

December 7, 2022

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

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 211202

Re: Notice of Data Security Incident

Dear Sir/Madam:

I am writing on behalf of Conduent HR Services, LLC ("Conduent") to notify you of a data security affecting Maryland residents.

R.R. Donnelley & Sons Company (RRD), a print and mail vendor, identified a system intrusion in its technical environment on December 23, 2021, which was the result of a spear phishing attack. RRD promptly implemented its response, containment, mitigation, and investigation activities. On August 3, 2022, RRD notified Conduent they identified Conduent data was impacted and exfiltrated from this event.

Conduent recently completed the data review and determined the incident impacted five (5) Maryland residents. The data elements exposed included name, address, and social security number.

To prevent a similar event from occurring, the vendor removed and blocked the threat, changed all passwords, increased resources, enhanced technological safeguards, and increased monitoring capabilities. RRD will notify and provide credit monitoring services to the Maryland residents of the event on December 8, 2022. A template of the individual notice is attached to this letter.

If you have any questions, please contact me via mail or at Janet.Parnell@Conduent.com.

Respectfully submitted,

Janet Parnell

Janet Parnell
Privacy Director



HR Services, LLC
100 Campus Drive, Suite 200
Florham Park, NJ 07932

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<ZIP>>

Re: **NOTICE OF DATA BREACH**

<<Mail Date>>

Dear <<Full Name>>,

We are writing to notify you of a security incident that involved the unintended disclosure of your personal information. We deeply regret this situation and are keenly aware of how important the security and privacy of your personal information is to you.

WHAT HAPPENED?

On December 27, 2021, R.R. Donnelley & Sons (RRD), a third-party print and mail supplier, identified a systems intrusion in their technical environment. RRD promptly implemented a series of containment measures to address this situation including activating incident response protocols, shutting down servers and systems and commencing a forensic investigation. The investigation recently revealed that your personal information appears to have been included in the data that was exfiltrated from their corporate data system.

WHAT INFORMATION WAS INVOLVED?

The personal information included your name, address, and social security number.

WHAT WE ARE DOING.

Shortly after discovering the intrusion, RRD engaged forensic resources and third parties to assist in its evaluation of the intrusion and shut down all impacted servers. RRD believes to the best of its knowledge that the intrusion has been removed and effective controls have been implemented to prevent further incidents from the attacker.

WHAT YOU CAN DO.

At this time, we are not aware of any misuse of the information. As a precautionary measure, we encourage all individuals to remain vigilant for incidence of fraud and identity theft by reviewing account statements, monitoring free credit reports, and promptly reporting any suspicious activity. Additionally, we have arranged for you to enroll, at your option, in a <<Subscription Term>> membership of Experian's® IdentityWorksSM at no cost to you. 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: 02/15/23** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: <<Activation Code>>

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 877-890-9332 by 02/15/23. Be prepared to provide your engagement number <<Engagement Num>> as proof of eligibility for the identity restoration services by Experian.

For additional details on Experian's IdentityWorks membership, please see the enclosed instruction sheet "Additional details regarding your Experian IdentityWorks Membership."

Kindly note: Due to Experian's security measures, if you attempt to login to your account from a location outside the U.S., you may not be able to gain access to your account. If you are located outside of the U.S., please call Experian's international non-toll-free number 877-890-9332 to get account related information while located outside the U.S.

FOR MORE INFORMATION.

For additional information on other steps you can take, please see the enclosed sheet "ADDITIONAL STEPS TO PROTECT YOURSELF." If you have any questions, please feel free to call (833) 796-8636. We sincerely regret this incident occurred.

Sincerely,

Janet Parnell

Janet Parnell, Privacy Director
Conduent Business Services, LLC

ADDITIONAL DETAILS REGARDING YOUR 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 **877-890-9332**. 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 one year 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.

* 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.

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert

You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts.

Fraud Alerts: There are also two types of fraud alerts that can be placed on credit reports to put creditors on notice that a consumer may be a victim of fraud: an initial alert and an extended alert. Consumers may ask that an initial fraud alert be placed on their credit report if they suspect they have been, or are about to be, a victim of identity theft. An initial fraud alert stays on credit reports for at least one year. An extended alert may be placed on credit reports if consumers have already been a victim of identity theft, with the appropriate documentary proof, and stays on credit reports for seven years. Consumers may place a fraud alert on their credit reports by contacting the toll-free fraud number of any of the three national credit reporting agencies listed below.

Credit Freezes: Consumers have the right to place a credit freeze or security freeze (referred to as "credit freeze") on their consumer reports. A credit freeze is designed to prevent credit, loans and services from being approved in a consumer's name without the consumer's consent. Using a credit freeze, however, may delay ability to obtain credit. Consumers may request that a freeze be placed on credit reports by sending a request to a credit reporting agency online or by certified mail, overnight mail or regular stamped mail to the three national reporting agencies listed below. Unlike a fraud alert, a credit freeze must be separately placed on a consumer's credit file at each credit reporting company. More information can be obtained about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

How to Place an Alert: You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241

Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013

TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

Directions for Obtaining a Credit Report

Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Additional Resources

Additional information on identity theft is available from the Federal Trade Commission (FTC). Consumers may obtain information about preventing and avoiding identity theft from the Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), <https://www.consumer.ftc.gov/>. If you are a resident of North Carolina, you may also obtain information from the North Carolina Office of the Attorney General by contacting them at 919.716.6400 and at their website: <https://ncdoj.gov/contact-doj/>. If you are a resident of Maryland, you may also obtain information from the Maryland Office of the Attorney General by contacting them at 1-888-743-0023 and at their website: <https://www.marylandattorneygeneral.gov/>. If you are a New York Resident: You may contact the New York Department of State's Division of Consumer Protection. This office can be reached at 1 (800) 697-1220 or www.dos.ny.gov/consumerprotection. The New York City office is located at 123 William Street, New York, NY 10038-3804. The Albany office is located at One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001.