

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

April 28, 2022

VIA E-MAIL: IDTheft@oag.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Breach

Dear Attorney General Frosh:

This notice is provided on behalf of my client, Janney Montgomery Scott LLC (“JMS”), following a ransomware attack at one of its vendors, R. R. Donnelley & Sons Company (“RRD”) that involved the names, dates of birth, addresses, financial account numbers, and Social Security numbers of one thousand five hundred and ninety eight (1,598) Maryland residents. JMS will provide written notice to these individuals on April 29, 2022, via U.S. Mail. The notice letter includes general advice on how to protect one’s identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services. A sample notice letter is enclosed and additional information about the incident is below.

On April 1, 2022, RRD notified JMS that certain RRD systems had been affected by ransomware, including systems that contained personal information of JMS clients. As soon as JMS learned about this incident, JMS immediately launched an investigation, engaged legal counsel with an expertise in cybersecurity, and began a comprehensive and thorough review of the data in order to determine what information was involved, who may have been affected, and where those people reside so that it could provide proper notice. On April 1, 2022, the investigation confirmed that the incident involved Maryland residents’ personal information.

JMS worked with RRD to understand which client accounts had been impacted, personal information that was compromised, and what steps RRD was taking to further protect data security. In addition, JMS conducted an internal review of the accounts that RRD reported had been impacted and, currently, neither identified nor suspects any suspicious behavior within the affected accounts due to this incident. JMS will continue to actively monitor the security of its systems and client accounts.

JMS is committed to protecting the security and confidentiality of sensitive information and is working with RRD to mitigate and remediate the incident and to help prevent something like this from happening again. Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure



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

April 29, 2022

H8281-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 CLIENT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

Dear Sample A. Sample:

On April 1, 2022, R. R. Donnelley & Sons Company (“RRD”), a third-party vendor that we use for processing customer communications, notified Janney that data, including a Janney client account file from 2017, had been removed from its computer network as a result of a recent ransomware incident. You are receiving this notice because your information was included in the information taken from RRD.

As soon as we learned this, we confirmed that Janney’s systems and your related account information at Janney remain safe and secure. Given our commitment to client service, we are providing this notice to all clients who have been affected, offering complimentary identity protection/credit monitoring, and sharing other proactive steps you may wish to take to help protect your information.

What Happened?

According to RRD, it identified an intrusion into its computer systems on December 23, 2021, and immediately took steps to contain the intrusion. Upon discovering the incident, RRD engaged a cybersecurity expert to determine what happened and assist in conducting a thorough review of any potentially compromised data.

What Information Was Involved

On April 1, 2022, RRD reported for the first time that the system intrusion resulted in the removal of a single Janney account file that included personally identifiable information belonging to some Janney clients. Based on the information made available to Janney, the file included: Name, Address, Account Number, Account Value, Birthdate, and Social Security Number.

What is Janney Doing?

We are committed to making this right and are investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Upon being notified that Janney client data had been removed from the RRD network, Janney immediately began following its cybersecurity protocols. We also worked with RRD to understand which client accounts had been impacted, the personal information that was compromised, and what steps RRD was taking to further protect data security.

In addition, we conducted an internal review of the accounts that RRD reported had been impacted. At this time, we do not suspect, nor did we identify, any suspicious behavior within your account due to this incident. We will continue to actively monitor the security of our systems and client accounts.

0000001



H8281-L01

What Can You Do Now?

- **Enroll in a complimentary, one-year membership with Experian:** In order to mitigate the potential impact of this breach, we are offering a **complimentary, one-year membership with Experian**. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.

What Else Can You Do Now?

We urge all Janney clients to remain vigilant against cybersecurity threats and identity theft. Please notify your Financial Advisor immediately if you notice anything suspicious. Additional proactive steps you can take to protect your accounts include:

- **Sign up for Online Access:** If you're not already enrolled, sign up for Online Access at www.myjanney.com.
 - **Set Notifications & Alerts Preferences:** You can elect to receive digital notifications and alerts for various account-related activities, including deposits and withdrawals.
 - **Eliminate paper mailings with eDelivery:** Elect to receive statements, confirmations, prospectuses, performance reports and/or tax forms electronically.
- Regularly review your account statements and monitor free credit reports for incidents of fraud and identity theft or any unauthorized activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

Please accept our apologies that this incident occurred and thank you for understanding. We remain fully committed to maintaining the privacy of personal information.

If you have questions or concerns about this issue, please contact your Financial Advisor. If your Financial Advisor is no longer at Janney, please contact our Service Desk at (215) 665-6100.

Sincerely,



David W. Houser
Chief Information Security and Privacy Officer

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com
--	---	--

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents. You may obtain one or more (depending on state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

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 new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance

0000001



statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

Office of the Attorney General Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
<https://ncdoj.gov/contact-doj/Phone>: 919-716-6000

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220

New York Attorney General
1-800-771-7755
<http://www.ag.ny.gov/home.html>

NEW MEXICO residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

RHODE ISLAND residents: You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General’s Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400



**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH
EXPERIAN IDENTITYWORKS MEMBERSHIP:**

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: July 19, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: ABCDEFGHI**

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 **July 19, 2022**. Be prepared to provide engagement number **B051862** as proof of eligibility for the identity restoration services by Experian. 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, Equifax and Transunion files 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.
- **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.