Avery Products Corporation
50 Pointe Drive
Brea, CA 92821
(714) 674-8500

January 16, 2025

VIA EMAIL ONLY

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

EMAIL: consumer@ag.iowa.gov

RE: Notice Of Data Event

Dear Attorney General:

I am writing to you on behalf of Avery Products Corporation ("Avery"), headquartered at 50 Pointe Drive, Brea, CA, 92821, a manufacturer and supplier of office supplies and print solutions. Pursuant to Iowa Code Chapter 715 , we are writing to notify you of a data security incident involving 556 Iowa residents.

Approximate date of incident: July 18, 2024-December 9, 2024.

How the breach was discovered: Ransomware attempt.

This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Avery does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

What Happened?

On December 9, 2024, Avery experienced a ransomware attempt on its network. Upon becoming aware of the attempt, Avery immediately took measures to secure its servers, network, and data and initiated an investigation with leading third-party forensic investigators to determine the scope and nature of the incident. The forensics firm determined that changes were made to the credit card entry form, and malware was added to the avery.com cart that might allow an unauthorized third party to view or "scrape" certain payment card information for online orders placed between July 18, 2024, and December 9, 2024, while customers entered information into the form. This ransomware attempt did not affect Avery's internal systems but rather an application used to process payments.

Initially, we had no evidence that any information was acquired (e.g., downloaded or exfiltrated from the website). Nor did we have any indication that the information had been used in any way – such as to make fraudulent purchases. We do not know if fraudulent charges are related to our website incident, but it now appears possible that payment-card (and other) information may have been acquired as we received two emails from a customer who indicated that they incurred a fraudulent charge. We received a number of similar reports this month, along with customers complaining about phishing attempts.

What Information Was Involved?

The investigation concluded that certain information was viewed or taken by an unauthorized third party, including first and last name, billing and shipping address, email address and phone number if provided, payment card information including CVV number and expiration date, and purchase amount, between July 18, 2024, and December 9, 2024, without authorization. Avery will notify the affected individuals because their information was present in the impacted system.

Number of Residents Affected

On January 8, 2025, Avery determined that 556 Iowa residents may be affected by this unauthorized access. Affected residents will receive notice via U.S. Mail pursuant to Pursuant to Iowa Code Chapter 715 in substantially the same form as the letter attached here as ***Exhibit A***. This notification is being sent simultaneously with the notification to affected residents.

Steps Taken and Steps to be Taken

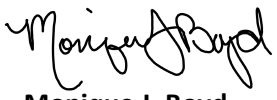
Upon learning of the incident, Avery immediately took measures to secure its network and data, launched an investigation, and engaged expert third-party cybersecurity firms for assistance. After determining there was unauthorized access, Avery undertook a lengthy and labor-intensive process to identify the personal information contained within the affected system.

Avery maintains a written information security program. In an effort to prevent something like this from happening again, Avery has implemented and will continue to adopt additional safeguards and security measures.

Avery will provide credit monitoring services for one (1) year, through CyberScout a TransUnion company to individuals whose personal information was potentially affected by this incident at no cost to these individuals.

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (440) 878-7273 or at mboyd@cclind.com.

Sincerely,



Monique J. Boyd
Senior Corporate Counsel **|** CCL Industries Inc.
Office: 440-878-7273**|** Email: mboyd@cclind.com
17890 Foltz Parkway, Strongsville, OH 44149

Avery Products Corporation
50 Pointe Drive
Brea, CA 92821
(714) 674-8500

Via First- Class Mail
Name
Address Line 1
Address Line 2
City, State, Zip

Date

Re: Notice of Data Security Incident

Dear [Name]:

Avery Products Corporation ("Avery") is writing to notify you of an incident that may affect the security your personal information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On December 9, 2024, Avery became aware of a ransomware attack relating to certain systems. Avery immediately launched an investigation, with the aid of forensic experts, to determine the nature and scope of the activity. Our investigation determined that an unauthorized actor inserted malicious software that was used to "scrape" credit card information used on our website avery.com (https://avery.com) between July 18, 2024, and December 9, 2024. Avery undertook a lengthy and labor-intensive process to identify the personal information contained in the affected system, and then reviewed its internal records to locate the appropriate mailing addresses for the impacted individuals. We are providing notice to you because we confirmed that your information was present in the affected system at the time of the incident and may have been viewed or taken by the unauthorized actor.

What Information Was Affected? Our investigation confirmed that the information present in the affected systems may have included: your first and last name, billing and shipping address, email address and phone number if provided, payment card information including CVV number and expiration date, and purchase amount. The information present is limited to the list in the preceding sentence. As you are aware, Avery does not collect Social Security numbers, driver's license numbers or other government-issued ID numbers, dates of birth, or other sensitive personal information. There is no indication that your online account credentials have been compromised. Impacted data may vary depending on the individual.

Initially, we had no evidence that any of the information was acquired (e.g., downloaded or exfiltrated from the website). Nor did we have any indication that the information had been used in any way – such as to make fraudulent purchases. We do not know if fraudulent charges are related to our website incident, but it now appears possible that payment-card (and other) information may have been acquired as we received two emails from customers who indicated that they incurred a fraudulent charge and/or phishing email. We received a number of similar reports this month. We are therefore providing you with this notice so you can take steps to protect yourself.

What Are We Doing? Avery takes the security of personal information in our care very seriously. Avery has security measures in place to protect the information in our possession and we continue to assess and update our security measures and train our employees to safeguard the privacy and security of information in our care. This incident has been reported to certain state regulators, and Attorneys General.
We are also providing you with access to 12 months of complimentary credit monitoring services through Cyberscout, a TransUnion company.

What Can You Do? Avery encourages you to remain vigilant, watch out for phishing attempts, review your financial and other account statements, and to monitor your credit reports for suspicious activity. We also encourage you to enroll in the 12 months of complimentary credit monitoring services through TransUnion. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll in and receive these services. Avery will cover the cost of this service, however, you will need to enroll yourself in the credit monitoring service if you would like to do so.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at (877) _____, Monday through Friday, 9:00 a.m. to 7:00 p.m. Eastern Time.

We sincerely regret any inconvenience this incident may cause you.

Sincerely,

Mark Cooper
President, Avery Products Corporation

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. 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.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>**

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.

Monitoring. You should always remain vigilant and monitor your accounts and credit reports for suspicious or unusual activity.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report.

If you request a security freeze with the above consumer reporting agencies, you may need to provide the following information: (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; and (5) any applicable incident report or complaint with a law enforcement agency. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Fraud Alerts. As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years.

Should you wish to place a security freeze or fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

File Police Report. You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. **This notice was not delayed by a law enforcement investigation.**

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to 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.

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, 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 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 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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island*:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16 th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft : New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697-1220, http://www.dos.ny.gov/consumerprotection

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov.