The notice below supplements our original press release and notification of May 12, 2018 pursuant to state law. It includes additional information on steps those potentially impacted can take to protect themselves and minimize the possibility of misuse of their information, including details on enrolling in the identity theft protection services we are offering. Additional information can be found at ***brinker.mediaroom.com/ChilisDataIncident.***

Notice of Unauthorized Access or Acquisition to Chili's Grill & Bar Guest Data

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 are working diligently to address this issue and 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.

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 its payment-related systems for in-restaurant purchases at certain Chili's restaurants. 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 We Are 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 by the incident with with MyIDCare™, a free fraud resolution and credit monitoring service, 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. 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.
If you have questions or concerns please visit brinker.mediaroom.com/ChilisDataIncident. We also have set up a dedicated call center and ID Experts 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 also may find contact information for us at *http://brinker.com/contact/default.html.*

What You Can 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

4849-8089-3286, v. 1