Notice of Data Breach

Dear [Customer],

This letter is to notify you of a security incident that Colson Group USA ("Colson") recently identified during a routine review of the operations of [merchant]'s website located at [merchant's website] (the "Website").

Colson maintains the Website provided by [merchant] and is therefore providing this notice on [merchant's] behalf. This letter is being sent to you because [merchant's] records reflect that you placed an order on the website between June 19, 2025 and December 16, 2025, which is within the time period that certain customer information may have been accessed without authorization. We sincerely apologize and deeply regret that this incident has occurred.

What Happened?

On December 16, 2025, Colson discovered unauthorized Javascript code that appeared to have been added to the Website's code. Colson believes that certain customer information may have been "skimmed" between June 19, 2025 and December 16, 2025.

What Information Was Involved?

It is undetermined whether any third parties have accessed or acquired customers' information. However, because the Website processes online orders and accepts credit card payments, Colson believes that credit card information and other customer information including first and last names and physical addresses may have been affected. You are receiving this letter because [merchant's] records reflect that you entered personal information while placing an order on the Website while the unauthorized Javascript code remained installed.

Notice of Data Breach

What We Are Doing.

Upon discovery of the unauthorized code, Colson shut down the Website, removed the unauthorized code, and decommissioned the Website. Colson also initiated its incident response procedures and immediately began an investigation. As part of Colson's ongoing investigation efforts, Colson retained an outside forensics company to complete a thorough review of the incident. As a result of this review, it could not be determined whether any customer information was accessed or acquired by third parties. Colson also has not been informed by any business partner or customer that specific information was accessed or acquired.

What You Can Do.

Although Colson's investigation of the incident has not conclusively determined that any customer information was directly impacted, we recommend as a precaution that you monitor your payment card statements and notify your card issuer immediately for any unfamiliar transactions. We also recommend you remain vigilant in reviewing your free credit reports, as well as placing fraud alerts and security freezes on your accounts.
We are providing you with the attached Recommended Steps document that includes steps you may take to help protect your personal information.

For More Information.

We value the security and privacy of your information and we apologize for any inconvenience or concern caused by this incident. We are working hard and increasing our efforts to help safeguard your personal data that is in our custody and protect it from future incidents.

If you have any questions or need additional information about this notice, please contact the [merchant] at [phone], [email], or [address].

Sincerely,

DocuSigned by:
Rob Switzer

Robert Switzer
Colson Incident Response Team Manager
Global Director of Infrastructure and Security

Recommended Steps to Help Protect Your Information

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You should report suspected identity theft to law enforcement, including your state's attorney general and the Federal Trade Commission. If you are a victim of identity theft, you may file a police report with your local law enforcement.

You can obtain information from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. The FTC can be reached at:

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

Free Credit Report: You are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting companies. To obtain your free credit report visit annualcreditreport.com or call 1-877-322-8228. You will need to provide your name, address, social security number, and date of birth to verify your identity.

Fraud Alerts: You can place fraud alerts with the three major credit bureaus by phone and also via their websites. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

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

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to initiate a security freeze.

You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	http://freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

You may obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

New York Residents: New York State Attorney General, The Capitol, Albany, New York 12224; https://ag.ny.gov/; Telephone: 1-800-771-7755.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001; www.ncdoj.gov; Telephone: 1-877-566-7226 or 1-919-716-6400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 2