SecureTrust™
a Trustwave® division

CASE STUDY

A Global Retailer Alleviated its PCI DSS Headache

Despite the continued growth of e-commerce sales—which grew to more than $3.5 trillion in 2019—bricks-and-mortar transactions still account for the majority of global retail sales. As such, today's merchants must offer multiple payment options for both online and in-person transactions, from debit cards and credit cards to gift cards and mobile payments.

While shoppers love the convenience of toggling between web and in-person payments, retailers struggle to secure payments, prevent breaches and meet the stringent PCI DSS compliance requirements that affect not just online card transactions, but also every point-of-sale machine in bricks-and-mortar stores. Because these requirements are regularly updated, maintaining compliance across large, complex organizations is expensive and time-consuming.

Client Spotlight:

A Level 1 merchant as defined by VISA and MasterCard, this retailer completes more than 6 million transactions across e-commerce, mail order and telephone, and thousands of retail stores around the globe. Because of the retailer's size and the number of payment cards it accesses, PCI DSS holds it to the strictest standards, requiring the retailer to attain an annual report on compliance from a qualified security assessor after an onsite audit, as well as quarterly network scans.

"PCI compliance is cumbersome due to constant evolution of both regulatory requirements and business infrastructure. By conducting quarterly business reviews with SecureTrust, working with experienced QSAs who understand local regulatory requirements, and using Compliance Manager, the client is able to stay ahead of these changes to ensure a constant state of compliance."

— Alexander Norell, Director of Global Risk and Compliance Services, SecureTrust

The Challenge:

A global retailer with a significant e-commerce presence and thousands of stores was struggling to track PCI DSS compliance and monitor evidence across more than a dozen countries. Its previous qualified security assessor (QSA) failed to deliver compliance expertise and pushed to include the whole company in its scope—a misstep that increased complexity, effort and costs.

Because the retailer's PCI strategy had no central compliance approach, each country followed different compliance methodologies based on assumptions rather than local expertise. Worse still, the merchant was bogged down by work that had to be constantly scrutinized and re-done, leading to steadily increasing internal costs and an inability to effectively plan and meet its budget.

The Solution:

SecureTrust created a straightforward approach based on a global compliance framework that could be applied across separate geographic regions while helping the merchant maximize cost efficiency. To fix the previous QSA's scoping error, SecureTrust performed a network segmentation to separate the retailer's cardholder data from the rest of its environment, thereby reducing the project's scope, effort and costs.

After identifying the merchant's compliance awareness as an area of weakness, SecureTrust created common policies and procedures that were rolled out via a new global training program. Its proprietary Compliance Manager portal—a real-time tool that proves clear, actionable information in a single, consolidated view—helped streamline and organize evidence gathering, making it easier to track progress while increasing accountability. What's more, SecureTrust introduced a subscription-based model combined with a dedicated partner approach to deliver a predictable monthly fee and lower total cost. Once this global framework was in place, SecureTrust's local QSAs offered expert guidance on regional regulations and variations in payment processes, improving compliance without increasing complexity.

Industry Threat:

Whether they're placing skimmers on point-of-sale terminals in stores, installing malware on brands' websites or taking advantage of site misconfigurations to steal confidential customer payment information, thieves have always held retailers in their crosshairs. From the breach of a major retailer that began in 2005 and lasted 18 months before it was detected, compromising the payment card details of 94 million customers, to the 2017 theft of card data belonging to more than 5 million shoppers, no merchant is immune. More recently, the COVID-19 pandemic has created additional security challenges as retailers rely more heavily on their online business.

These cyberattacks have the potential to seriously harm retailers, who may be faced with hefty regulatory fines and legal fees, as well as reputational damage and general financial losses. According to a 2020 report from research firm the Ponemon Institute, the global average cost of a data breach is $3.86 million, while one that occurs in the U.S. averages $8.64 million. That's a price no retailer, battered as they have been by the pandemic and its economic effect, wants to pay.

"By properly scoping the business, segmenting the network and implementing repeatable processes, the client now meets global and national regulatory requirements without encroaching on business innovation or blowing their budget."

— Alexander Norell, Director of Global Risk and Compliance Services, SecureTrust

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com