Two Chipotle Restaurants in Darien Affected by Security Breach Leaving Customers Vulnerable to ID Theft

Author : David Gurliacci

Categories : Business, Food & Drink, Restaurants & Bars, Public Safety

Tagged as : Chipotle 2017Identity Theft 2017

Date : May 28, 2017

When some hacker got into Chipotle digital records containing customer debit and credit card information, only some of the chain's restaurants were affected, but among them were the two restaurants in Darien, according to the company.

Chipotle announced on Friday that the data breach affected certain restaurants at certain times. In its online announcement, the company also provided a search function to show whether its restaurants in particular communities were affected by the breach. Both the Chipotle at 71 Post Road and at the Interstate 95 Darien location were affected. Only credit or debit cards used from March 26 to April 18 were vulnerable from the hacking.

If you went to either Chipotle in Darien in that span of time, your credit card information could be used and someone could charge something to your account, according to Chipotle. The company advises checking your accounts for any unauthorized payments.

Chipotle restaurants in Greenwich, Riverside, Westport, Fairfield, Bridgeport and Milford were also affected.

Here's the company's announcement*:*

Chipotle Mexican Grill, Inc. (Chipotle) is providing further information about the payment card security incident that Chipotle previously reported on April 25, 2017. The information comes at the completion of an investigation that involved leading cyber security firms, law enforcement, and the payment card networks.

The investigation identified the operation of malware designed to access payment card data from cards used on **point-of-sale (POS) devices** at certain Chipotle restaurants between March 24, 2017 and April 18, 2017.

The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS device.

There is no indication that other customer information was affected. A list of affected Chipotle restaurant locations and specific time frames is available here. Not all locations were involved, and the specific time

frames vary by location.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

During the investigation we removed the malware, and we continue to work with cyber security firms to evaluate ways to enhance our security measures. In addition, we continue to support law enforcement's investigation and are working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring.

If customers have questions regarding this incident, you can call 888-738-0534 Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. EDT, or Saturday and Sunday between the hours of 9:00 a.m. and 5:00 p.m. EDT.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- **Equifax**
  Phone: 1-800-685-1111
  P.O. Box 740256
  Atlanta, Georgia 30348
  www.equifax.com
- **Experian**
  Phone: 888-397-3742
  P.O. Box 9554
  Allen, Texas 75013
  www.experian.com
- **TransUnion**
  Phone: 888-909-8872
  P.O. Box 105281
  Atlanta, GA 30348-5281
  www.transunion.com

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies:

- **Equifax**, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert.

An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

Security Freeze: 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.

There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. In order to request a security freeze, the consumer reporting agencies may require proper identification prior to honoring your request and ask that you provide:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As the instructions for establishing a security freeze differ from state to state, please contact the three consumer reporting agencies to find out more information.