SecureTrust™
a Trustwave® division

CASE STUDY

Keeping Pace with the Electronic Payment Explosion

As customer expectations around convenience continue to increase, failing to optimize electronic and online payments can have serious consequences: According to the 2019 American Express Digital Payments Survey, 62 percent of customers said they had left a store when it took too long to pay, and 85 percent said they had abandoned a digital shopping cart for the same reason.

Accordingly, merchants are increasingly calling on payment service providers (PSP) to manage and streamline their electronic transactions. Rapidly growing PSPs are tasked with managing multiple payment forms for a wide swath of merchants across many industries and, increasingly, many countries. Managing PCI compliance across this landscape will only become more dizzyingly complex, as global non-cash payments are expected to increase at a compound annual rate of 14 percent through 2022, according to the 2019 World Payment Report.

Client Spotlight:

One of SecureTrust's largest and longest established clients, this PSP now works with SecureTrust on behalf of thousands of customers across more than a dozen countries.

"SecureTrust's framework allows us to deliver the same high-quality assessment across the globe. The team heading up compliance receives a weekly status update that summarizes all projects—and the client knows that when an issue arises, they can pick up the phone and get immediate solutions."

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

"The transparency created by using Compliance Manager allows the client to know where they are in the compliance process and where they need to go."

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

The Challenge:

A leading global service provider and manufacturer of point-of-service and payment software, works with thousands of global customers that each handle huge quantities of online and offline transactions. The PSP has completed several acquisitions in recent years and is poised for continued growth—but its rapid expansion has created an increasingly unmanageable assortment of entities using different technology platforms and different processes.

As the acquisitions made the company's compliance needs ever more complicated, it was evident it was difficult for the internal teams to have an on-demand overview of all assessments. The PSP was also implementing a multitude of security controls over multiple environments making it costly to keep up with the PCI DSS requirements. With few resources and many moving parts, the PSP had resorted to simply duplicating compliance budgets across different entities rather than unifying them under one budget to gain economies of scale.

The Solution:

SecureTrust helped the company create a global master services agreement for all its entities, adding local qualified security assessors (QSAs) in each region. SecureTrust guided the company on how to manage the assessments in a way that enabled a global service environment to support multiple locations making the approach to security and compliance very efficient. By implementing Compliance Manager—a proprietary real-time tool that provides clear, actionable information in a single, consolidated view—as well as a subscription-based pricing model, the PSP was able to create a highly efficient one-stop-shop approach to compliance, easily managing and monitoring all ongoing assessments and weekly status updates while improving cost efficiency and budget control.

SecureTrust also streamlined the company's technology platforms, processes and procedures so the PSP was able to manage enterprise-wide PCI compliance assessments with centralized, single points of contact and local QSAs that saved time and reduced risk. A subscription-based pricing model further increased efficiency and lowered costs. Moreover, the centralized MSA eased the company's growth pains, making it easier to integrate new entities.

SecureTrust's unified framework allowed the business to implement not only PCI DSS validation, but also validation for PA DSS, PCI PIN and PCI 3DS. It also added a suite of technology solutions to help the PSP meet specific security controls and better understand its risk environment. This increased security maturity profile has allowed the PSP to meet its PCI requirements around the globe with a decreased burden on its internal resources, while creating an ongoing compliance cycle that allows it to look ahead to the next round of requirement changes coming with PCI DSS 4.0.

Industry Threat:

Point-of-service data breaches—often executed by installing malware in the POS software—not only cripple the systems of retailers, restaurants and other merchants, but also risk ruining their reputations and costing them huge sums of money.

In 2019 alone, a major food delivery service, convenience store chain, chain restaurant, hospitality company, and more reported POS malware or other unauthorized access of their payment systems' networks, potentially affecting many millions of customers. What's worse, the average time it took a company to discover a breach increased to 280 days in 2020, according to global security research—and the average cost per compromised customer record was $162. For companies with millions of impacted customers, the price tag could run into the hundreds of millions of dollars.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com