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

December 29, 2020

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of certain Dickey's Barbecue Pit franchisee entities (collectively, "Dickey's"), to notify you of a security incident potentially involving Iowa residents. Dickey's corporate headquarters is located at 4514 Cole Avenue, Suite 1015, Dallas, TX 75205.

After receiving reports on October 13, 2020 that a payment card security incident may have occurred at certain Dickey's franchise restaurants, Dickey's immediately took action to identify and stop the unauthorized activity and began working with its franchisees to conduct a coordinated and thorough investigation. Forensic investigation firms were engaged. Dickey's also notified law enforcement and worked with the payment card networks to coordinate the investigation. Additionally, Dickey's provided a preliminary notice of the incident by posting a statement on the Dickey's corporate website on November 20, 2020, while the investigation was ongoing.

The investigation is nearly complete. The investigation found the installation of unauthorized code designed to find payment card data at certain franchise restaurant locations at different times over the general period of June 9, 2019, to November 24, 2020, for most locations and a few weeks later for a few locations. The unauthorized code was removed during the investigation.

The unauthorized code was only found at approximately fifty-five franchise locations. There are other franchise locations that were investigated, and the unauthorized code was not found. In Iowa, the investigation did not identify unauthorized code at any franchise locations.

In addition to these locations, there are other locations that updated their payment application server or system before the investigation began or that otherwise had a server or system that was no longer available for analysis, including one franchise location in Iowa. If the unauthorized code had been installed at those locations, the change or update ended the operation of the unauthorized code. Because the investigation identified some locations that still had their original payment application server or system and that had no evidence of the installation of unauthorized code, Dickey's does not believe that every location that changed or updated its payment application server or system would have had unauthorized code installed.

The code searched for data in the format of track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. That data may have included the cardholder's name, primary account number, expiration date, and internal verification value.

Although the investigation was largely able to identify the locations and time frames involved or potentially involved, it was not able to identify the specific individuals potentially involved. Consequently, Dickey's is providing substitute notice today by issuing a press release, posting a statement on the Dickey's corporate website, and emailing its Big Yellow Cup Rewards members who used a payment card at an involved or potentially involved franchise location during the time frame for that location. Copies of the press release, website statement, and email are attached. The website will contain a tool that customers can use to look up the franchise locations and time frames involved. In addition, Dickey's has established a dedicated, toll-free call center that customers can call to obtain more information regarding the incident.

Before this incident occurred, many Dickey's franchise restaurants had already implemented a new payment system that uses EMV payment technology. Dickey's has requested that any franchisee who has not yet done so complete that implementation. Dickey's also deployed an endpoint detection and response tool to devices in its corporate environment during the investigation and is developing plans to keep an EDR tool in place moving forward. Dickey's is exploring additional measures to further enhance payment card security and to help prevent a similar incident from occurring in the future.

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

Sincerely,

Craig A. Hoffman
Partner

Enclosures

FOR IMMEDIATE RELEASE

Dickey's Provides Update About Payment Card Incident

DALLAS, TX—December 29, 2020—Dickey's provided additional information today regarding the payment card security incident reported on November 20, 2020.

After receiving reports that a payment card security incident may have occurred at certain Dickey's franchises or locations, Dickey's immediately began working with our franchisees to conduct an investigation and forensic investigation firms were engaged. Dickey's also notified law enforcement and the payment card networks.

A thorough investigation is being conducted and is nearly complete. The investigation identified the installation of unauthorized code designed to find payment card data operated at certain franchised restaurant locations at different times over the general period of June 9, 2019 to November 24, 2020 for most locations and a few weeks later for a few locations.

The unauthorized code was only found at approximately 55 locations. In addition to these locations, there are other locations that updated their payment application server or system before the investigation began or that otherwise had a server or system that was no longer available for analysis. If the unauthorized code had been installed at those locations, the change or update ended the operation of the unauthorized code. There are other locations that were investigated, and the unauthorized code was not found.

The code searched for data in the format of track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. That data may have included the cardholder's name, primary account number, expiration date, and internal verification value.

A list of the Dickey's restaurants and corresponding time frames involved, which vary by location, and a list of the locations that had changes before the investigation started, is available at https://www.dickeys.com/payment-card-notification. This site also provides information about the incident and additional steps customers may take.

Dickey's quickly took measures to contain the incident, remove the unauthorized code, and is working to implement measures to further enhance payment card security. Nonetheless, it is always advisable for customers to 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 the bank that issued the card, 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.

For more information regarding this incident, customers may visit the website listed above or call the dedicated customer call center at (833) 971-3302, Monday through Friday, from 9:00 a.m. to 6:30 p.m., Eastern Time.

Subject: Notice of Data Security Incident

Dear Valued Rewards Member:

Dickey's values the relationship we have with our customers and understands the importance of protecting payment card information. We are writing to update you about an incident that may have involved your payment card information. This notice explains the incident, measures we have taken, and steps you can take in response and updates the information we posted on our website on November 20, 2020.

After receiving reports on October 13, 2020, that a payment card security incident may have occurred, Dickey's immediately began working with our franchisees to conduct an investigation and forensic investigation firms were engaged. Dickey's also notified law enforcement and the payment card networks.

A thorough investigation is being conducted and is nearly complete. The investigation identified the installation of unauthorized code designed to find payment card data operated at certain franchised restaurant locations at different times over the general period of June 9, 2019 to November 24, 2020 for most locations and a few weeks later for a few locations. The unauthorized code was removed during the investigation.

The unauthorized code was only found at approximately 55 locations. In addition to these locations, there are other locations that updated their payment application server or system before the investigation began or that otherwise had a server or system that was no longer available for analysis. If the unauthorized code had been installed at those locations, the change or update ended the operation of the unauthorized code. There are other locations that were investigated, and the unauthorized code was not found.

The code searched for data in the format of track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. That data may have included the cardholder's name, primary account number, expiration date, and internal verification value. A list of the Dickey's restaurants and corresponding time frames involved, which vary by location, and a list of the locations that had changes before the investigation started, is available here [will include hyperlink]. We are notifying you because our records indicate you used your payment card at one of these locations during the time frame the location was involved or potentially involved. Please continue to check this website as updated information about locations involved will be provided if it is received.

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 the bank that issued your card, 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.

Dickey's quickly took measures to address the incident, and we are working to implement measures to further enhance payment card security. We regret that this occurred and apologize for any inconvenience. If you have any questions, please call (833) 971-3302 from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday.

Sincerely,

Dickey's

[Will appear on http://www.dickeys.com/paymentcardnotification]

DICKEY'S PROVIDES UPDATE ON PAYMENT CARD SECURITY INCIDENT NOTIFICATION

December 29, 2020

Dickey's is providing an update to the notice it issued on November 20, 2020. Dickey's values the relationship we have with our customers and understands the importance of protecting payment card information. After receiving reports on October 13, 2020 that a payment card security incident may have occurred, Dickey's immediately began working with our franchisees to conduct an investigation and forensic investigation firms were engaged. Law enforcement and the payment card networks were notified.

A thorough investigation is being conducted and is nearly complete. The investigation found the installation of unauthorized code designed to find payment card data at certain franchised restaurant locations at different times over the general period of June 9, 2019 to November 24, 2020 for most locations and a few weeks later for a few locations. The unauthorized code was removed during the investigation.

The unauthorized code was only found at approximately 55 locations. In addition to these locations, there are other locations that updated their payment application server or system before the investigation began or that otherwise had a server or system that was no longer available for analysis. If the unauthorized code had been installed at those locations, the change or update ended the operation of the unauthorized code. There are other locations that were investigated, and the unauthorized code was not found.

The code searched for data in the format of track data read from the magnetic stripe of a payment card as it was being routed through a restaurant's server. That data may have included the cardholder's name, primary account number, expiration date, and internal verification value. A list of the Dickey's restaurants and corresponding time frames involved, which vary by location, and a list of the locations that had changes before the investigation started, is available in the Locations tab. Please continue to check this website as updated information about locations involved will be provided if it is received.

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 the bank that issued your card, 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.

We quickly took measures to address the incident, and we are working to implement measures to further enhance payment card security. We regret that this occurred and apologize for any inconvenience. If you have any questions, please call (833) 971-3302 from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday.

ADDITONAL STEPS YOU CAN TAKE

We are required by law to provide you with the following information. We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your payment card statements for any unauthorized activity. Although we have no reason to believe that your consumer credit profile is at risk, 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 review them for accuracy. 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

If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of 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 below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 (1) 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

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 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

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written

request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

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). Here is a summary of your major rights under FCRA. 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.