Hotels in 10 states and DC may have been hit by hackers

15 August 2016

This Feb. 1, 2010, file photo, shows The Westin Philadelphia hotel in Philadelphia. Hyatt, Sheraton, Marriott and Westin hotels in 10 states and the District of Columbia may have been targeted by hackers for months. Hotel operator HEI Hotels & Resorts, said Monday, Aug. 15, 2016, that malware put into place in at least 20 locations may have collected names, card account numbers, card expiration dates and verification codes. (AP Photo/Matt Rourke, File)

An undisclosed number of people who used credit cards at 20 Hyatt, Sheraton, Marriott, Westin and other hotels in 10 states and the District of Columbia may have had their cards compromised as a result of hack of the hotels' payment system.

HEI Hotels & Resorts, which operates just under 60 hotels and resorts under a variety of brands, said that after being notified by its credit card processor of a potential breach, it conducted an internal investigation that found malware on its payment processing systems at the 20 properties . The malware was designed to capture debit and credit card information such as names, card account numbers, card expiration dates and verification codes, as it flowed through the systems.

According to the Norwalk, Connecticut company, the hack potentially affected cards used at point of sale terminals, such as those at the hotels' restaurants and stores, between December 2015 and June 2016. Systems at a few of the affected locations were found to have been infected with the malware as early as March 2015.

Retailers and other companies that deal with large numbers of credit cards have become popular targets for hackers looking to make a quick buck by collecting and selling the information on the internet in bulk. A couple years ago, massive breaches involving the thefts of millions of card numbers at retailers such as Target, Home Depot and Neiman Marcus grabbed headlines. And in in Target's case, its breach ultimate led to the departure of its CEO.

Among the hotel chains, Hilton Worldwide, Trump Hotel Collection and Starwood Hotels & Resorts have all confirmed POS system breaches within the past year or so. More recently, fast food chains Wendy's and Cici's Pizza acknowledged breaches of their systems in the past few months.

Yet the black market value of credit card numbers has tumbled, largely as a result of better fraud prevention technology that allows banks to spot and stop bad transactions faster. As a result, many thieves have moved on to target more lucrative information such as health care data.

HEI said in its notice to consumers that once it found out about the breach of its systems it transitioned payment card processing to a stand-alone system that's completely separate from the rest of its network. It disabled the malware and is in the process of reconfiguring various components of its network and payment systems to make them more secure.

The company said in its statement that it's continuing to cooperate with the law enforcement investigation and coordinating with banks and

payment card companies. It added that the breach has been contained and customers can safely use cards at all of its properties. HEI officials didn't immediately return a call seeking additional comment.

HEI advised anyone who used a card at the hotels in question during the given time frame to review their account statements and look for discrepancies or unusual activity, both over the past several months and going forward. Customers who notice anything out of place should contact their card issuer.

As with any breach, consumers are not liable for fraudulent charges on their credit cards. And once a breach such as this is disclosed, as a precaution, banks will often automatically issue new cards to any of their customers that potentially could be affected.