Giant Food of Maryland, LLC
8301 Professional Place, Suite 115
Landover, MD 20785

May 12, 2020

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing to notify you regarding the nature and circumstances of a recent data security issue.

On March 5, 2020, we learned that someone had illegally placed a device that skims information from payment cards on top of a pin pad at one of the store's self-checkout registers at the Giant Food store located at 1345 Park Road, NW, Washington, DC.

Immediately upon learning of the issue, we took steps to secure this checkout lane and review video surveillance to attempt to determine how long the device had been in use. We also contacted law enforcement and began working closely with a third-party forensic investigator to determine what, if any, data it had captured.

The device was installed on *only one* pinpad in the store and the forensic investigation concluded that it was capable of capturing data from payment card EMV chips but not from magnetic stripes. The personal information found on the device included names, payment account numbers, and expiration dates for a limited number of customers who used that particular self-checkout terminal for a limited time period before March 5th. The device was designed such that extraction of the captured payment card transaction data would require manual insertion of a reader device into the card capture device, but the data could not be accessed remotely. We have been unable to determine if any data was extracted from the device, but it is possible that data was extracted before the shimmer was discovered by Giant Food. Based on our investigation, at this time, we have no evidence that any of the information has been misused as a result of this issue.

There is approximately one (1) New Hampshire resident affected by this issue. Attached for your reference is a copy of the notice that is being sent to the affected individuals today. Please do not hesitate to contact me if you have any questions.

Very truly yours,

Bob Bennett, Vice President of Operations, Giant Food

Enclosure

Giant Food of Maryland, LLC
8301 Professional Place, Suite 115
Landover, MD 20785

May 12, 2020

Dear **[Name]**,

We are writing to notify you of a recent issue that involves aspects of your personal information. On March 5, 2020, we learned that someone had illegally placed a device that skims information from payment cards on top of a pin pad at one of the self-checkout registers at the Giant Food store located at 1345 Park Road, NW, Washington, DC.

We have identified that you may have been affected, and we want to make you aware of how we are handling the situation and offer recommendations for how you may remain vigilant in safeguarding your information.

Immediately upon learning of the issue we took steps to secure this checkout lane and review video surveillance to determine how long the device had been in use. We also contacted law enforcement and began working closely with a third-party forensic investigator to determine what data, if any, it had captured.

The device was installed on *only one* pin pad in the store and the forensic investigation concluded that it was capable of capturing data from payment card EMV chips, but not from magnetic stripes. The personal information found on the device included names, payment account numbers, and expiration dates for a limited number of customers who used that particular self-checkout terminal for a limited time period before March 5th. The device was designed such that extraction of the captured payment card transaction data would require manual insertion of a reader device into the card capture device, but the data could not be accessed remotely. We have been unable to determine if any data was extracted from the device, but it is possible that data was extracted before the shimmer was discovered by Giant Food.

Based on our investigation, at this time, we have no evidence that any of the information has been misused as a result of this issue. However, out of an abundance of caution, we are notifying you as we have identified that you may be affected. Please know we take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies (Equifax, Experian and TransUnion). To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

The attached Reference Guide provides recommendations by the U.S. Federal Trade Commission on the protection of personal information. We hope this information is useful to you. If you have any questions regarding this issue, please call 888-469-4426 Monday-Friday from 8:00am-7:00pm ET or Saturday 8:00am-5:00pm ET.

We apologize for any inconvenience.

Sincerely,

Bob Bennett, Vice President of Operations, Giant Food

Reference Guide

We encourage affected individuals 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") 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 consumer reporting agencies provide free annual credit reports only through their websites, toll-free numbers or request forms.

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 can't be explained, then you will need to call the creditors involved. Information that can't 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 company 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 (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	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	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); and
- Proof of your current residential address (such as a current utility bill or account statement).

For District of Columbia Residents. You can obtain information from the Office of the Attorney General for the District of Columbia about steps you can take to avoid identity theft. You may contact the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
www.oag.dc.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us