Clean reviews preceded Target's data breach, and others

April 2 2014

Trustwave Holdings gave Target Corp. the green light on payment card security last September, just weeks before malware installed on the retailer's networks began sucking up customer information in a mega data heist.

It's a rough position for a company that built its brand reputation selling payment compliance and security to some of the country's largest corporations.

But it's not the first time Trustwave's been there.

The Chicago-based company has given a clean review to at least six other companies in recent years that subsequently suffered breaches, one of which rivals Target's in size. They include some of the nation's largest payment processors, such as Heartland Payments Systems, which suffered a monster breach in 2008 about two months after Trustwave deemed it compliant with payment card industry, or PCI, security standards.

A giant in the small world of PCI compliance, Trustwave has performed thousands of audits for retailers and payment processors, most of which haven't preceded any known problems.

But critics, including one former Trustwave employee, see a pattern. Some say the incidents illustrate the payment industry's flawed system for policing the safety of consumer information.

"Trustwave is the largest player in a PCI auditing or assessment system that is rife with conflicts of interest and hence produces less-than-optimal results," said Avivah Litan, a financial services security analyst at Connecticut-based Gartner Research.

Litan pointed to Trustwave's record of assessments at companies that have been breached, as well as arrangements with top payment processors who use Trustwave as a preferred vendor to provide security services for merchants. Its relationship with Chase Paymentech is so close, for instance, that it offers merchants Trustwave's risk assessments for free.

Trustwave declined to comment for this report. So did Target.

Privately held Trustwave, with more than 600 employees, is a central and global player in PCI compliance, an assessor with deep roots in the payment industry's body of checks and rules for protecting credit and debit card information in the United States. The standards are set by the PCI Security Standards Council, an industry group in Wakefield, Mass., created and run by the world's five major card brands - Visa, Discover, MasterCard, American Express and JCB (Japan) - nearly eight years ago. Enforcement lies with the individual card networks.

Today's Trustwave grew out of a 2005 merger between Chicago information security company Ambiron and Annapolis, Md.-based Trustwave. It continued on a path of rapid growth, acquiring a slew of data loss prevention companies - at least 10 since 2008. In the spring of 2011, when filing to go public, Trustwave reported annual revenue of $111 million. It shelved the IPO that summer when markets seesawed.

Although it's a dominant player in PCI compliance, it provides a range of other services, such as threat assessments and managing security services for companies that want to outsource it. The company website is

full of case studies showcasing a range of satisfied customers.

Minneapolis-based Target Corp. started working with Trustwave several years ago. A former Target information technology employee said that Trustwave essentially taught Target how to be PCI-compliant and that it mostly interacted with the Target Information Protection team, called TIP.

"The TIP team had a high level of confidence in Trustwave," the person said.

Target has already said in government filings that it expects to be found noncompliant, despite being found compliant at the end of September, because companies that suffer data security breaches are almost always found to be out of compliance with PCI standards.

Just how many companies suffered a breach shortly after a Trustwave assessment of compliance can't be determined because the lists of merchants and the vendors who do their annual compliance checkups are closely guarded secrets held by Visa and MasterCard.

What is available on the Internet is Visa's separate list of the companies that store or process payment data for merchants and the vendors who do their compliance checkups. A cross-check of the 2011-2013 lists with a database of breaches maintained by the Open Security Foundation indicates a few were breached not long after a Trustwave compliance assessment.

Most of the companies either did not return phone calls or declined to comment.

One, Hosting.com, a Denver-based cloud service provider that operates multiple data centers, got its report on compliance from Trustwave in

June 2012. That October, cyberthieves hacked a dedicated server housing information for several medical groups, exposing the information of more than 15,000 people, many in Massachusetts.

Several knowledgeable industry veterans interviewed for this report said it's an open secret in the PCI compliance world that Trustwave assessments are lax. The company pushes for speed, not accuracy, in its compliance reports, they said, selling cheap audits with an eye to selling clients more lucrative security services.

A former Trustwave assessor, who asked not to be named because he continues to work in PCI compliance, said he routinely saw Trustwave compliance audits with errors. He said he was doing about one assessment every week, and described the quality control issues as so severe that he left.

He said he thinks the company's incentive structure fueled the problem. "The more assessments you could cram into a quarter, the bigger and juicer your bonus was going to be," he said.

An employee with a base salary of $100,000, for instance, could generate $30,000 to $50,000 more a year by churning out as many assessment reports as possible, he said.

Heartland Payments Systems, one of the country's largest payment processors, experienced some of those issues firsthand. Starting around June 2008, thieves hauled off nearly 130 million records from the Princeton, N.J.-based company in a cyberheist that remains one of the country's largest recorded data thefts. Trustwave had given Heartland a clean bill of health the previous April.

The compliance report was full of "glaring errors," Heartland Chairman and Chief Executive Bob Carr said in an interview, noting as an example

that Trustwave assessors had overlooked one of Heartland's data centers altogether.

"They didn't even know we had a data center and they were certifying it was compliant. Seriously? Really?" Carr said.

Carr said he didn't think the PCI assessment could have thwarted the breach even if it were done right.

In July 2008 Trustwave gave a passing grade to Atlanta-based card processor RBS WorldPay (now WorldPay US Inc.). About three months later, RBS was hacked. An international crime gang took just 12 hours to rack up more than 15,000 fraudulent transactions at ATMs around the world, draining away more than $9.4 million.

Doug Sandberg, WorldPay's general counsel, said Trustwave's assessment "might have been a little less than stellar ... and frankly we didn't use them again after our situation."

Hacked companies typically have little to fall back on. Most companies doing PCI assessments have contracts restricting the liability of the assessors in the event something goes wrong, said David Navetta, a partner in Information Law Group's Denver office who concentrates on data security breaches.

South Carolina taxpayer Amber Strautins sued Trustwave in 2012 in a putative class action after thugs hacked the computer systems of the South Carolina Department of Revenue, exposing the Social Security numbers of about 3.6 million people. The Revenue Department had contracted with Trustwave for security services. A federal judge in Illinois recently dismissed Strautins' case, saying she didn't demonstrate that her information had actually been stolen and compromised.

The PCI Security Standards Council would not make an executive available to discuss Trustwave. A spokesman said it can't speculate on the quality of assessments, and doesn't disclose whether complaints about vendors have been filed or whether vendors have in the past been sanctioned by being put in remediation for improvement. Trustwave is not on the council's current remediation list.

"From the council's perspective what these recent incidents indicate is the need for a strong focus for organizations on security payment card data on a daily basis," said council spokesman Mark Meissner. "Compliance does not equal security."

"PCI Standards are the floor, not the ceiling."

Neither Visa Inc. nor MasterCard Inc. would comment for this report.

Julie Conroy, a payment security analyst at Boston-based Aite Group, called the disconnect between PCI compliance and breaches "a fundamental opportunity for improvement."

"I'm not sure what the path forward is," Conroy said, "because a comprehensive audit of complex organizations like Target would be prohibitive from both a time and cost perspective."