Retail Merchandising Services
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

RMS
RETAIL MERCHANDISING SERVICES, INC.

[redacted]

March 16, 2026

P 0000101103G0500

Dear [redacted],

Retail Merchandising Services ("RMS") is writing to inform you of a recent data security event that may impact certain information related to you. As discussed further below, we take this matter seriously, and have been working with cybersecurity specialists to investigate and respond. As our diligent investigation is now complete, we are sending you this letter because certain information related to you may have been affected.

What Happened? In January 2026 we first detected unusual activity within our email environment, and quickly took steps in response, including to secure the relevant account, as well as engage specialists to conduct a comprehensive investigation. The investigation determined that a single email account was intermittently accessed without authorization between November 24, 2025 and January 7, 2026. Accordingly, we conducted a thorough review of the relevant portions of the email account to determine the specific information present and to whom the information related. The preliminary results of the diligent review process were completed on February 25, 2026. Thereafter, we continued our efforts to identify necessary contact information and align resources for notification, which was completed on March 2, 2026. As certain information related to you was identified within the relevant data, we are providing you with this notification.

What Information Was Involved? Our review identified the following information related to you may have been accessed in connection with this matter: [redacted].

What We Are Doing. In response to this event, we took steps to secure the relevant account in our email environment and conducted a comprehensive investigation, which was aided by specialists. Once the information that may have been impacted was confirmed, we diligently reviewed the information and to whom it related in order to assess potential notification obligations. Once all necessary aspects of the comprehensive investigation were completed, notification was issued to relevant individuals and requisite regulatory authorities. As the obligation to safeguard the information in our care is of paramount importance to us, we are implementing additional security measures to further enhance our cybersecurity infrastructure, as well as revising and implementing additional policies and procedures regarding data and providing training to our workforce with a goal of minimizing the risk of a future similar incident.

What You Can Do. It is recommended that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact the financial institution or credit/debit card company. Additional information and resources are outlined in the *Steps You Can Take to Help Protect Your Information* section of the letter below.

Other Important Information. As an added measure, out of an abundance of caution, RMS is offering you complimentary credit monitoring for 12 months through Cyberscout, a TransUnion company. Please note, we cannot enroll you in these services directly, however, if you would like to enroll, information and instructions are included in this letter.

For More Information. We understand that you may have additional questions about this letter. Should you have questions or concerns, please contact our dedicated assistance line through Cyberscout, a TransUnion company at [redacted], from Monday - Friday 7:00am to 7:00pm Central Time. Please know that we take this matter and the obligation to safeguard the information in our care very seriously, and we are taking additional steps to bolster our environment and existing cybersecurity protocols.

Sincerely,

Retail Merchandising Services

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Offered Monitoring Services

We are providing you with access to single bureau credit monitoring/single bureau credit report/single bureau credit score services at no charge. To enroll in the monitoring services, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following code to enroll in the offered monitoring services: [redacted].

These services provide you with alerts for 12 months 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 bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services. Below please find descriptions of the offered services we are providing through Cyberscout.

- Credit Monitoring
    - Provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. The alert will be sent to you the same day that the change or update takes place with the bureau.
- Identity Theft Insurance
    - Enrolled individuals will have access to $1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud.
    - Available worldwide and includes coverage for identity theft expenses as well as unauthorized electronic fund transfer fraud.
- Fraud Remediation Services
    - Access to team of dedicated specialists at Cyberscout to help you in the event you experience fraud and assist with remediation.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Retail Merchandising Services is located at 8801 Brooklyn Blvd Brooklyn Park, MN55445.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 25 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection.