



Issued 5/31/17

Chipotle: Hackers Did Us In

Fast-food chain Chipotle says hackers infected its point of sale terminals to gain access to card data from stores in 47 states and Washington, DC. The self-described "Mexican Grill" says that the malware was active earlier this year from March 24 to April 18, when it was detected, triggering the company to issue an alert [<https://www.chipotle.com/security>]. "The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS device," Chipotle said in its latest summary of the incident. "There is no indication that other customer information was affected."

That last sentence is a bit puzzling, as a fraudster who has payment card numbers, dates, and security codes would have little need for any other info. Chipotle says that while the compromised stores are located in every state save Alaska, Hawaii and South Dakota, not every location was breached. Chipotle's disclosure page includes a section to check individual stores.

Chipotle recommends that anyone who paid with a card at one of the compromised stores keep a close eye on bank statements and consider

having an alert placed to their credit file to catch possible fraud. The fast food chain is far from alone in falling victim to this type of scam.

Hackers have targeted the POS terminals of dozens of retailers, restaurants, and hotel chains with malware payloads that collect and transmit the payment card data of customers, often resulting in the theft of thousands of card numbers.