ReedSmith
Driving progress
through partnership
Gerard M. Stegmaier
Direct Phone: +1 202 414 9228
Email: gstegmaier@reedsmith.com

Reed Smith LLP
1301 K Street, N.W.
Suite 1000 - East Tower
Washington, D.C. 20005-3373
+1 202 414 9200
Fax +1 202 414 9299
reedsmith.com

May 17, 2023

VIA Electronic Mail: consumer@ag.iowa.gov

Office of the Attorney General of Iowa
Consumer Protection Division
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of a Data Security Incident

To The Office of the Attorney General:

I write on behalf of the firm's client, Sysco Corporation (the "Company"). The Company was recently the target of a cybersecurity event in which personal information requiring legal notification was likely involved. It has no reason to conclude that any individual is at any increased risk for identity theft or any other risk as a result of this incident at this time.

I. Nature of the Security Incident

On March 5, 2023, the Company became aware of a cybersecurity event initiated by an external threat actor believed to have begun on January 14, 2023, in which the threat actor gained access to its systems without authorization and claimed to have acquired certain data. Immediately upon detection, the Company launched an investigation, with the assistance of cybersecurity and forensics professionals and contacted federal law enforcement. After a preliminary review of the data believed to have been extracted by the threat actor, which was completed on March 31, 2023, the Company determined that personal information for some of its current and former employees, as well as more limited customer and supplier personal information, was likely involved and has since undertaken further analysis which is ongoing. Accordingly, out of an abundance of caution, the Company determined to provide notice to potentially affected employees as soon as practicable and continues to investigate or otherwise evaluate personal information impacts and possible notification obligations. The Company is actively communicating with its customers and suppliers as appropriate.

II. Number of Residents Notified

The number of notified Iowa residents whose personal information could be affected is eight hundred seventy-four (874). While the investigation cannot confirm at this time specifically what categories of information may have been impacted for each individual employee, the Company believes it could include some combination of the following data: personal information provided to the Company for payroll purposes, including name, social security number, account numbers or similar information. Notices to Iowa residents were sent via electronic mail starting on May 5, 2023 and postal mail starting on May 8, 2023.

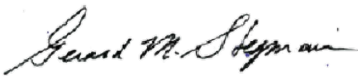
III. Steps Taken to Address the Incident

ReedSmith

The Company is in the process of reviewing its security program and determining whether to implement changes or additional controls and safeguards now or in the future to prevent similar incidents from occurring. The Company also notified federal law enforcement of the incident. In addition, it arranged to have Experian help protect affected individuals from identity theft by offering, free of charge, 24 months of credit monitoring, fraud consultation, and identity theft restoration services. It also provided an explanation of additional steps that affected individuals may consider taking to further protect themselves and their information, including checking credit reports, utilizing fraud alert services, and placing a security freeze on credit reports. Enclosed is a copy of the notification letter to individuals.

Please contact me if you have any questions.

Sincerely,



Gerard M. Stegmaier
Reed Smith LLP

Enclosure

Cc: Eric Manski, Reed Smith LLP

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

May 12, 2023

J4283-L04-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 COLLEAGUE US MAIL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Breach and Steps You Can Take to Protect Your Information

To our Valued Colleague/Former Colleague,

Sysco was recently the target of a cybersecurity event in which personal information for some of our current and former colleagues may have been impacted. First and foremost, I apologize that this happened and regret any concern this may cause. We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously.

Please read below for additional information about what happened, the steps we are taking, as well as steps you can take to protect your information.

Sysco has provided for you, free of charge, two years' worth of identity theft protection and credit monitoring. In order to enroll in your complimentary membership, **we need for you to contact Experian by visiting https://www.experianidworks.com/credit, and providing the following activation code: Y3SV7Q29C.**

What Happened? On March 5, 2023, Sysco became aware of a cybersecurity event perpetrated by a threat actor believed to have begun on January 14, 2023, in which the threat actor gained access to our systems without authorization and claimed to have acquired certain data. While we have not yet fully validated these claims, we have determined that personal information for some of our current and former colleagues has been impacted.

What Information Was Involved? While we cannot confirm at this time specifically what information may have been impacted for each individual colleague, we believe it could include some combination of the following data: personal information provided to Sysco for payroll purposes, including name, social security number, account numbers or similar information.

What We Are Doing: Upon discovery of the event, Sysco immediately opened an investigation in partnership with a leading cybersecurity firm and other experts. We also notified federal law enforcement.

Sysco's operational systems and related business functions suffered no impact as a result of the event, and Sysco's service to customers continued uninterrupted. Additionally, there is no ongoing threat to our network or systems. We've implemented additional controls and safeguards to help prevent a similar event from occurring in the future.

In addition, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft.

What You Can Do: Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further details on how to activate your complimentary 24-month membership of Experian's® IdentityWorks℠, as well as additional steps you can take to protect your information.

For More Information. We sincerely regret the concern this may cause, and deeply appreciate your support as we work to resolve it. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (800) 984-8152 and for Spanish at (800) 984-8308 between the hours of 6 a.m. to 8 p.m. PT and Saturday through Sunday from 8 a.m. to 5 p.m. PT (excluding major US holidays). Please be prepared to reference engagement number B090569 when speaking with an agent.

Thank you,

Jim Peck

B090569

0000002

J4283_L04

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior 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**: **August 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **Y3SV7Q29C**

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 (800) 984-8152 by **August 31, 2023.** Be prepared to provide engagement number **B090569** 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 agents 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 information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. 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 event 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 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. You will also find self-help tips and information about identity protection at this site.

Credit Reports: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
1-888-378-4329	**1-888-397-3742**	**1-800-916-8800**
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen TX 75013	Chester, PA 19016

* 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.

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, or obtain more information regarding fraud alerts, contact any of the three credit reporting agencies identified above. You also may contact the Federal Trade Commission ("FTC") as identified below for more information on fraud alerts.

Security Freeze: You may want to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. Under Federal law, there is no charge to place, lift, or remove a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as identified above or the FTC as identified below. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Additional Steps and Resources. We advise that you remain vigilant for events of fraud or identity theft by reviewing your account statements and monitoring credit reports closely to detect any errors or unauthorized activity resulting from this event. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

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 FTC and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You may also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

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

Additional Information for Residents of:

District of Columbia: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.gov/.

Iowa: You may report suspected identity theft to local law enforcement and/or the Iowa Attorney General at Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5164; www.iowaattorneygeneral.gov.

Maryland: You may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General at: Maryland Office of the Attorney General**,** Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; https://www.marylandattorneygeneral.gov/.

New Mexico: You have rights pursuant to the Fair Credit Reporting Act ("FCRA")**.** Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.

- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

New York: You can obtain information from the New York State Office of the Attorney General or the New York Department of State Division of Consumer Protection about how to protect yourself from identity theft and tips on how to protect your privacy online. The Attorney General's office can be reached at: 1-800-771-7755; https://ag.ny.gov. The Division of Consumer Protection can be reached at: 1-800-697-1220; http://www.dos.ny.gov/consumerprotection.

North Carolina: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.gov.

Oregon: You may report suspected identity theft to law enforcement, the FTC and/or the Oregon Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392; www.doj.state.or.us.

Rhode Island: You may contact and obtain information from your Attorney General at: 1-401-274-4400; www.riag.ri.gov. If you are the victim of identity theft, you have the right to file a police report and obtain a copy of it.