DATA BREACH ALERT

# Inside the Dickey's Barbecue Pit Data Breach

Rippleshot

## WHAT HAPPENED

### +3 Million Cards

Since about mid-2019, credit card data from roughly 3 million payment cards were stolen.

### ~16 Months of Data Exposed

Reports indicate credit card data was exposed between May 2019-Sept. 2020

### 156 Locations

The BBQ franchise operates 156 locations across 30 states, but not all locations are believed to have been compromised.

### Cards from 35 U.S. States

Reports indicate the +3 million credit cards stem from 35 states, spanning a time frame of over a year.

## WHAT YOU NEED TO KNOW

- It's believed payment systems were compromised by card-stealing malware, with the highest exposure believed to be in California and Arizona.
- Gemini Advisory, a cybersecurity firm, found the stolen cards on a Joker's Stash, a hacker's forum for stolen payment data. The data was traced back to the compromised point of purchase (CPP) — Dickey's Barbecue Pit.
- It's believed the transactions were made with magstripe cards.
- The breach could have occurred on a single central processor, according to Gemini.
- Joker's Stash is reportedly posting the batch of +3 million card records as "BLAZINGSUN." The hacker forum has also advertized that the cards have "valid rates" between 90-100%.
- The company released a statement saying: "We are currently focused on determining the locations affected and time frames involved."

DATA BREACH ALERT

# Inside the Dickey's Barbecue Pit Data Breach

Rippleshot

## What Financial Institutions Can Do About the Breach

- ❑ Manually identify the list of cards that may have been compromised.
- ❑ 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.

## For Rippleshot Sonar Clients:

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 Dickey's Barbeque Pit locations using the "Search by Store Name" feature on the CPP List page.

# Inside the Dickey's Barbecue Pit Data Breach

Rippleshot

## Rippleshot's Take: The Potential Fraud Fallout

The hacker's forum reportedly announced the a majority of the cards are still active and in good standing, which indicates that many financial institutions, along with potentially impacted cardholders, may be unaware of the impact. Financial institutions should be taking measures to proactively prevent any future fraudulent activity on potentially impacted cards.

Gemini Advisory reports the payment transactions were made using magstripe cards, which could mean that some of the POS payments may not have been chip and pin compliant or the transactions was swiped instead of inserted. Dickey's is a franchise, and unlike a chain, allows each individual location to choose their own point-of-sale payment processing device. It's believed that the breach was linked to a single central processor that was used by over a quarter of all Dickey's locations.

- These point-of-sale, malware breaches underscore the importance of relying on fraud tools that use predictive technology to proactively stop compromised card fraud originating from breached POS devices.

- Knowing which merchants are risky, identifying them early, and having a mechanism to write more effective rules on those merchants, is particularly helpful for financial institutions trying to determine where their greatest fraud risks exist to lower fraud costs.