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]

NOTICE OF DATA BREACH

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.

What Happened?

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.

What Information Was Involved?

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 on the Locations tab. Please continue to check this website as updated information about locations involved will be provided if it is received.

What We Are Doing.

We quickly took measures to address the incident, and we are working to implement measures to further enhance payment card security.

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 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.

For More Information:

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 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.