Morgan Lewis

Gregory T. Parks
Partner
215.963.5170
gregory.parks@morganlewis.com

October 2, 2023

VIA EMAIL TO CONSUMER@AG.IOWA.GOV

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

Re: Notice of Potential Exposure of Personal Information

Dear Office of the Attorney General:

This Firm represents Day & Zimmermann, and we are writing to notify your office on their behalf regarding the nature and circumstances of a recent potential exposure of personal information. The information of 685 residents of your state may have been involved.

On Friday, September 8, 2023, at approximately 7:00 p.m. ET, a Day & Zimmermann vendor was updating Success Factors, the company's Human Resources information system. The vendor inadvertently modified the settings in a manner that allowed employees to access information about other employees rather than just themselves. An employee could only view another employee's information by intentionally searching for it. The company believes this was unlikely given the company's culture and expectations. Immediately upon learning of the issue on Sunday, September 10, the settings were corrected, and the proper restrictions to access were restored by approximately 10:00 a.m.

Upon investigation, Day & Zimmermann determined the following types of information could have been accessible during this window of time: home address, bank routing and account numbers, tax withholding information, and other information regarding the individuals' employment with the company. Day & Zimmermann's investigation confirmed that social security numbers and race and ethnicity information were not accessed during this time. The investigation revealed that only 116 employees logged in during the time, and there is no evidence that any of these employees accessed another employee's information. Day & Zimmermann was also able to confirm that no employee data was changed without authorization.

Notifications are being sent by company email to the employees whose information was improperly accessible to explain what happened, what information was involved, and what has been done. One year of credit monitoring is being offered to all employees.

Morgan, Lewis & Bockius LLP

1701 Market Street
Philadelphia, PA 19103-2921
United States

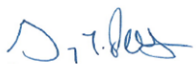
T +1.215.963.5000
F +1.215.963.5001

Day & Zimmermann carefully evaluates the cybersecurity posture of third-party software and will continue this effort. Day & Zimmermann is also taking steps to further ensure that employees' personal information would not be subject to such inadvertent access in the future.

Further information about what mitigations have been completed to date and what further mitigations are recommended to the affected individuals can be found in the enclosed notification that was sent to 685 Iowa residents via email on October 2, 2023.

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

Regards,



Gregory T. Parks

Enclosure

From:	Corporate Communications
Subject:	Notice of Potential Exposure of Information and Reference Guide - Please Read
Date:	Monday, October 2, 2023 2:56:44 PM
Attachments:	image001.png Reference Guide to Accompany Notices.pdf
Importance:	High

From Dan Ross, SVP and CHRO

NOTE: We are resending this email with the attached reference guide that was not included in the original email. There are no changes to the issue or our response – this is only to include the additional information contained in the attached reference guide for your use. Please also look for the activation code via email from TransUnion in the next few days. This will be sent from the email domain of @cyberscout.com and is safe to view and use.

Dear Colleagues:

We are writing to notify you of a **potential** exposure of information at Day & Zimmermann. If there was any exposure, it was both inadvertent and temporary. This letter is being sent to provide you with additional information and to advise you of services Day & Zimmermann is offering at no charge to you to help protect your continued privacy. **A reference guide on credit reporting and identity theft is also included for your information.**

It is important to note that we have no evidence that your personal information has been accessed or misused in any way, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done, and what you can do to address this situation.

What Happened?

On Friday, September 8, 2023, at approximately 7:00 p.m. ET, a Day & Zimmermann vendor was updating SuccessFactors, our Human Resources system of information, and inadvertently modified the settings to allow employees to access information about other employees rather than just themselves. An employee could only view another employee's information by intentionally searching for it. We do not know whether this happened. While we hope this is unlikely given our company's cultural values, we cannot rule out the possibility that another employee looked at your information. The settings were corrected and the proper restrictions to access were restored by approximately 10:00 a.m. ET on Sunday, September 10, 2023. The total time of the inadvertent exposure was less than two days. We know that only 116 employees logged in during this time, meaning the number of people who could have looked at your information is relatively small.

What Information Was Involved?

Our new human resources system, SuccessFactors, is the only system that was involved and the

following types of information about impacted employees may have been exposed during this window time: home address, bank routing and account numbers, tax withholding information, and other information within SuccessFactors, **except that** we do know that no other employee viewed your social security number or race and ethnicity information, and no employee data was changed without authorization.

What We Are Doing

Immediately upon learning of this potential exposure, we fixed the error and restored the proper restrictions in SuccessFactors. We then sought to determine what information may have been involved so that we could notify you. Rest assured; we also worked with the vendor to prevent something like this from occurring in the future. Now that we have completed the SuccessFactors implementation, going forward we will have the ability to determine if any employee data field was viewed, not just Social Security, Race, and ethnicity.

Finally, out of an abundance of caution, we have retained the assistance of TransUnion credit monitoring service to help protect your identity.

In response to the incident, Day & Zimmermann is providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services will provide you with alerts (for (1) one year from the date of enrollment) when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the credit bureau. For U.S. and Canadian employees only, this service also includes proactive fraud assistance to help with any questions that you might have or if you become a victim of fraud.

In the next several days, you will receive an activation code via email from TransUnion. ***This will be sent from the email domain of @cyberscout.com***. Please follow the instructions provided to enroll in credit monitoring services at no charge to you. You must enroll within 90 days from the date of the activation email. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

To help protect your personal information, we strongly recommend you take the following steps:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and personal information to establish credit and to block that credit from being established if you were not the one who initiated it.

- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Canada Revenue Agency (CRA). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this potential exposure, please contact Human Resources.

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Dan Ross,
SVP & CHRO

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 P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

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 you 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 200001, 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.