Payment Card Incident Notice

NOTICE OF DATA BREACH

Landry's, Inc. ("Landry's") takes the security of payment card data very seriously. Years ago (beginning in 2016), Landry's installed a payment processing solution that uses end-to-end encryption technology at all Landry's owned locations.

We are notifying customers of an incident that we recently identified and addressed involving payment cards that, in rare circumstances, appear to have been mistakenly swiped by waitstaff on devices used to enter kitchen and bar orders, which are different devices than the point-of-sale terminals used for payment processing. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened?

Landry's recently detected unauthorized access to the network that supports our payment processing systems for restaurants and food and beverage outlets. We immediately launched an investigation, and a leading cybersecurity firm was engaged to assist. Although the investigation identified the operation of malware designed to access payment card data from cards used in person on systems at our restaurants and food and beverage outlets, the end-to-end encryption technology on point-of-sale terminals, which makes card data unreadable, was working as designed and prevented the malware from accessing payment card data when cards were used on these encryption devices. Besides the encryption devices used to process payment cards, our restaurants and food and beverage outlets also have order-entry systems with a card reader attached for waitstaff to enter kitchen and bar orders and to swipe Landry's Select Club reward cards. In rare circumstances, it appears waitstaff may have mistakenly swiped payment cards on the order-entry systems. The payment cards potentially involved in this incident are the cards mistakenly swiped on the order-entry systems. Landry's Select Club rewards cards were not involved.

What Information Was Involved?

The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card after it was swiped on the order-entry systems. In some instances, the malware only identified the part of the magnetic stripe that contained payment card information without the cardholder name. The general timeframe when data from cards mistakenly swiped on the order-entry systems may have been accessed is March 13, 2019 to October 17, 2019. At a small number of locations, access may have occurred as early as January 18, 2019. A full list of Landry's owned restaurants and food and beverage outlets involved is available here.

What We Are Doing.

During the investigation, we removed the malware and implemented enhanced security measures, and we are providing additional training to waitstaff. In addition, we continue to support law enforcement's investigation.

What You Can Do.

It is always advisable for individuals to closely monitor their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to the financial institution 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. Please see the section that follows this notice for additional steps you may take.

For More Information.

If you have any questions, please call 833-991-1538 from 8:00 a.m. to 8:00 p.m. CT, Monday through Friday. (The call center will be closed on New Year's Day).

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 over the next 12 to 24 months. 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