Identity Theft Device Found Attached to One Darien Stop and Shop Self-Checkout Scanner

Author : David Gurliacci

Categories : Consumer and Finances, Public Safety

Tagged as : Skimmer, Skimmer 2020, Skimmer Device, Stop and Shop 2020

Date : May 17, 2020

Darien Stop & Shop customers who used one of the self-checkout scanners may be the victims of identity theft, the grocery company has announced.

Someone illegally installed a skimming device (or "skimmer") at that register at the Stop & Shop in the Goodwives Shopping Center at 25 Old Kings Hwy. North.

The skimmer was attached for five days at the end of last month — from April 26 to 30 at the Darien store, according to the company.

If you may have opted for self-checkout at the Darien supermarket from April 26 to 30, you may want to check the account of any card you may have used to see if there are suspicious transactions, the Stop & Shop

announcement said. You may also want to change the password on those accounts. (See below for what else you can do.)

The company said it doesn't know whether or not data was extracted from cards or that the information has been misused.

The company announcement said: "We have been unable to determine if any data was extracted from the devices, but it is possible that data was extracted before the devices were 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 some of our customers may be affected."

What Else You Can Do

"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," said the announcement, which went out over the name of Dean Wilkinson
senior vice president, operations for the Stop & Shop Supermarket Company.

If your bank or credit card account is at risk, you can do the following, the company said:

- 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 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 8:00am-7:00pm ET, or Saturday 8:00am-5:00pm ET.

See the bottom of this article for even more things you can do, according to Stop & Shop.

Some Information on How It Happened

The company didn't say a lot about the crimes, including how it found out that the skimmers had been installed, but it did indicate it knows when and where, presumably the result of checking security camera records.

"We recently discovered that, at each of five Stop & Shop stores, 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," the company said in a news release on Friday.

Other skimmers were found at four other Stop & Shop supermarkets — three clustered within 20 miles of each other in northern New Jersey (all closer to New York City than Darien is) and another in Framingham, Massachusetts, near Boston, more than 200 miles away. Here's a map.

"The devices were installed on only one pin pad at each of the affected stores, and the forensic investigation concluded that the devices were capable of capturing data from payment card EMV chips, but not from magnetic stripes," the announcement said.

EMV Chips

- Ironically, EMV chips were introduced in recent years to provide better security than magnetic strips on the back of credit cards. CreditCards.com explains:
- EMV — which stands for Europay, Mastercard and Visa — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. In the wake of numerous large-scale data breaches and increasing rates of counterfeit card fraud, U.S. card issuers have migrated to this new technology to protect consumers and reduce the costs of fraud.
- “These new and improved cards are being deployed to improve payment security, making it more difficult for fraudsters to successfully counterfeit cards,” says Julie Conroy, research director for retail banking at Aite Group, a financial industry research company. “It’s an important step forward.”

When It Happened

The time periods of when the skimmers were in place varies within each store, and only two skimmers were working on the same days, both in New Jersey locations.

Of the four locations, the first time a scanner is known to have been used was in Berkeley Heights, New Jersey, where it was used for only three days — from Feb. 8 to 10.

At a Clifton, New Jersey Stop & Shop, a skimmer was in place for the longest period among the four stores — about a month, from March 14 to April 16. During part of that period, from March 28 to April 9, a skimmer was used in the Bloomfield, New Jersey store.

From April 22 to 26, the Framingham store was hit, then, finally, Darien from April 26 to 30. Stop & Shop didn't say whether or not any of the same devices may have been used at more than one store.

(The Darien store was extensively renovated in late 2019, several months before company officials found that the skimmer was installed there.)

The company said it "recently" discovered the crimes.

"It is important to understand that not all Stop & Shop locations were impacted by this issue," the announcement said, indicating that other stores, perhaps all of them, have been checked.

The Last Skimmer Incident in Darien

More than three years ago, on Feb. 1, 2017, Darienite.com reported:

"Bank officials at Fairfield County Bank at 714 Post Road, doing a regular check of their video surveillance recordings, found that a man was trying to attach a skimming device to an automated teller machine at the bank, failed, then returned to scam the bank out of $2,500 to $3,000."

Skimmers typically are used as a way of getting a cardholder's PIN code, which is why it's important to change it if one of yours may have been used in the recent incident.

Text of the Announcement

Here's the entire announcement *from the Stop & Shop website, except for information on steps customers can take to protect themselves that are specific to states other than Connecticut:*

To Our Valued Stop & Shop Customers,

We recently learned of an issue involving some of our customers' personal information. We recently discovered that, at each of five Stop & Shop stores, 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.

A list of locations affected by this activity and their respective estimated dates of exposure is available below. It is important to understand that not all Stop & Shop locations were impacted by this issue. In addition, not all customers who visited the listed stores during the relevant time periods are affected.

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 devices were installed on only one pin pad at each of the affected stores, and the forensic investigation concluded that the devices were capable of capturing data from payment card EMV chips, but not from magnetic stripes. The personal information found on the devices included names, payment account numbers, and expiration dates for a limited number of customers who used the particular self-checkout terminals during the estimated dates of exposure below. The devices were 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 devices, but it is possible that data was extracted before the devices were 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 some of our customers 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 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 8:00am-7:00pm ET, or Saturday 8:00am-5:00pm ET.

We apologize for any inconvenience.

Sincerely,

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

List of Stores Affected by the Activity and Estimated Windows of Exposure

- **Connecticut**
  Stop & Shop #2610
  25 Old King's Highway N.
  Darien, CT 06820
  Exposure Dates: 4/26/2020-4/30/2020
- **Massachusetts**

Stop & Shop #8
19 Temple Street
Framingham, MA 01701
Exposure Dates: 4/22/2020-4/26/2020

- **New Jersey**
  Stop & Shop #834
  404 Springfield Avenue
  Berkeley Heights, NJ 07922
  Exposure Dates: 2/8/2020-2/10/2020
- **New Jersey**
  Stop & Shop #800
  8 Franklin Street
  Bloomfield, NJ 07003
  Exposure Dates: 3/28/2020-4/9/2020
- **New Jersey**
  Stop & Shop #2802
  1185 Broad Street
  Clifton, NJ 07013
  Exposure Dates: 3/14/2020-4/16/2020

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 Information Services LLC
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com
Experian Inc.
P.O. Box 9554
Allen, TX 75013
1-888-397-3742 www.experian.com
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).