WHITE PAPER

Web Risk Monitoring:

HOW TO HIT THE MOVING TARGET OF CARD BRAND COMPLIANCE

SecureTrust™
a Trustwave® division

Overview

As e-commerce has mushroomed, so too have unethical merchants attempting to sell counterfeit merchandise, illegal drugs, offensive pornography and more. And because these merchants collect payment in advance of delivering the product, the risk when one sells something illegal is borne by the merchant acquirer—the entity that maintains the merchant account and settles card transactions for the seller.

To protect themselves against malicious merchants, each major credit card network—Visa, Mastercard, American Express and Discover—has created a set of stringent regulations that acquiring banks, payment processors, payment gateways and independent sales organizations (ISOs) must meet.

These standards were established in addition to the industry-wide Payment Card Industry (PCI) Data Security Standard to help acquirers prevent financial and reputational harm, but their complexity combined with the ever-evolving creativity of online criminals have left banks and payment processors struggling to keep up. And if they're found to be in violation of these rules, banks and other acquirers' risk hefty fines that can reach into the six figures.

To evaluate your security posture and ensure your organization maintains compliance, it's important to take a 360-degree approach to risk mitigation by combining artificial intelligence with a team of human experts who monitor merchants' operations. SecureTrust Web Risk Monitoring helps you stay abreast of regulatory and industry mandates while preventing fraud, lowering the cost of manual website reviews and eliminating noncompliance fines.

In this white paper, we'll examine the origin of web risk monitoring and the five key services provided, including:

Content Monitoring for card brand monitoring and onboarding requirements such as MasterCard Business Risk Assessment and Mitigation (BRAM) and Visa Global Brand Protection Program (GBPP)

Merchant Intelligence to validate business operations, identify third-party relationships, and conduct URL discovery

Malware Monitoring that allows you to deliver a Merchant Malware Report to your merchants as well as reviewing merchant website security

Custom Monitoring for your specific requirements such as counterfeit merchandise, terms of service violations, and searches for false claims

Transaction Laundering Detection for identification and reporting of previously unknown illicit websites associated with a merchant

The Evolution of Merchant Risk Management

During the Wild West days of e-commerce in the early 2000s, payment fraud began to increase. Recognizing the need to track and shut down bad actors who were processing illegal or otherwise harmful online transactions, credit card companies launched the Payment Card Industry (PCI) Data Security Standard in 2004.

Created to unify industry standards for storing, processing and transmitting cardholder data, the PCI DSS has evolved rapidly over the past 15 years. Today, the set of 12 data security requirements include technical, policy and training protocols to help merchants secure their systems and protect sensitive payment card data from compromise. As of 2020, the PCI Security Standard Council has begun work on version 4.0, highlighting the ever-changing nature of both technology and security threats.

Around the time the PCI standards were created, large credit card companies also launched their own propriety programs. MasterCard, for example, launched its Business Risk Assessment and Mitigation (BRAM) Program in 2005 to protect MasterCard and its customers from illegal and brand-damaging transactions. Visa, too, began its Global Brand Protection Program (GBPP) to guard against its cards being used to process transactions involving prescription or illegal drugs, counterfeit merchandise, child and offensive pornography, pirated movies and more.

These programs required merchant acquirers to identify high-risk merchants and monitor their activity to ensure the merchants are not processing illegal or problematic transactions. An acquirer who fails to do so faces fines that can reach into the six figures per transaction—a potentially devastating financial blow.

Trustwave, a Chicago-based firm that helped create the original PCI DSS, quickly established itself as the industry leader in compliance and security solutions. In 2018, Trustwave spun off its PCI compliance division, rebranding as SecureTrust. Today, these deep roots in PCI compliance and its experts' many years of experience allow SecureTrust to help businesses of all sizes secure their data and achieve compliance.

In the ensuing years, compliance with PCI and individual card brand standards has become a moving target as technology changes, businesses grow, and criminals become more cunning.

"The rules about which type of transactions are forbidden have become a little bit foggy," says Jon Marler, SecureTrust's Product Manager. "We all know you can't buy illegal weapons or drugs online, but beyond that, there are lots of gray areas and confusion. There are several areas of online product marketing that are not always obvious and need experts to help navigate."

As such, acquirers, payment processors and service providers need a sophisticated monitoring program to ensure compliance and avoid potentially huge fines. That's why today, businesses small and large rely on SecureTrust's cloud-based Web Risk Monitoring—managed through the SecureTrust web portal—to detect and shut down problematic transactions with a state-of-the-art combination of artificial intelligence and human expertise.

Five Steps to Fight Back Against E-Commerce Fraud

#1: The Foundation: Content Monitoring

Successful web risk monitoring begins with robust website content monitoring. This includes both broad, automated scanning and manual deep dives by a team of experts to review merchant sites and activity that is illegal or violates card brand regulations and threatens your business. SecureTrust's content monitoring is built around the needs of standard card brand requirements and supports both MasterCard's Business Risk Assessment and Mitigation Program (BRAM) and Visa's Global Brand Protection Program (GBPP). Using leading-edge artificial intelligence, SecureTrust's content monitoring scans, detects, inventories and analyzes e-commerce sites' content in a fraction of the time required to perform the same functions manually.

The automated system then creates a special queue for any findings, which is then carefully reviewed in real time by Trustwave's expert auditors. From there, the potentially problematic sites are reported, with the results presented in an easy-to-read, customized dashboard. Potential violations are immediately presented for your review to ensure that all violations are eliminated, and you are spared costly fines.

#2: Diving Deeper: Merchant Intelligence

Merchant intelligence augments your existing Know-Your-Customer (KYC) process and provides a fuller view of your merchants' online activity through five specific tools:

- **Merchant Policy Monitoring:** This service tracks changes in merchants' published policies, including privacy, shipping and return policies as well as terms of service.
- **Technology Stack Detection:** This module will help you identify the e-commerce platforms, web technologies, and service providers your merchants employ to deliver their website. By detecting and managing every component of the merchant's technology stack, you dramatically reduce the risk of a breach and regulatory risk.
- **Merchant Discovery:** Often during the onboarding process, the URLs of the websites that a merchant deploys are not immediately available or captured as part of underwriting. Merchant Discovery can identify the websites each merchant deploys so that they can be added to the program quickly and all merchants are constantly monitored.
- **Geolocation and IP Analysis:** This service confirms your merchants' physical addresses via Google Street View and then analyzes the website IP addresses to understand where the merchants are hosting sites and how many other sites are associated with the same IP address.
- **Additional Risk Checks:** Merchant Intelligence also analyzes the merchant website to verify that the assigned Merchant Category Code (MCC) is correct, and checks site categorization to ensure a merchant actually sells what it says it sells; looks for hidden content on a merchants' website by discovering password protected pages; domain WHOIS registration details; and analyzes previous known risk alerts.

#3: Identifying Third-Party Risks: Malware Monitoring

Malware, like all online crime, continues to evolve. According to Trustwave's 2020 Global Security Report, cybercriminals who have traditionally stolen credit card data through point-of-sale malware are now beginning to target e-commerce sites. What's worse, many e-commerce platforms and other third-party services lack integrated tools to detect malware, and out-of-date, unsupported open-source platforms such as shopping carts and web technologies are particularly vulnerable.

The card brands such as Visa and MasterCard are concerned about the risks posed by third-parties – especially unsupported/outdated shopping carts, which could expose cardholder data to hackers. As a result, they have required their acquiring banks to (1) identify merchants using unsupported/outdated shopping carts and (2) to move those merchants to platforms that will enable the merchant to be PCI DSS compliant and lessen the risk of a data breach associated with outdated technology.

The SecureTrust Malware Monitoring service also fights back by offering targeted vulnerability scans—including site encryption (SSL) validation and malware detection powered by industry leading malware detection technologies—as you add new merchants, plus continuous, concise reports of merchants currently affected by malware. It goes further by offering an easy-to-use malware report you can offer to your merchants to drive additional revenue. The automated merchant tool includes:

- Automated malware scanning
- SSL certificate detection and analysis
- Webserver SSL vulnerability detection and configuration auditing
- Simple alerts and remediation instructions

#4: Defining Your Own Parameters: Custom Monitoring

Custom Monitoring allows you to identify merchants and content that violates your Terms of Service (TOS) even if they technically adhere to card brand program rules. This service searches for the exact requirements you define—which can include a specific product, service, policy or false claim—and issues an alert when such content is identified by a Trustwave auditor. You can customize the scan frequency and language capabilities, as well as greenlight the automatic onboarding of merchants who pass your customized inspection.

#5: Connecting the Dots: Transaction Laundering Detection

Unfortunately, even vigilant content and merchant monitoring won't catch all malfeasance. Criminals frequently use websites for legitimate businesses to mask a hidden site that sells services prohibited by card brands. For example, BobsFlowers.com really sells flowers, but the owner could be a collusive merchant who also processes transactions on behalf of two other businesses selling illegal drugs—or his merchant processing account might have been compromised by criminals. Either way, a customer who purchases illegal goods online will see a charge from a flower shop appear on their card statement. The illegal transaction is directed through the legitimate account's payment gateway and unwittingly laundered by the payment service provider. This leads to chargebacks and subsequent investigations by the card brands and law enforcement that will eventually uncover the illegal activity.

Transaction launderers have become increasingly skilled at evading detection and have adapted to better risk monitoring by closely monitoring their fraud ratio to avoid any alert to their multiple banking and account providers. As online storefronts have proliferated and software makes it easy for someone to set up a shop in minutes, criminals have ample targets. They can also easily create their own fraudulent storefronts to generate fake invoices for false transactions.

SecureTrust's reliable, scalable and easy-to-use Transaction Laundering Detection service locates these previously unrecognized problematic sites and associates them with the merchant responsible. You receive a report of sites connected to each merchant and a separate report with the sites discovered to be in violation of a card brand standard—which is integrated into the MasterCard MMP Reporting tool, allowing easy delivery of your monthly reports to Mastercard.

Conclusion

As card brand requirements grow ever more complex and cybercriminals grow increasingly savvy, merchant service providers need a well-designed, fully supported program to ensure compliance and mitigate risk. By offering a high-touch, dedicated team of experts who review your website content in concert with automated, easy-to-use tools, SecureTrust delivers an integrated approach that ensures you meet card brand requirements while also expanding the services you can offer merchants. Through a five-pronged approach, SecureTrust provides the guidance to help you master regulatory and industry mandates while preventing fraud, reducing costs and achieving the revenue goals that will take your company to the next level.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com