SecureTrust™
a Trustwave® division

CASE STUDY

Preventing payment fraud in a post-pandemic world

The COVID-19 pandemic has significantly accelerated the shift to digital payments and the adoption of a cashless economy. As consumers avoided in-person shopping and turned to e-commerce, U.S. online sales spiked 44 percent to more than $861 billion in 2020, according to Digital Commerce 360. But even that figure pales in comparison to the e-commerce growth in Australia and New Zealand, which led the globe with 108 percent growth in the second quarter of 2020 and 107 percent growth in the third.

To streamline these purchases, consumers moved en masse to mobile banking. Mobile payment options were already popular pre-pandemic, as consumers accessed mobile finance apps more than 1 trillion times in 2019, according to app marketing firm Liftoff. But in April 2020 alone, mobile banking registrations skyrocketed by 200 percent, while mobile banking traffic rose 85 percent, per Fidelity National Information Services.

As a result, demand for payment service providers (PSP) is also increasing. PSPs manage and streamline merchants' electronic transactions, offering services that allow the merchants to easily collect and reconcile online payments.

Client Spotlight:

Established in 1987, Card Access Services is the longest-tenured payment solutions provider in Australia, offering solutions to Australian and international businesses of every industry and size. The company, a PCI DSS Level 1 service provider, partners with 10 Australian banks and more than 80 banks around the globe to deliver real-time e-commerce, batch processing, recurring billing, IVR phone payments and tokenization, among other options that allow merchants to quickly and easily collect and reconcile payments collected via any payment channel. The company operates under the Card Access Services (CAS), Paymate and VendAccess brands.

Recently, Card Access Services also expanded to provide payment technology to governments in Southeast Asia and plans to increase its presence throughout the region by servicing merchants in both the public and private sectors. It also continues to introduce new products to support clients as ecommerce and online technologies evolve.

cardaccessservices

The Challenge:

Card Access Services, an Australian leader in the payment processing industry, has grown rapidly as ecommerce, mobile banking and new online technologies surged during the pandemic. The firm needed to ensure its increasing operations, new services and system changes remained compliant with PCI DSS—as well as begin to look ahead to the next round of standards, PCI DSS 4.0, expected to be released later this year. Additionally, Card Access Services required help in automating its system monitoring technologies and ensuring its migration to cloud operations met or exceeded stringent regulatory requirements.

The Solution:

Card Access Services' longstanding relationship with SecureTrust—one that dates back to 2011—has created rapport that ensures the two teams efficiently implement compensating controls to maintain Card Access Services' PCI DSS compliance during its rapid expansion.

By using SecureTrust as its Qualified Security Assessor (QSA), Card Access Service has help in performing the highest level of due diligence after each infrastructure upgrade and new system component installation. Through regular scope assessments, internal and external vulnerability scans and penetration testing, and updated dataflow diagrams, SecureTrust guarantees that every change is assessed, addressed and documented.

Moreover, SecureTrust's team of experts meets quarterly with Card Access Services executives for a wide-ranging discussion of threats, industry developments and more, so the client can continue to look around corners and stay ahead of complex, evolving security needs.

Industry Threat:

Defending against cyberthieves in an increasingly cashless world is complex—and will only become more so, as the number of consumers who make 51 to 100 percent of their monthly purchases online nearly doubled during the pandemic and will continue after the virus is contained, according to the 2020 World Payment Report.

Moreover, as fraud deterrents such as EMV chips have significantly reduced losses on payment cards, cybercriminals have moved on to the digital world of card-not-present transactions. CNP fraud now accounts for 74 percent of all ecommerce compromises, according to Trustwave's 2020 Global Security Report. Authorized push payment (APP) – in which a person or business erroneously allows an authorized mobile payment to a fraudulent recipient – and synthetic identities, created by cyberthieves through a combination of legitimate and fake information, continue to plague payment providers around the globe.

> *"The key thing for us is the insights and the guidance that SecureTrust provides to us, the support with PCI when we're introducing new applications into our technology, and making sure from a PCI compliance point of view and security point of view everything is streamlined and fitted within our existing process, that's been a big plus for us."*
>
> — Stelios Savva, General Manager
> Card Access Services

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com