

# BakerHostetler

## Baker&Hostetler LLP

312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202-4074

T 513.929.3400  
F 513.929.0303  
www.bakerlaw.com

Craig A. Hoffman  
direct dial: 513.929.3491  
cahoffman@bakerlaw.com

May 26, 2017

### VIA EMAIL ([CONSUMER@IOWA.GOV](mailto:CONSUMER@IOWA.GOV)) AND UPS NEXT DAY AIR

Office of the Attorney General of Iowa  
Director of the Consumer Protection Division  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines, IA 50319

*Re: Incident Notification*

Dear Sir or Madam:

Chipotle Mexican Grill, Inc. (“Chipotle”) understands the importance of protecting the payment card information of its customers. On April 5, 2017, Chipotle identified a suspicious process running on the point of sale devices at certain Chipotle Mexican Grill restaurants. Chipotle immediately started an investigation with the assistance of leading computer security firms to determine the nature and scope of the issue. On April 25, 2017, Chipotle added a page to its website notifying its customers of the investigation. By May 23, 2017, findings from the investigation were available to accurately identify the restaurants and specific time frames involved in this incident.

Findings from the completed investigation show the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Chipotle Mexican Grill and restaurants between March 24, 2017 and April 18, 2017. The malware specifically 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, and the incident did not involve payment cards used on Chipotle’s websites.

Chipotle does not collect the mailing or email address from customers when they use their payment cards. Thus, Chipotle is not able to identify the name and mailing address of individuals who used their card during the time period of this incident. Chipotle, therefore, is

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

unable to identify the number of Iowa residents that used a card during the time frame of this incident. Instead, on May 26, 2017, pursuant to Ia. Code Ann. §§ 715C.1 et seq., Chipotle provided substitute notification to Iowa residents who may have used their payment cards at affected Chipotle Mexican Grill restaurants during the time period of this incident by posting a statement on its websites and issuing a press release (copies enclosed). Notification is being provided in the most expeditious manner possible and without unreasonable delay after measures were taken to eradicate the malware and findings became available to determine the apparently affected restaurants and specific time frames. *See* Ia. Code Ann. §§ 715C.1 et seq.

Chipotle has removed the malware and continues to work with cyber security firms to evaluate ways to enhance its security measures. In addition, Chipotle has notified law enforcement about the incident and is also working closely with the payment card companies to identify potentially affected cards. Lastly, Chipotle established a dedicated call center that customers can call with related questions.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Craig A. Hoffman  
Partner

Enclosure



MENU NUTRITION FOOD WITH INTEGRITY WHAT'S HAPPENING CATERING  
DELIVERY TALK TO US

# CHIPOTLE MEXICAN GRILL REPORTS FINDINGS FROM INVESTIGATION OF PAYMENT CARD SECURITY INCIDENT


California residents please [click here](#).

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](http://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](http://www.equifax.com)

**Experian**

Phone: 888-397-3742  
P.O. Box 9554  
Allen, Texas 75013  
[www.experian.com](http://www.experian.com)

**TransUnion**

Phone: 888-909-8872  
P.O. Box 105281  
Atlanta, GA 30348-5281  
[www.transunion.com](http://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](http://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](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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/](http://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.

---

**If you are a resident of Maryland**, you may contact the Maryland Attorney General’s Office at 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 .

**If you are a resident of North Carolina**, you may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716- 6400.

**If you are a resident of Massachusetts**, note that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$5 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

**If you are a resident of Rhode Island**, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401)-274-4400 . You have the right to obtain a police



report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

**If you are a resident of West Virginia**, you have the right to the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

---

## **RESIDENTS OF CALIFORNIA**

### **NOTICE OF DATA BREACH**

#### **WHAT HAPPENED**

Chipotle Mexican Grill, Inc. 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.

#### **WHAT INFORMATION WAS INVOLVED**

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.


#### **WHAT YOU CAN DO**

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.


#### **WHAT WE ARE DOING**

During the investigation we removed the malware, and we continue to work with cyber security firms to evaluate ways to enhance 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.

## FOR MORE INFORMATION

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](http://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](http://www.equifax.com)

### Experian


Phone: 888-397-3742   
P.O. Box 9554  
Allen, Texas 75013  
[www.experian.com](http://www.experian.com)

### TransUnion

Phone: 888-909-8872   
P.O. Box 105281  
Atlanta, GA 30348-5281  
[www.transunion.com](http://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](http://www.ftc.gov/idtheft)

---

## RESTAURANTS AND TIMEFRAMES THAT RELATE TO THIS NOTIFICATION

You can use the locator tool below to check for a restaurant identified during the investigation and its specific time frame. **Please note that not all locations were identified, and the specific time frames vary by location.**

**SELECT THE STATE YOUR PAYMENT CARD WAS**

Please select a state 

**USED:**

## SUBSCRIBE TO OUR EMAIL

Enter your email address to receive future updates and newsletters from Chipotle. You can unsubscribe at any time. View [Terms of Use](#) and [Privacy Policy](#).

## SUBSCRIBE TO OUR MOBILE LIST

Enter your mobile number to receive Chipotle updates and offers via text. Recurring automated marketing messages will be sent to the mobile number provided. Consent is not a condition of purchase. Msg and data rates may apply. Text **STOP** to 888222. Text **HELP** for help. View [Terms of Use](#) and [Privacy Policy](#).

## STAY CONNECTED



## SEARCH FOR CAREERS NEAR YOU

### ABOUT

[Company](#)

[Investors](#)

[Careers](#)

[California Transparency  
in Supply Chain Act](#)

[Privacy Policy](#)

[Terms of Use](#)

[Accessibility Statement](#)

[Talk To Us](#)

### OUR OTHER SITES

[Cultivate Foundation](#)

[The Chipotle Store](#)

[Gift Cards](#)

[Pizzeria Locale](#)

[Tasty Made](#)

### CHIPOTLE AROUND THE WORLD

USA ▼

© 2017 Chipotle Mexican Grill  
1401 Wynkoop St.  
Denver, CO 80202  
[www.chipotle.com](http://www.chipotle.com)







## **Chipotle Mexican Grill Reports Findings from Investigation of Payment Card Security Incident**

DENVER, May 26, 2017 – Chipotle Mexican Grill (NYSE:CMG) is providing further information about the payment card security incident that the company 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 and Pizzeria Locale 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. Lists of affected Chipotle and Pizzeria Locale restaurant locations and specific time frames are available at [www.chipotle.com/security](http://www.chipotle.com/security) and [www.pizzerialocale.com/security](http://www.pizzerialocale.com/security), respectively. Not all locations were involved, and the specific time frames vary by location.

Customers that used a payment card at an affected location during its at-risk time frame should remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their 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 the payment card.

During the investigation, Chipotle removed the malware and continues to work with cyber security firms to evaluate ways to enhance its security measures. In addition, Chipotle continues to support law enforcement's investigation and is 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, they can visit [www.chipotle.com/security](http://www.chipotle.com/security) or [www.pizzerialocale.com/security](http://www.pizzerialocale.com/security), as applicable, or call 1-888-738-0534 Monday through Friday between the hours of 9:00 a.m. and 9:00 p.m. ET (closed for Memorial Day). During Memorial Day weekend, customers may call Saturday and Sunday, 9:00 a.m. to 5 p.m. ET.

### **ABOUT CHIPOTLE**

Steve Ells, Founder, Chairman and CEO, started Chipotle with the idea that food served fast did not have to be a typical fast food experience. Today, Chipotle continues to offer a focused menu of burritos, tacos, burrito bowls, and salads made from fresh, high-quality raw ingredients, prepared using classic cooking methods and served in an interactive style allowing people to get exactly what they want. Chipotle seeks out extraordinary ingredients that are not only fresh, but that are raised responsibly, with respect for the animals, land, and people who produce them. Chipotle prepares its food using only real, whole ingredients, and is the only national restaurant brand that uses absolutely no added colors, flavors or other industrial additives typically found in fast food. Chipotle opened with a single restaurant in Denver in 1993 and now operates more than 2,300 restaurants. For more information, visit [Chipotle.com](http://Chipotle.com)

###