Issued 4/18/17

Shoney's Hit By Apparent Credit Card Breach

Multiple sources in the financial industry say they've traced a pattern of fraud on customer cards indicating that the latest victim of a credit card breach may be **Shoney's**, a 70-year-old restaurant chain that operates primarily in the southern United States.

Shoney's did not respond to multiple requests for comment left with the company and its outside public relations firm over the past two weeks. Based in Nashville, Tenn., the privately-held restaurant chain includes approximately 150 company-owned and franchised locations in 17 states from Maryland to Florida in the east, and from Missouri to Texas in the West — with the northernmost location being in Ohio, according to the company's Wikipedia page.

Sources in the financial industry say they've received confidential alerts from the credit card associations about suspected breaches at dozens of those locations, although it remains unclear whether the problem is limited to those locations or if it extends company-wide. Those same sources say the affected locations were thought to have been breached between December 2016 and early March 2017.
It's also unclear whether the apparent breach affects corporate-owned or franchised stores — or both. In last year's card breach involving hundreds of Wendy's restaurants, only franchised locations were thought to have

been impacted. In the case of the intrusion at Arby’s, on the other hand, only corporate stores were affected.

The vast majority of the breaches involving restaurant and hospitality chains over the past few years have been tied to point-of-sale devices that were remotely hacked and seeded with card-stealing malicious software. Once the attackers have their malware loaded onto the point-of-sale devices, they can remotely capture data from each card swiped at that cash register. Thieves can then sell the data to crooks who specialize in encoding the stolen data onto any card with a magnetic stripe, and using the cards to buy gift cards and high-priced goods from big-box stores like Target and Best Buy.

Many retailers are now moving to install card readers that can handle transactions from more secure chip-based credit and debit cards, which are far more expensive for thieves to clone. Malware that makes it onto point-of-sale devices capable of processing chip card transactions can still intercept data from a customer’s chip-enabled card, but that information cannot later be used to create a cloned physical copy of the card.