Appendix

Chipotle recently concluded an investigation into unauthorized access to certain Chipotle employee email accounts. Upon discovering the incident, Chipotle immediately took steps to secure the accounts, a cyber security firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to the email accounts from January 19, 2020, through January 21, 2020. Chipotle believes that the account access occurred as part of an attempt to obtain money from Chipotle, not to access individuals' personal information. The investigation was not able to determine whether any emails or attachments were actually viewed during the period of access, however, so Chipotle reviewed the contents of the email accounts to determine the information they contained. Because one of the email accounts involved was used by an employee whose role involved access to workers' compensation and insurance claims, Chipotle conducted a document-by-document review. For individuals identified by this document review, Chipotle then had to use other resources to look for a mailing address, because many of the records in the email accounts did not contain addresses. Chipotle completed this process on September 30, 2020, and through it, Chipotle determined that information stored in the email accounts contained personal information of nineteen Maine residents, including the residents' names and Social Security numbers.

Beginning today, Chipotle is notifying the Maine residents via First-Class U.S. mail.[1] A copy of the notification letter is enclosed. Chipotle is offering a complimentary one-year membership in credit monitoring and identity theft protection services through Experian. Chipotle also has established a dedicated call center that individuals can call with questions about the incident or enrolling in credit monitoring.

To reduce the risk of a similar incident happening in the future, Chipotle has taken steps to re-educate employees about phishing emails and to further enhance its existing security measures.

[1] This report does not waive Chipotle's objection that Maine lacks personal jurisdiction over Chipotle regarding any claims related to this incident.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Chipotle Mexican Grill recognizes the importance of protecting information. We are writing to let you know of an incident that may have involved some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

We recently concluded an investigation into unauthorized access to certain Chipotle employee email accounts. Upon discovering the incident, we immediately took steps to secure the accounts, a cyber security firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to the email accounts from January 19, 2020, through January 21, 2020. The investigation was not able to determine whether any emails or attachments were actually viewed during that time. So, we reviewed the contents of the email accounts to determine the information they contained. Because one of the email accounts involved was used by an employee whose role involved access to workers' compensation and insurance claims, we conducted a document-by-document review. For individuals identified by this document review, we then had to use other resources to look for a mailing address, because many of the records in the email accounts did not contain addresses. We completed this process on September 30, 2020, and through it, we determined that an email or attachment in the accounts contained some of your information, including your name, <<Data Elements>>.

The investigation did not find any evidence that your information was actually viewed or accessed, and we believe that the account access occurred as part of an attempt to obtain money from Chipotle (not to access personal information). Nevertheless, we wanted to notify you of this incident and assure you that we take it very seriously. As a precaution, we have arranged for you to receive a complimentary one-year membership to Experian's® IdentityWorks℠ credit monitoring service. This product helps detect possible misuse of your information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks℠ is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks℠, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in this letter.

We regret that this occurred and apologize for any inconvenience. To help prevent another incident from occurring, we are re-educating employees about phishing emails and are taking steps to further enhance our existing security measures. If you have any questions, please call 855-914-4640, Monday through Friday, from 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

Chipotle Mexican Grill

Activate IdentityWorks Credit 3B Now in Three Easy Steps

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<Activation Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877.288.8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877.288.8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

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*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 and Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Health or Health Insurance Information

If your health or health insurance information was involved, we also recommend that you review any statements that you receive from your health insurer or healthcare providers. If you see services that you did not receive, please contact the insurer or provider immediately.

Additional Information for Residents of the Following States

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have 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.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.