SecureTrust™
a Trustwave® division

CASE STUDY

A different kind of food safety

The COVID-19 pandemic has further accelerated the shift to online shopping—and nowhere is this trend more evident than within the grocery industry, as consumers around the globe embrace online delivery and curbside pickup options. In fact, the number of new online grocery customers grew by 30% globally since the pandemic started, according to research firm Kantar Group, on top of a 22% spike in global online sales in 2019.

This growth, however, creates vulnerabilities. As the industry continues to evolve, stores increasingly rely on card-not-present transactions and network-connected devices. In recent years, credit cards with EMV chip technology have been so successful in fighting card-present fraud that cybercriminals have increasingly turned to the card-not-present space. Grocery stores - many of which have hundreds or thousands of stores—risk tremendous financial loss if bad actors disrupt operations or steal large amounts of customer information.

Client Spotlight:

Axfood, a leading food retail group in Sweden, reaches more than four million customers every week across 560 stores.

Axfood

The Challenge:

Axfood, a major grocery company in Sweden, had long relied on SecureTrust to help it meet the strict PCI DSS compliance requirements that affect both online card transactions and point-of-sale machines across its hundreds of stores. As COVID-19 changed shopping patterns, the grocery store wanted to ensure its card-not-present security solution was as robust as possible. Axfood also recognized that its centralisation made it especially vulnerable to a major operational disruption and wanted to focus on preventative efforts.

The Solution:

SecureTrust's cloud-based platform provided additional visibility into threats while continuing to manage the grocery stores' PCI compliance. Its elite SpiderLabs team and global network of security operations centers conducted regular vulnerability scanning and penetration testing across the company's databases, networks and applications to offer unique threat intelligence. It even went beyond the standard penetration testing required for PCI compliance, also completing active directory testing. What's more, because the in-house IT team had a longstanding relationship with its SecureTrust QSA and other consultants, it was able to dig deeper and establish more detail in every annual round of PCI assessments, ensuring that its compliance is impeccable.

> *"Over the years, we have developed a very comfortable relationship with our SecureTrust QSA and have learned a lot from him about PCI DSS scoping and compliance. He is extremely involved and really takes care of us as the customer."*
>
> — Jonas Garpedal, Payment Systems Operations Manager, Axfoods

> *"The longevity of our partnership with SecureTrust has allowed us to dive deeper each year with our PCI DSS compliance. Every year, our PCI approach has evolved, becoming more and more detailed as complexity and challenges increase."*
>
> — Jonas Garpedal, Payment Systems Operations Manager, Axfoods

Industry Threat:

The retail industry suffers the bulk of card-not-present breaches, according to the 2020 Trustwave Global Security Report. In fact, 53% of industry breaches are CNP events. Payment fraud involving CNP transactions is expected to cost merchants an estimated $130 billion in revenue between 2018 and 2023, according to U.K.-based consultancy Juniper Research.

On top of the payment fraud issue, grocery stores are also grappling with the rising threat posed by network-connected devices. In 2019, a Dutch man was arrested after hacking into a supermarket refrigeration system and changing the temperature system to ruin the food inside. Although centralised, automated systems may streamline operations in many ways, they risk opening a Pandora's box of new security threats.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com