

16954



The Stop & Shop Supermarket Company, LLC
1385 Hancock Street
Quincy, MA 02169

May 15, 2020

[Customer Name]
[Customer Address]
[City], [State] [ZIP]

Dear [Customer Name],

We are writing to notify you of a recent issue that involves aspects of your personal information. On [insert date], 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 Stop & Shop store located at [insert store address].

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 to review video surveillance to determine when the device was installed. We also notified law enforcement and began working closely with a third-party forensic investigator to determine what data, if any, it had captured.

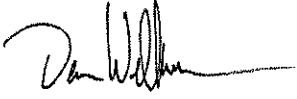
The device was installed on *only one* pin pad in the store and the forensic investigation concluded that it was capable of capturing data from payment card EMV chips, but not from magnetic stripes. The personal information found on the device included names, payment account numbers, and expiration dates for a limited number of customers who used that particular self-checkout terminal from [insert start date] to [insert end date]. 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 device was discovered by Stop & Shop.

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. 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 us at 1-800-767-7772 Monday-Friday from 8:00 a.m. - 7:00 p.m. ET, or Saturday 8:00 a.m. - 5:00 p.m. ET.

We apologize for any inconvenience.

Sincerely,

A handwritten signature in black ink, appearing to read "Dean Wilkinson", with a long horizontal flourish extending to the right.

Dean Wilkinson
Senior Vice President, Operations
The Stop & Shop Supermarket Company, LLC

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 Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/internet/resource-center>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
<http://www.riag.ri.gov>

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.