SecureTrust™
a Trustwave® division

CASE STUDY

Protecting the flow of money in a global economy

Modern consumers expect convenience and simplicity throughout the payment process—including when traveling abroad. Dynamic currency conversion (DCC) is a payment card feature allowing customers to make a payment in a foreign country using the currency of their home country.

The customer is offered an on-screen option on the POS device displaying the exact amount their card will be charged, including the exchange rate fee, preventing exposure to changing rates and eliminating unpleasant surprises when the payment card statement arrives. As consumers know the final payment amount at the time of transaction, they're less likely to contest a charge due to unrecognised transaction amounts. As a result, the merchants' risk of chargebacks plummets.

Dynamic currency service providers offer technology that enables and supports acquirers and their merchants to deliver currency conversion in both card-present and card-not-present environments—including ATMs, bricks-and-mortar locations and ecommerce sites.

Client Spotlight:

Founded in 1997, Monex Financial Services Ltd, an Irish based company is the world's largest and longest-established dynamic currency provider and a leader in online multi-currency pricing. It serves multiple sectors including retail, financial services, ecommerce, hospitality, travel and gaming, processing more than 407 million secure online transactions across 50 countries and four continents.

MONEX
FINANCIAL SERVICES LTD

"Winning the race against cybersecurity threats is absolutely critical to our success as a company. By partnering with SecureTrust for continuous PCI compliance and security support, we've avoided being caught flat-footed."

— Brian Kiely, IT Director, Monex Financial Services Ltd.

The Challenge:

Monex Financial Services LTD, a major dynamic currency provider, was sourcing assistance to guard against an array of cybersecurity attacks, including ransomware and phishing attempts, as part of its ongoing effort to maintain PCI DSS compliance.

Monex handles high volume card transactions annually on behalf of acquirer and merchant clients and qualifies as a Level 1 service provider under PCI regulations, requiring the highest compliance standards. Accordingly, Monex submits continuous assessment material including an annual compliance report completed onsite by a qualified security assessor (QSA), a quarterly network scan and ongoing penetration testing.

As part of its development planning, Monex reviewed additional markets worldwide, adding complexity to its cybersecurity needs by requiring international offices to quickly get up to speed on PCI protocols.

The Solution:

SecureTrust's relationship with Monex began in 2005 when SecureTrust helped the company became the first DCC provider to obtain PCI DSS compliance. Since then, Monex continues to rely on SecureTrust's expertise to remain compliant with constantly evolving and increasingly complex PCI standards. Today, SecureTrust serves as Monex's QSA and maintains the company's sterling record of integrating secure payments in a global environment.

SecureTrust has the most QSAs of any security and compliance company in the world and speedily placed multilingual experts at Monex's international offices. Teams work together across continents using SecureTrust's proprietary Compliance Manager, a real-time, cloud-based tool that provides actionable information in a single, consolidated view. Monex satisfies requirement criteria of the most recent PCI DSS 3.2 standard and has settled into a reliable, efficient, PCI maintenance program to continuously address and anticipate evolving security requirements.

As part of its compliance, Monex utilises leading-edge encryption and tokenization—a security measure which generates an alternate account number, or "token," to replace a cardholder's 16-digit card number—to assist acquirers and merchants in shielding cardholder details and dramatically reducing fraud associated with online payments while improving the customer experience.

Industry Threat:

As consumer spending continues to move online, payment fraud is on the rise: A recent report by Juniper Research estimates that ecommerce merchant losses due to online payment fraud will exceed $25 billion in 2024, up from $17 billion in 2020.

This spike in ecommerce fraud is partially due to cybercriminals refocusing their efforts toward card-not-present environments as an increase in EMV chip-card readers has made stealing card data from physical POS systems more difficult, according to Trustwave's Global Security Report.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com