

August 04, 2022

Amelia M. Gerlicher  
AGerlicher@perkinscoie.com  
D. +1.206.359.3445  
F. +1.206.359.4445

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

**Re: Notification of Security Incident**

To Whom It May Concern:

I am writing on behalf of R. R. Donnelley & Sons Company (RRD), headquartered in Chicago, Illinois, to inform you a security incident involving access to personal data.

On December 23, 2021, RRD identified a systems intrusion in its technical environment. The Company promptly implemented a series of containment measures to address this situation, including activating its incident response protocols, shutting down its servers and systems and commencing a forensic investigation. Based on observed tactics, RRD identified the Threat Actor as being affiliated with a foreign ransomware group. RRD also determined that the Threat Actor gained access through a phishing attack that targeted several employees on or about November 29, 2021. RRD notified and is working with appropriate law enforcement authorities. Following this incident, RRD has also enriched its monitoring and analysis capabilities to combat future cyber threats.

RRD initially did not believe that the Threat Actor had removed any data from its environment. However, in mid-January 2022, RRD became aware that certain of its corporate data was accessed and exfiltrated by the Threat Actor. It evaluated the affected data with the assistance of a third-party data discovery provider and ultimately identified certain employee personal data among the documents exfiltrated. RRD also determined that the exfiltrated documents included certain data related to clients for whom RRD provides printing and mailing services. It has notified the affected clients accordingly. It expended significant effort to review each of the documents in order to identify potentially affected clients and individuals. The vendor provided the lists of affected individuals that included Maryland residents on July 12, 2022. Affected documents included names, addresses, social security numbers, and, in some cases, dates of birth, driver's license numbers, and/or credit card numbers of Maryland residents.

Office of the Attorney General  
August 04, 2022  
Page 2

RRD is notifying approximately 1173 Maryland residents of this incident beginning on August 5, 2022. A copy of that notification is attached.

Sincerely,

A handwritten signature in black ink, appearing to read "Amelia M. Gerlicher". The signature is fluid and cursive, with the first name "Amelia" being more prominent.

Amelia M. Gerlicher

Enclosure

RR DONNELLEY  
PO Box 474  
Monroe, WI 53566



0000003 01 SP 0.570 \*\*SNGLP H1 1 0031 07110-263165 -C01-P00003-I



JANE DOE  
123 Main Street  
NUTLEY, NJ 07110-2631

August 5, 2022

Dear JANE DOE:

We are writing to notify you of a matter that involved the unintended disclosure of some personal information about you held by R. R. Donnelley & Sons Company ("RRD"). 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 23, 2021, RRD identified a systems intrusion in our technical environment. We promptly implemented a series of containment measures to address this situation, including activating our incident response protocols, shutting down our servers and systems and commencing a forensic investigation. We took immediate action to isolate the incident. We determined that outside actors first accessed RRD systems on November 29, 2021, but it was not initially clear whether any personal data had been accessed or removed. However, on July 12, 2022, we learned that your personal information appears to have been exfiltrated from our corporate data system.

#### **WHAT INFORMATION WAS INVOLVED?**

The personal information included <<Data Elements>>.

#### **WHAT ARE WE DOING?**

Shortly after discovering the intrusion, RRD engaged forensic resources and other third parties to assist in its evaluation of the intrusion and shut down all impacted servers. While our investigation is complete, remediation efforts have been ongoing since discovery of the intrusion. RRD believes to the best of its knowledge that the intrusion has been removed and effective controls have been further implemented to prevent additional incidents from the attacker. Our information security response team and application quality assurance team have performed testing on our data environment prior to these systems being restored.

#### **WHAT CAN YOU 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, RRD has arranged for you to enroll, at your option, in a <<#>> Month membership of Experian's® IdentityWorks<sup>SM</sup> at no cost to you. 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: 10/15/22** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **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 10/15/22. Be prepared to provide RRD's engagement number ##### 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 additional information on other steps you can take, please see the enclosed sheet "ADDITIONAL STEPS TO PROTECT YOURSELF."

Sincerely,

A handwritten signature in cursive script that reads "Deborah L. Steiner".

Deborah Steiner  
Chief Compliance Officer  
[ethics@rrd.com](mailto:ethics@rrd.com)

## 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](http://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 or Credit Freeze

**Fraud Alerts:** 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. 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 online or 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 on-line 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.

Equifax: 877-478-7625 [www.equifax.com](http://www.equifax.com); PO Box 740241, Atlanta GA, 30374-0241

Experian: 888-397-3742 [www.experian.com](http://www.experian.com); PO Box 9532, Allen TX 75013

TransUnion LLC: 800-680-7289 [www.transunion.com](http://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](http://www.annualcreditreport.com). 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.

### 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 MARYLAND RESIDENT:** You may contact the Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, [marylandattorneygeneral.gov](http://marylandattorneygeneral.gov)

**IF YOU ARE A NORTH CAROLINA RESIDENT:** You may contact the North Carolina Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226, [ncdoj.com](http://ncdoj.com)

**IF YOU ARE AN RHODE ISLAND RESIDENT:** This incident affected approximately ## Rhode Island residents. You may also obtain information about preventing identity theft from the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903, (401) 274-4400, [riag.ri.gov](http://riag.ri.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](http://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.

**IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT:** You may contact the D.C. Attorney General's Office of Consumer Protection, 441 4th Street, NW, Washington, DC 20001, (202) 442-9828, [oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection)