NOTICE OF DATA INCIDENT

Dated: January 24, 2024

Co-opportunity Market ("Co-opportunity Market," "we," "us," "our") recently experienced a data security incident that could affect some of your personal information.

While we are currently investigating the incident and while we do not know that any particular individual has been affected, in the interest of protecting our customers, Co- opportunity Market has elected to disclose what it has learned about this criminal act.

Please review this notice carefully to learn about the incident and about the resources you can use to monitor your personal information and help protect against identity theft.

What Happened?

On January 21, 2024, Co-opportunity Market's Santa Monica store discovered that credit card skimmers were installed on four of our point-of-sale ("POS") devices. A credit card skimmer is a device that is illegally installed on POS devices so that when customers swipe their credit or debit cards using the card reader, the credit card skimmer can scan or skim their card information. On January 22, 2024, we discovered a credit card skimmer was also installed at one of our devices in Culver City, as well. At this time, Co-opportunity Market is not able to provide the precise timeframe during which the credit card skimmers were put in place.

Co-opportunity Market immediately contacted the Santa Monica Police Department and the Culver City Police Department and the affected POS devices were removed.

What Information Was Involved?

The credit card skimmers may have collected credit or debit card information, including credit and debit card numbers and security codes or pins.

What Are We Doing?

Co-opportunity Market deeply regrets any inconvenience that this criminal incident may have caused to our customers. As stated above, Co-opportunity Market immediately contacted the Santa Monica and Culver City Police Departments and the affected POS devices were removed.

Please be assured that Co-opportunity Market takes this matter seriously and will continue to diligently work to protect our customers.

What Can You Do?

If you have recently shopped at Co-opportunity Market, you should:

- Monitor your credit card statements for unusual and unauthorized charges.
- Contact your credit card company to advise them of the incident and to inquire about any proactive steps you should be taking to protect your credit card account.

- Review the California Attorney General website on protecting yourself following a data breach: https://oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers.

For more information on how you can help protect yourself, please review the page “Additional Resources” attached to this notice.

More Information

If you have any questions or concerns about this incident, please contact us by e-mailing us at Membership@Coopportunity.com

Additional Resources

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).