

Morgan Lewis

Ezra D. Church

Partner
215.963.5710
ezra.church@morganlewis.com

September 13, 2024

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Aramark, and we are writing to notify your office on behalf of Aramark about a recent data security incident impacting some current or former employees of Aramark.

On or about August 22, 2024, Aramark learned that a bad actor had created a website designed to look like the Aramark myPay portal with the intent of confusing and tricking current or former Aramark employees to log in with their username and password. In a relatively small number of cases, the bad actor may have used that information to access the official Aramark myPay site and change direct deposit information, with the goal of sending the Aramark employee's pay to another bank account. It appears that this is part of a larger scheme to target companies who use myPay or similar services. Upon learning about the issue, we immediately took steps to support any employees who were victims of this scheme.

Through its investigation, Aramark has determined that, where the bad actor used the stolen credentials to access the official Aramark myPay site, the bad actor may have also had access to personal information including first name, last name, address, and Social Security Number. Although there is no indication that the personal information has been used for any fraudulent purpose beyond the changing of direct deposit information, notifications are being sent by mail to the affected individuals to explain what happened, what information was involved, what has been done, and how affected individuals can get further information and protect themselves. Two years of credit monitoring are being offered to affected individuals.

Since learning of this incident, Aramark has been working with industry partners to help prevent future fraud involving fake myPay sites, and it will continue with these efforts.

A copy of the notification sent to the affected individuals is attached, which is being sent to 5 Maryland residents via electronic mail on September 10, 2024.

Morgan, Lewis & Bockius LLP

2222 Market Street
Philadelphia, PA 19103-3007
United States

 +1.215.963.5000
 +1.215.963.5001

State of Maryland
Office of the Attorney General
September 13, 2024
Page 2

If you have any questions, please feel free to contact me.

Best regards,

A handwritten signature in black ink, appearing to read "E.D. Church", with a stylized, cursive script.

Ezra D. Church

Enclosure

Sample Individual Notification Letter



September 10, 2024



Re: Notice of Data Security Incident

Dear [REDACTED],

We have received recent reports about a security incident, where bad actors created a fraudulent myPay website to mislead Aramark employees into divulging their Aramark myPay account credentials. We are writing to provide additional information about the incident, including potential access to your personal information.

What Happened?

Over the past several weeks, we learned that a bad actor had created a website designed to look like our Aramark myPay portal with the intent of confusing and tricking current or former Aramark employees to log in with their single sign-on username and password. In some cases, the bad actor may have used that information to access the official Aramark myPay site and change direct deposit information, with the goal of sending your pay to another bank account. Unfortunately, this is part of a larger scheme to target companies who use myPay or similar services, and we are actively working with industry partners to help prevent this type of fraud. Upon learning about the issue, we immediately took steps to support any employees who were victims of this scheme.

What Information Was Involved?

In addition to changing direct deposit details, the bad actor may have accessed other personal information such as your name, address, and social security number. Although there is no evidence that the information has been used in an unauthorized way beyond the changing of direct deposit details, we did want to make you aware of this risk out of an abundance of caution and let you know about some steps that you can take to protect yourself, outlined below.

What We Are Doing

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 12-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 12/31/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: [REDACTED]

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 1-877-890-9332. Be prepared to provide engagement number B130555 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.

What You Can Do

All Aramark employees are encouraged to exercise particular care in the use of myPay including the following specific recommendations:

- **Stay vigilant over phishing emails.** Cyber criminals will often try to impersonate other Aramark employees, partners, or customers. Never click on unfamiliar links or provide sensitive information over email without verifying its legitimacy.
- **Be careful to only use <https://www.aramark.com/mypayinfo> for access to your payroll information.** Look out for any variations in that address, which may indicate a fraudulent site. We also recommend that you enter the site address directly into your internet browser—do not click on links in emails, documents or on other websites that purport to link to Aramark myPay.
- **Please report any suspicious activity to Aramark IT!**

In addition, if you choose not to use Experian IdentityWorksSM or would like to take additional steps, we strongly urge you to do the following:



If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
7289)

P.O. Box 4500
Allen, TX 75013

www.experian.com

Equifax (1-800-525-6285)

P.O. Box 740241
Atlanta, GA 30374

www.equifax.com

TransUnion (1-800-680-

P.O. Box 2000
Chester, PA 19016

www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Aramark.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For More Information

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you. If you have questions about this notice, please feel free to contact us at or sending an email to: AramarkSupport@morganlewis.com.

Sincerely,

Aramark Privacy Team



REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit

<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

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

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com



TransUnion Fraud Victim Assistance Division www.transunion.com
P.O. Box 2000
Chester, Pennsylvania 19016

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov



For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office

Bureau of Internet and Technology

(212) 416-8433

<https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of

Consumer Protection

(800) 697-1220

<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.