 1-800-628-2141 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 or learn more about fraud alerts, 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, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed by law enforcement.

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/>.

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 4 Rhode Island residents impacted by this event.



