DATA BREACH ALERT

Inside the Landry's Inc. Payment Data Breach

Rippleshot

WHAT HAPPENED

+600 Establishments

Landry's Inc., a Houston-based company owns and operates more than 600 restaurants, hotels, casinos and entertainment destinations.

7 Months

The data breach likely impacted cards swiped between March 13 and Oct. 17, 2019.

CP-Based Breach

The breach is believed to have occurred from servers swiping customers' credit cards in machines intended to submit food and drink orders to the kitchen and bar, and not POS terminals.

2.5 Months

The breach was announced roughly 2.5 months after the impacted period ended.

WHAT YOU NEED TO KNOW

- The breach occurred because waitstaff mistakenly swiped payment cards on the order-entry systems instead of POS terminals.
- The malware installed on Landry's' payment processing system servers was used to exfiltrate customers' card numbers, expiration dates and internal verification codes.
- Only cards swiped on the order placement kiosks instead of the POS system were impacted by the breach.

Questions? Reach out to Customer Success Manager Jesse Sherwood at jesse@rippleshot.com

DATA BREACH ALERT

Inside the Landry's Inc. Payment Data Breach

Rippleshot

What You Can Do About the Breach

- ❏ Manually identify the list of cards that may have been compromised. Using this list of compromised Landry's brands.
- ❏ Determine which cards to re-issue, which cards to write decision rules against, and which cards to monitor based on mitigation strategies.
- ❏ Continue monitoring the velocity of fraud from compromised cards to adjust strategies.
- ❏ Be on the lookout for additional news and development on this breach.
- ❏ Monitor potential fraud In real-time to get ahead of incidents before they spread.
- ❏ Track the fallout of the breach to identify potential Incidents from compromised data.

Questions? Reach out to Customer Success Manager Jesse Sherwood at jesse@rippleshot.com

DATA BREACH ALERT

Inside the Landry's Inc. Payment Data Breach

Rippleshot

What Rippleshot Sonar Users Can Do

On the Fraud Forecast Page*:

- ❑ Continue reissuing based on the recommendations made on the Fraud Forecast page.
- ❑ If you are concerned about additional risk due to the scope of the breach, consider reissuing cards with high orange scores to prevent additional fraud.

On the CPP Page:

- ❑ Search for compromised locations using the "Search by Store Name" feature on the CPP List page.

On the Alerts Page:

- ❑ A list of cards from your portfolio that visited an impacted Landry's brand location during the exposure window will be uploaded to your Alerts page on Monday, January 13, 2020.

*A Fraud Forecast Score™ assesses each card's total exposure risk to determine the probability that it will become fraudulent in the next 90 days.