



You are here: [Homepage](#) → [About ALDI](#) → [Notice Regarding Payment Card Issue](#)

June 6, 2023

Notice of Data Breach

To Our Valued Customers,

We recently experienced an issue involving payment card skimming devices that were placed by an unauthorized third party in six ALDI stores located in California.

What Happened?

We recently learned that an unauthorized party gained physical access to a checkout terminal at six stores located in California and installed a device designed to acquire certain customer payment card information. Based on our investigation, we believe the issue involved a single terminal at each of the following six stores located at:

- 1352B W Valley Pkwy, Escondido, CA on approximately May 15, 2023
- 14626 Roscoe Blvd, Panorama City, CA between approximately May 13 and May 15, 2023
- 5190 Stockdale Hwy, Bakersfield, CA between approximately May 8 and May 15, 2023
- 203 Towne Center Dr, Compton, CA on approximately May 16, 2023
- 3330 W. Century Blvd, Inglewood, CA between approximately May 16 and May 17, 2023
- 22741 Victory Blvd, West Hills, CA on approximately May 17, 2023

What Information Was Involved?

The issue may have affected the payment card information of customers who swiped their cards at the affected terminals during the relevant timeframe, including cardholder names, card numbers, card expiration dates, card pins and security codes.

What We Are Doing

After learning of the issue, we quickly removed the device from the affected terminal at each of the six stores, and took steps to secure our systems and determine the nature and scope of the issue. We also reported the issue to the payment card brands and law enforcement authorities. In addition, we have conducted additional reviews at ALDI stores nationwide to help prevent similar issues.

What You Can Do

We sincerely regret that this issue may affect some of our customers who shopped at the affected stores in California. We take our obligation to safeguard customer information very seriously and are alerting customers about this issue so they can take steps to protect themselves. If you believe your payment card information may have been affected, you should contact the issuer of the card used at the affected store to let them know. U.S. consumers are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage affected customers to remain vigilant by reviewing their account statements and monitoring their free credit reports. See the Reference Guide below for additional steps customers can take to protect their information.

For More Information

If you have any questions regarding this issue, please call 1-800-325-7894, Monday through Friday from 9 a.m. to 5 p.m. Eastern Time.

Again, we regret any inconvenience this may cause our customers.

Sincerely,

Paul Piorkowski
ALDI Inc.
Regional Vice President

Reference Guide

We encourage affected customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card issuer or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services, LLC. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	https://www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	https://www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016-2000	1-800-680-7289	https://www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)