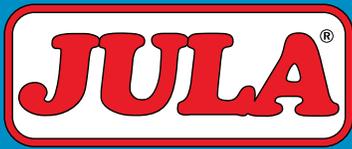# SecureTrust™
a Trustwave® division

CASE STUDY

Staying PCI DSS compliant as the global payment landscape evolves

As COVID-19 lockdowns forced consumers to embrace online shopping at a new level, shoppers compressed a decade's worth of e-commerce adoption into just three months during 2020, according to McKinsey & Co. Today, the global payment landscape continues to rapidly shift as the world looks ahead to a post-pandemic future. In fact, the EY Future Consumer Index notes that 80% of consumers are still changing the way they shop in 2021, and 43% maintain their COVID-19 habits of shopping online for products they previously would have purchased in-store.

The Challenge:

Jula Holding, a Swedish conglomerate primarily known for its home improvement stores, needed help reaching PCI DSS compliance beginning in 2011. Over the years, the company opened physical stores in new markets while also re-starting e-commerce operations in 2017, creating new complexity and requiring ongoing support to establish and maintain PCI compliance.

Today, Jula operates more than 110 stores while also planning e-commerce expansion across Europe. As its physical and online reach expands, the company needs to ensure its IT environment can meet strict compliance requirements for both the point-of-sale machines in its stores and online card transactions.

> *Every year, we've learned more about PCI DSS. There were complexity and challenges, but SecureTrust helped us to dig deeper and to understand the different requirements.*

— Lars-Göran Blomgren, CISO & Data Protection Officer, Jula Holding

The Solution:

The company's longstanding relationship with SecureTrust, who has produced Jula's annual Report on Compliance (RoC) since 2013, has resulted in the retailer reducing scope, along with addressing and documenting every system change, allowing them to complete and maintain PCI DSS compliance year-after-year.

> *The partnership with SecureTrust has brought Jula good knowledge and structure for an important security area. This provides stability and assurance of regular checks for PCI DSS compliance.*

— Lars-Göran Blomgren
CISO & Data Protection Officer, Jula Holding

Industry Spotlight:

While security breaches occur across every industry, retail has historically borne the largest brunt. In 2019, retail experienced 24% of all security incidents, followed by financial firms at 18%, according to Trustwave's 2020 Global Security Report. Moreover, e-commerce environments represented 22% of environments breached.

Cybercriminals perpetually target retailers to gain access to their vast troves of consumer data and credit card details. Whether by installing malware on POS systems or exploiting weak security on a wireless network to access a retailer's central database, bad actors continually hunt for and find ways to steal personal data that can be sold on the black market. And as retailers look to leverage data to boost sales and better serve customers, the opportunities for cyberthieves will continue to grow.

Retailers that experience a breach often spend many years and millions of dollars dealing with the aftermath. In late 2020, a large home improvement retailer finally agreed to a $17.5 million settlement over a 2014 breach related to POS system malware. But even as the retailer put its breach behind it, many more retailers experienced new compromises in 2020, showing that even large brands continue to struggle to protect their customer information.