CASE STUDY

# Breach Compromises Credit Card Data of More Than 13,000 Restaurant Customers

**INDUSTRY**
Retail

**EVENT TYPE**
Data Breach

**REVENUE**
$50–100M

**EMPLOYEE COUNT**
251–1,000

**LOCATION**
Texas

**KEY COVERAGE**
Breach Response

After receiving an unexpected phone call, a restaurant group learned it was experiencing an ongoing cyber attack. But it wasn't a threat actor on the other end of the line — it was the Federal Bureau of Investigation.

The FBI notified the business that data from four of its servers had been compromised: three corporate servers and one restaurant server containing customer credit card information. Considering it processes more than $8 million in credit card transactions annually, the restaurant group immediately notified Coalition in hopes of minimizing the damage and exposure.

Within 48 hours, incident responders utilized script collectors to identify how the threat actor was accessing the servers and what data was impacted. Coalition's breach response partner ejected the threat actor and reclaimed control of the network. Unfortunately, even with quick action, the breach compromised customers' credit card data.

Our investigation determined the incident began with a simple phishing email. Once the threat actor entered the network, they elevated their own credentials to access other accounts. With unfettered access, the threat actor was able to compromise credit card data for more than 13,000 individuals. The data breach eventually resulted in a class-action lawsuit, but one key coverage reduced the business' cost to a fraction of the overall amount. Breach Response covered the costs of notifying customers about the data breach, as well as costs related to litigations, depositions, and negotiations during the lawsuit. In the end, the restaurant group only paid $21,000 out of pocket, while its policy covered the rest of the $3 million claim.

Network segregation can limit the impact of intrusion by making it significantly more difficult for a threat actor to locate and gain access to sensitive information.

## Lesson Learned: Segregate Networks and Require Multi-Factor Authentication

Without the right security controls in place, one errant click on a phishing email can quickly transform into a multimillion dollar data breach. Similarly, enforcing multi-factor authentication for administrative access to internal networks can make initial entry significantly more difficult.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization's cyber risk. To learn more, visit coalitioninc.com.

[1] *The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.*



Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc., ("CIS") a licensed insurance producer with its principal place of business in San Francisco, CA (Cal. license #0L76155), acting on behalf of a number of unaffiliated insurance companies. Insurance products offered through CIS may not be available in all states. Complete license information is available here.