

Snell & Wilmer

TABOR CENTER
1200 SEVENTEENTH STREET
SUITE 1900
DENVER, CO 80202
303.634.2000 P
303.634.2020 F

Aloke S. Chakravarty
(303) 634-2121
achakravarty@swlaw.com

April 25, 2025

VIA EMAIL AND CERTIFIED MAIL RETURN RECEIPT REQUESTED

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

Re: Notice of Cryoport, Inc. Data Security Incident

To Whom it May Concern:

On behalf of our client, Cryoport, Inc. ("Cryoport"), and in compliance with Md. Code Ann., Com. Law § 14-3504(h), Cryoport is notifying the Maryland Attorney General regarding a data security incident that may have exposed the personal information of four (4) Maryland residents.

Specifically, on or about March 18, 2022, Cryoport received information from one of its vendors that the vendor had received an email from a third party (the "suspicious email") purporting to forward a data file (the "suspicious file") containing Cryoport employees' personal information that had previously been sent via attachment (the "original file") to an email address (the "original email") from Cryoport to the vendor (against company policy). The original file contained personal data of four (4) employees located in Maryland.

As soon as Cryoport learned of the incident, Cryoport retained a third-party firm to immediately begin an investigation to assess the security of its systems. Cryoport has implemented additional security measures to prevent the recurrence of such unauthorized access.

While Cryoport's investigation did not find any evidence that its email or other systems were compromised, Cryoport is evaluating various additional measures that would reduce the risk its systems would be compromised in the future. Cryoport anticipates determining which measures to implement in the next 4-6 weeks. As a precautionary measure, Cryoport has implemented

April 25, 2022

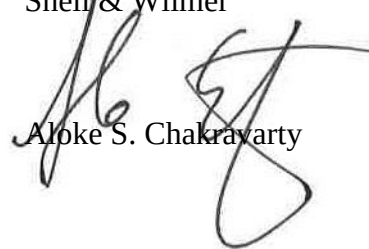
Page 2

Multifactor Authentication and password resets for the email accounts that were party to the original email. As a precautionary measure, Cryoport has arranged for Experian to offer twelve (12) months of credit monitoring free of charge to the notified individuals.

If you have any questions regarding this notification, please contact me at (302) 634-2121 or at achakravarty@swlaw.com.

Best Regards,

Snell & Wilmer

A handwritten signature in black ink, appearing to read 'Aloke S. Chakravarty', is written over the printed name. The signature is stylized with a large, sweeping 'A' and a long, horizontal stroke extending to the right.

Aloke S. Chakravarty

ASC:cl

Enclosure

<<FirstName>> <<LastName>>
<<Address1>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

You have received this letter to inform you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident and the actions we have taken.

While we have no reason to believe that your personal information has been misused, we are notifying you so that you have the information and tools necessary to help detect and prevent any potential misuse of your personal information.

What Happened?

Cryoport, Inc. ("Cryoport") recently learned of a potential data security incident, which may have resulted in the exposure of a data file containing your personal information. Upon learning about the potential incident, Cryoport immediately began an investigation to assess the security of its systems. On April 15, 2022, we determined that certain files were accessed on or about March 18, 2022, without authorization.

Cryoport began a review of the data file to determine whether sensitive information was present. On or about April 15, 2022, Cryoport confirmed that some of your information was present in the relevant files.

This notification is the result of a thorough and comprehensive investigation by Cryoport, Inc. and a third-party firm and has not been delayed as a result of a law enforcement investigation.

What Information Was Involved?

The personal information affected by the incident may have included your first and last name and social security number.

What We Are Doing.

Cryoport regrets that this incident occurred. As soon as we learned of the incident, we immediately retained a third-party firm to conduct a forensic investigation concerning this incident. Furthermore, we have implemented additional security measures designed to prevent the recurrence of such an incident and to protect the privacy of our employees.

To help protect your identity, we are offering a complimentary 12-month membership of Experian's IdentityWorksSM. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by July 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code**: <<ActivationCode>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by July 31, 2022. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-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, Equifax and Transunion files for indicators of fraud.
- **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 ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [REDACTED]. 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 (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 this Identity Restoration support is available to you for 12 months from the date of this letter, free of charge, and does not require any action on your part at this time. The Terms and Conditions for the services provided by Experian are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also recommend that you remain vigilant by reviewing account statements and monitoring your free credit reports.

For More Information.

Protecting your information is important to us. We regret any inconvenience this may cause you. If you have any questions, please email [REDACTED], VP – Global Human Resources & Organizational Development directly at [REDACTED].

Sincerely,



Tony Ippolito, VP and General Counsel

ADDITIONAL RESOURCES

Contact information for the Nationwide Credit Reporting Agencies:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2104	PO Box 2000
Atlanta GA, 30374	Allen, TX 75013	Chester, PA 119016
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Free Credit Report: You may obtain a free copy of your credit report, once every 12 months from each of the three nationwide credit reporting agencies. You may request a report online at www.annualcreditreport.com or by calling toll free **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to **Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281**.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report free of charge if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze: You can place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices: If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. The FTC and your State Attorney General's Office can provide you with more information about preventing identity theft, fraud alerts, and security freezes. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, www.ct.gov/ag, 1-860-808-5318.

For District of Columbia Residents: You may contact the Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington DC, 2001, www.oag.dc.gov, (202) 442-9829.

For Iowa Residents: You are advised to report suspected indents of identity theft to local law enforcement or the Iowa Attorney General. You may contact the Office of the Iowa Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, 1-888-777-4590.

For Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For New York Residents: For more information on identity theft, you can contact the following state agencies: The Office of the New York Office of the Attorney General, The Capitol, Albany NY 12224-0341, www.ag.ny.gov, 1-800-771-7755 or The New York Department of State Division of Consumer Protection, Assistance Unit 99 Washington Avenue Albany, New York 12231-www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566- 7226.

For Rhode Island Residents: You may contact the Rhode Island Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report if you are a victim of identity theft. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Rhode Island Attorney General.

Rights under the Fair Credit Reporting Act, 15 U.S.C. 1681a.

For New Mexico Residents: You have rights under the Fair Credit Reporting Act, such as the right to be told information in your credit files 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. The consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information, consumer reporting agencies may not report outdated negative information. You may have additional rights under the Fair Credit Reporting Act not summarized here. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting <https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores>.