POSTED AT HTTPS://BRINKER.MEDIAROOM.COM/CHILISDATAINCIDENT

NOTICE OF UNAUTHORIZED ACCESS TO OR ACQUISITION OF CHILI'S® GRILL & BAR GUEST DATA

Updated May 18, 2018

Dear Valued Guests,

This notice is to make you aware that some Chili's restaurants have been impacted by a data incident, which may have resulted in unauthorized access or acquisition of your payment card data, and to provide you information on steps you can take to protect yourself and minimize the possibility of misuse of your information.

We sincerely apologize to those who may have been affected and assure you we are working diligently to resolve this incident. We are offering free credit monitoring and fraud resolution services for those who may have been affected by this incident.

+++++++

What Happened? On May 11, 2018, we learned that some of our Guests' payment card information was compromised at certain Chili's restaurants as the result of a data incident. Currently, we believe the data incident was limited to between March – April 2018; however, we continue to assess the scope of the incident. We deeply value our relationships with our Guests and sincerely apologize to those who may have been affected.

We immediately activated our response plan upon learning of this incident. We are working with third-party forensic experts to conduct an investigation to determine the details of what happened. Below is information on how you can protect yourself and your information.

We are working diligently to address this issue and our priority will continue to be doing what is right for our Guests. We are committed to sharing additional information on this ongoing investigation with our Guests as we learn more.

What Information Was Involved? The investigation into this incident is ongoing; however, based on the details currently uncovered, we believe that malware was used to gather payment card information including credit or debit card numbers and cardholder names, and potentially expiration dates and CVV codes from our payment-related systems for in-restaurant purchases at certain Chili's restaurants. Currently, we believe the data incident was limited to between March – April 2018; however, we continue to assess the scope of the incident.

Chili's does not collect social security numbers, full date of birth, or federal or state identification numbers from Guests. Therefore, this personal information was not compromised.

What Are We Doing? We are working with third-party forensic experts to conduct an extensive investigation to confirm the nature and scope of this incident. Law enforcement has been notified of this incident and we will continue to fully cooperate. We are working with ID Experts® to provide Guests who may have been impacted with free fraud resolution and credit monitoring services.

ID Experts – Enrollment

For those who may have been impacted by the incident, we are offering free identity theft protection services through ID Experts to provide you with MyIDCare™, which will help you resolve issues if your information is compromised. MyIDCare services include:

- 12 months of credit monitoring
- $1,000,000 insurance reimbursement policy
- Exclusive educational materials
- Fully managed identity theft recovery services

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (888)710-8606 or going to https://ide.myidcare.com/*ChilisDataIncident*. MyIDCare experts are available Monday through Friday from 8 a.m. - 8 p.m. Eastern Time. Please note the deadline to enroll is August 15, 2018.

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information. We are committed to sharing additional information on this ongoing investigation with our Guests as we learn more and will continue to update this website.

FREQUENTLY ASKED QUESTIONS:

Updated May 18, 2018

Who is responsible for this attack?

We are working with third-party forensic experts and law enforcement in an effort to determine those responsible. At this time, the responsible party or parties have not been identified.

Who should I contact if I have questions?

If you have any further questions, or for information on the services that are being provided please feel free to contact our dedicated call center at (888)710-8606 or go to https://ide.myidcare.com/*ChilisDataIncident*. We will also be updating this website.

What are the risks of identity theft with the information that was compromised?

Being notified of this incident or having visited a Chili's between March – April 2018 does not mean that you are a victim of identity theft. However, we recommend that people enroll in the ID Experts membership and review the recommendations provided online at brinker.mediaroom.com/ChilisDataIncident and by ID Experts.

Is there anything I need to do to in response to the exposure of my personal information?

Once you are enrolled in the ID Experts membership, you may also take advantage of your rights to the free fraud alert services offered by the three major credit bureaus. Placing fraud alerts will provide your credit with additional protection. In addition, doing so will give you access to copies of each of your credit reports at no cost to you. Additionally, there are a number of steps you can take, many of which were detailed in the notification below and by ID Experts.

I received an email from Chili's regarding this incident. Is this legitimate?

We will endeavor to provide notification to potentially affected individuals via email (if Chili's has a valid email address), as well as responding to emails you may have initiated. However, Chili's has yet to initiate emails directly to Guests related to this incident and you should be aware of the possibility there may be scam email campaigns related to this incident. These scams, designed to capture personal information (known as "phishing") are designed to appear as if they are from us and the emails may include a "click here" link or ask you to "open" an attachment. These emails are NOT from Chili's.

- DO NOT click on any links in email.
- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
- DO NOT open any attachments that arrive with email.

I received a call from Chili's regarding this incident and the caller was asking for my information. Is this legitimate?

No. We are NOT initiating any calls to individuals regarding this incident and are not asking for any of your personal information over the phone.

How can I be sure that my personal data won't be subject to attack again in the future?

We take data privacy and security very seriously. We are working hard to ensure there is no further vulnerability to Chili's Guests. We are working with third-party forensic experts to conduct an extensive investigation and identify additional safeguards which may be utilized to secure data. As mentioned below, law enforcement has been notified of this incident and we will continue to fully cooperate.

Why does Chili's have my information?

It is necessary for us to have certain data from customers paying with a credit or debit card as part of the in-restaurant point of sale process.

Was my home address included with the information and am I in any danger of being robbed?

Your home address information was not included as a result of this incident.

What restaurants were affected?

We are working diligently with third-party forensic experts to conduct an extensive investigation to confirm the nature and scope of this incident. We are committed to sharing more information regarding this ongoing investigation with our Guests as we learn more.

How many individuals were affected by the data incident?

The investigation into this incident is ongoing and Chili's is working with third-party forensic experts to determine those who have been affected. We believe the data

incident was limited to between March – April 2018; however, we continue to assess the scope of the incident.

Should I call my bank and close my account? Should I cancel my credit cards?

You do not have to close your bank and credit card accounts. Be sure to monitor your bank and credit card statements for accuracy. If you notice any suspicious activity or you believe your information is being misused, please contact your bank.

Am I safe to use my credit or debit card at Chili's today?

We have no reason to believe you're putting yourself at risk by using your payment card today.

How can I stay up-to-date on this incident?

The most up-to-date information can be found on this website. We are committed to sharing additional information with our Guests as we learn more. We also have set up a dedicated call center and website for Guests to obtain information about the incident and to enroll in credit monitoring services. The number for the call center, again, is (888)710-8606, and the address for the website is **https://ide.myidcare.com/ChilisDataIncident.** We are working hard to make sure these resources have the most up-to-date information. You may also find contact information here.

What Can You Do?

If you used your payment card at a Chili's restaurant between March – April, 2018, it does not mean you were affected by this incident. However, out of an abundance of caution, in addition to taking advantage of the fraud resolution and credit monitoring services described above, we recommend that you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information.

1. Contact the nationwide credit-reporting agencies as soon as possible to:

- **Fraud Alert**. Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90-day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.
- **Security Freeze**. Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation

for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

Equifax Experian TransUnion
P.O. Box 740256 P.O. Box 9554 P.O. Box 2000
Atlanta, GA 30374 Allen, TX 75013 Chester, PA 19022
(800) 525-6285 (888) 397-3742 (800) 888-4213
www.equifax.com www.experian.com/consumer www.transunion.com

- **Free Credit Report**. Receive a free copy of your credit report by going to annualcreditreport.com.
- **Watch Bills, Statements and Mailing Lists**. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

2. Contact the Federal Trade Commission ("FTC") either by visiting ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

3. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general. Attorney General contact information may be found at: http://www.naag.org/naag/attorneys-general/whos-my-ag.php.
4. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.
5. *For Massachusetts Residents:* You have the right to obtain a police report relating to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

6. For *North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: ncdoj.com/.
7. *For Puerto Rico Residents*: The total number of affected individuals is currently unknown.
8. *For Rhode Island Residents*: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is currently unknown.
9. *For New Mexico Residents*: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf