SecureTrust™
a Trustwave® division

CASE STUDY

Fueling Fraud Protection

The number of businesses that accept credit cards and other forms of electronic payment has skyrocketed in the past decade. As the complexity of merchants' payment systems increased, payment service providers, or PSPs, have proliferated to help. PSPs work with the acquiring bank to manage the electronic payment process, beginning when a customer inputs their credit card details and ending when the money appears in the merchant's bank account.

Because PSPs process, store and/or transmit cardholder data, they must comply with PCI DSS. However, even when a merchant relies on a PCI-compliant provider to process its payment card transactions, the merchant itself must also meet PCI DSS standards.

Client Spotlight:

This payment service provider works with more than 400 petrol station and convenience store clients in the United Kingdom, each of which run a high volume of cardholder-present transactions. Because petrol stations and convenience stores are common targets for credit card fraud, they are eager for help in establishing best practices, including segmenting their networks to protect data, and the process of reaching and maintaining PCI compliance.

"Thanks to our deep expertise in complex programmes and large volume of assessments completed annually, SecureTrust was able to deliver three ROCs in less than four months, as well as a PCI-compliant service year on year."

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

The Challenge:

A PSP based in the United Kingdom had worked with SecureTrust on its own PCI compliance for more than a decade. The provider worked with hundreds of petrol station and convenience store clients that outsourced an increasing amount of their payment-related needs; accordingly, the PSP wanted to offer a ready solution that would minimise the efforts its clients, and its own business need to expend to reach PCI compliance. It struggled, however, to define scope for its clients across multiple assessments, including managed service systems, payment processors and point-to-point encryption. What's more, the PSP needed to submit multiple reports on compliance (ROCs) for itself and its clients in fewer than six months.

The Solution:

SecureTrust worked with the PSP and its clients to determine the best approach to bring the petrol stations and convenience stores into a Compliance framework, including efficiently managing the scope across a complex set of processes. Then SecureTrust's team of qualified security assessors (QSAs) stepped in and introduced an easy five-step process to guide the PSP and clients through the process of writing the ROCs. Action items for each step were embedded in SecureTrust's proprietary Compliance Manager software platform—a real-time tool that proves clear, actionable information in a single, consolidated view—to ensure effective tracking and a faster compliance process.

Using Compliance Manager also enabled the PSP to store the petrol station's data in a secure, cloud-based environment for at least three years, as required by PCI mandates, as well as to manage its own compliance budget. And because SecureTrust has the most experienced QSAs of any security compliance firm, it was particularly equipped to handle a complex compliance program of this nature—as evidenced by the fact that it delivered three ROCs in less than four months for the business' own services, dedicated managed services for the retail client and shared services provision. By partnering with SecureTrust, the PSP is able to help a large number of clients maintain PCI compliance and peace of mind.

Industry Threat:

Cyberthieves have long zeroed in on self-service petrol pumps, lured by the high number of daily payment transactions and the historically lax security. Years ago, they applied physical skimmers to the credit card pad to glean card details; more recently, they've begun installing malware in the petrol stations' corporate networks, according to a 2019 report by Visa. Once the hackers gain entry to the networks, they're able to move through connected point-of-sale machines to steal credit and debit card data.

Today, card terminal fraud remains commonplace. In fact, attacks increased 35 percent in 2019, according to the European Association for Secure Transactions, and total losses were up slightly, to €249 million.

"SecureTrust quickly established a framework with the payment service provider so that by the time its clients signed a contract, we were prepared and ready to roll."

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

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com