EverCompliant
More Intelligence. Less Risk.

MORE INTELLIGENCE. LESS RISK.
EVER COMPLIANT.

Pioneers of transaction laundering prevention.

We help you
see more

ONLINE TRANSACTION LAUNDERING

And the Evolving Landscape of E-Commerce Merchant Fraud

Imagine you own a property that you are renting out when not in use. This might be a summer house, or maybe a city apartment before you moved out with your family in the suburbs. You take great care to make sure that your tenants are trust worthy ones, clean, well mannered, and financially stable. You have adopted a due diligence process in which you ask for some documentation and recommendations, and invest what you consider reasonable efforts to guarantee your tenants are good honest people.

Now suppose that one day you get a call from a neighbor telling you that there is noise and suspicious activity around the property, The neighbor seems to think that the tenants maybe connected or selling illegal drugs from your rented home. The next day your internet service provider is calling to tell you that extreme illegal content has been downloaded through your internet subscription. You are quite worried, and you call the police to go check in on the property and what they tell you is not less than shocking – your approved tenant has been subletting your property, and the people living in your house are using the property to sell illegal drugs.

What's more, your failure to recognize and stop the activity from occurring on your property has implicated you as an accessory to this crime since the facilities are owned by you and the services are registered under your name. What could you do more? What is expected of you?

ONLINE FRAUDSTERS OUTSMARTING THE PAYMENTS SYSTEM

Merchant service providers (MSPs) [1] are no different. They go to great lengths to ensure that the businesses they serve — and their corresponding activities — are both known and legitimate. By carefully vetting their incoming merchants, these service providers strive to build a profitable business while minimizing the associated risk. But, can they?

The underwriting process for online sellers often includes automated technologies, as well as manual checks to ensure that the merchant, its products/services and its customers align with the details provided on the merchant application. After years of getting burned, the payments industry has become adept at discovering anomalies on the merchant's reported website.

> Fraudsters' ongoing attempts to avoid detection create an evolving landscape that challenges the risk monitoring methods used by payments industry stakeholders today.

Within this evolving online landscape a new enemy has emerged, and it's catching many MSPs off guard. Now, rather than hiding their illegal pharmacies, counterfeit product sales, illicit pornography, unlicensed gambling, and the like on a primary website (i.e. the site listed on their merchant application), unscrupulous merchants are creating an ecosystem of unreported e-commerce. In this new scenario, the site the MSP knows about serves as a storefront to which payments are funneled, effectively masking the nefarious sales activity taking place on one or more associated yet undisclosed websites.

[1] For the purposes of this paper, merchant service providers (MSPs) are defined as sponsor banks, independent sales organizations (ISOs), acquirers, payment facilitators and other entities providing services that enable businesses to accept credit and debit cards as a form of payment.

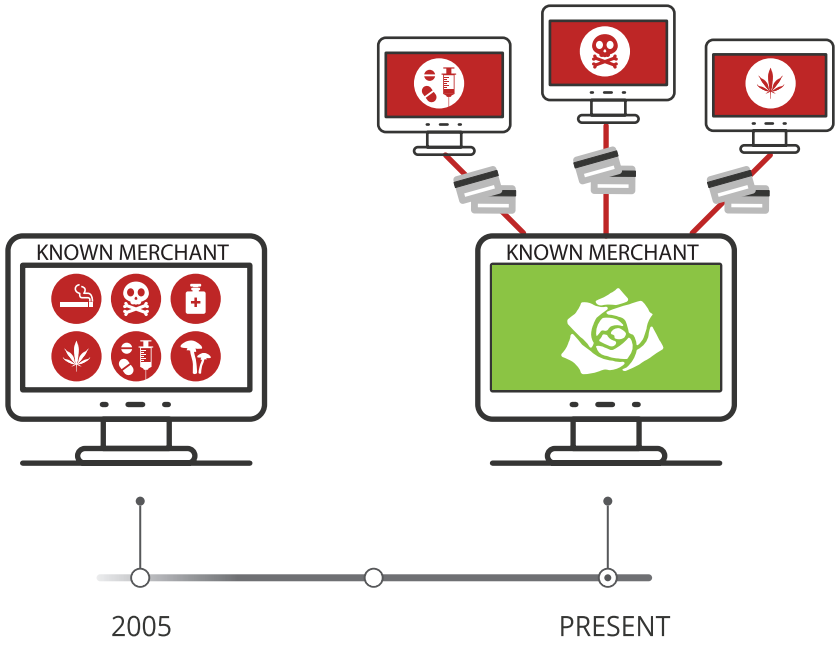

Figure 1: *The progression of online merchant fraud*

Referred to as "online transaction laundering" or "undisclosed aggregation," the payment activity emanating from merchants' unknown websites is now implicating MSPs in a web of prohibited, brand-damaging e-commerce activity they don't know how to detect, let alone prevent. Fines are being levied and regulatory scrutiny is being applied, yet the conversation on how to properly address transaction laundering is in its infancy.

Referred to as "online transaction laundering" or "undisclosed aggregation," the payment activity emanating from merchants' unknown websites is now implicating MSPs in a web of prohibited, brand-damaging e-commerce activity they don't know how to detect, let alone prevent.

This white paper discusses the size and scope of the online transaction laundering problem, its sophistication over previous methods for hiding illegal e-commerce, and how payments industry stakeholders are working to detect it and mitigate the associated business risks. MSPs can utilize this information to better understand their organization's risk and options to reduce their exposure.

MERCHANT SERVICE PROVIDERS IN THE CROSSHAIRS

Over the past decade, credit card brands and government regulators have placed increasing pressure on MSPs to "know their customers" and take responsibility for the business being transacted under their watch. MSPs have responded by assembling resources and implementing technologies and processes to better monitor merchant risk, knowing that this risk includes the potential of 7-figure fines as well as lawsuits.

Yet to remain viable, risk-monitoring initiatives must strike a balance between the related overhead costs and a proven return on investment for avoidance of potential fines (i.e. reduced financial losses in terms of card brand fines, legal fees and excessive chargebacks). The investment

involved in successfully managing portfolio risk may be in competition with working capital that enables MSPs to more rapidly grow their business. Therefore, any added burden in terms of risk-management personnel, processes and/or technologies can cause conflict in the organization as they weigh their priorities in balancing risk mitigation versus growth investments.

In the traditional online merchant brand/content violation scenario, risky or illegal sales activity is typically hidden within the website that's registered with the MSP. Risk management professionals use processes and technologies that can review these known websites and quickly hone in on the unusual patterns and attributes that signal a problem. The migration of illicit e-commerce schemes toward online transaction laundering involves additional websites that are unknown to the MSP, thereby disrupting the streamlined risk management processes MSPs have come to rely on. With undisclosed websites in the mix, previous methods to inspect and validate merchants for onboarding are called into question, and ongoing monitoring initiatives are equally complicated.

The advent of online transaction laundering places MSP organizations in a precarious position. While traditional monitoring methods have made it nearly impossible to spot the unreported websites and the associated illegal activity that certain merchants are facilitating, the card brands are holding firm to a zero-tolerance stance.

TRANSACTION LAUNDERING'S ONLINE BREEDING GROUND

Innovation within online payments — including the payment facilitator model for rapid onboarding, instant website/web store creation technology and inexpensive hosting — has helped make the online landscape conducive for transaction laundering activity. That's because those undertaking this activity are innovating as well, taking advantage of expedited onboarding and leveraging the latest technologies and processes to exploit weaknesses and continue operating under the radar of the payments industry.

Figure 2 is a simple illustration of a transaction laundering scenario. In this example, the acquirer underwrites an online flower shop after it passes all website inspection requirements, including scans for content issues. The acquirer believes it has a low risk online business on the books, but in reality the flower shop is serving as a "faux storefront" for a web store that sells illegal prescription drugs. As the drug shop's transactions process through the flower shop, the fraudulent merchant makes sure to cover the trail by making each transaction appear like a legitimate purchase from within the flower shop itself.

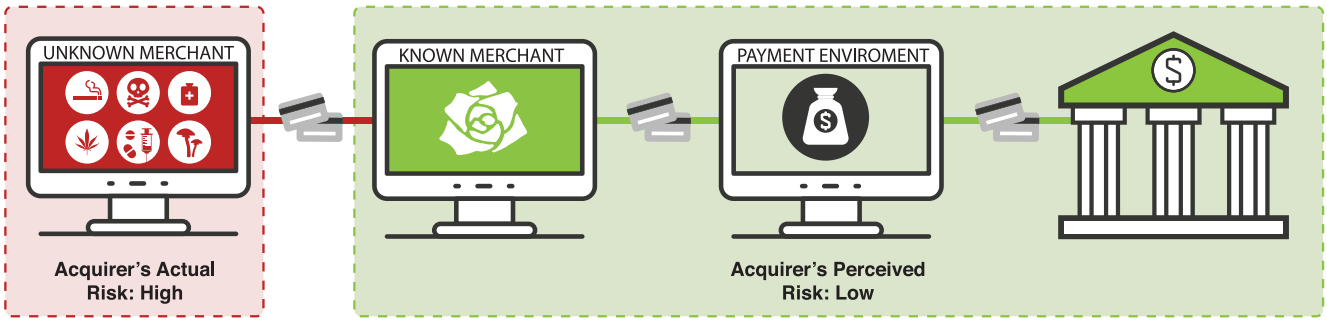

Figure 2: *The progression of online merchant fraud*

HOW IS TRANSACTION LAUNDERING POSSIBLE?

There are various methods for hiding the extended ecosystems that support transaction laundering. As can be expected, the approaches range in sophistication from simple payment-environment credential sharing (Figure 3A) to embedding the same payment form used by the known website into one or more unreported websites (Figure 3B). And, in some cases, an unreported website is operating independently of the known site, with no direct cyber linkage between the two sites (Figure 3C). In this situation, the unreported website could be using the most low tech means of passing transactions to the registered merchant, sending a spreadsheet for manual input or calling the information into the merchant with the legitimate account. This is the most challenging scenario to identify.

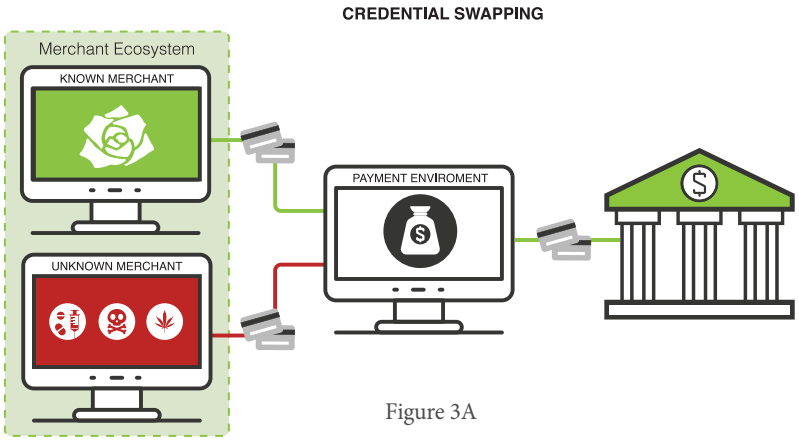

Figure 3A

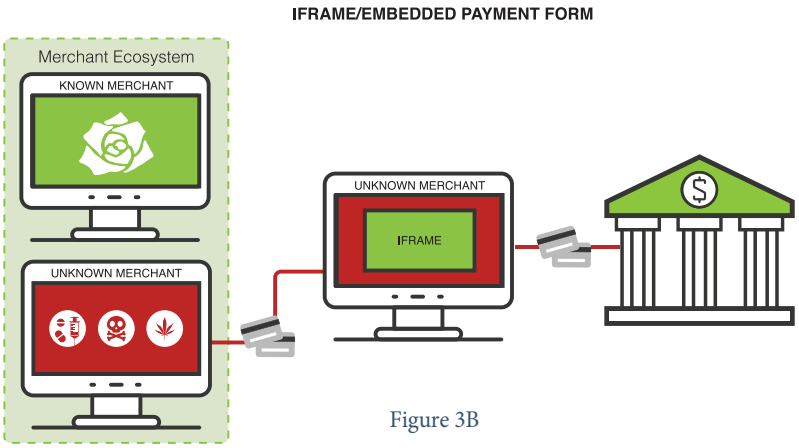

Figure 3B

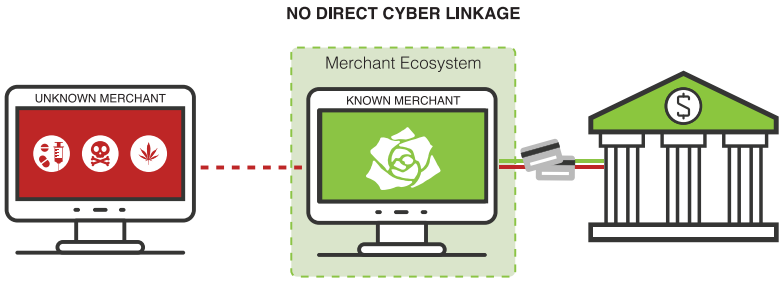

Figure 3C

Figure 3: Transaction laundering techniques

HOW PREVALENT IS TRANSACTION LAUNDERING TODAY?

While conducting online merchant fraud detection for two international acquiring banks over the course of six months, EverCompliant, a leading cyber intelligence technology pioneer, discovered that an average of five unknown websites existed for every known website they examined. Further, an average of 3% of those unknown sites contained high risk content, as well as e-commerce environments, a combination that is a strong indicator of potential transaction laundering risk. Of this population, 3% of the sites were confirmed to be laundering transactions through the legitimate merchants' sites.

It's important to note that the two banks in this study carry low-risk portfolios. MSPs boarding high-risk merchants will very likely see a higher percentage of undisclosed websites conducting transaction laundering activity.

5
unknown websites existed for every known website

↓

3%
contained high risk content

TRANSACTION LAUNDERING IN ACTION

The following case studies illustrate the hidden transaction laundering activities (and associated risk) discovered through various MerchantView engagements.[2] As shown here, a single, known site can be connected to hundreds of unreported sites, many of which include the embedded payment environments that are a hotbed for transaction laundering.

A single, known site can be connected to hundreds of unreported sites, many of which include the embedded payment environments that are a hotbed for transaction laundering.

[2]MerchantView is a cloud-based technology solution that identifies unreported websites and their content, including established payment environments that indicate transaction laundering activity.

Case Study #1: Card-brand fine leads to ugly discovery.

A payment facilitator received a card-brand fine for a content violation for nefarious activity attributed to a seemingly legitimate fundraising website. The payment facilitator initiated an investigation revealing that the merchant's known site actually had an extensive online ecosystem associated with it. In all there were 70 unreported websites, with more than 20 of them conducting activity related to illicit pornography. The transaction that caused the fine was confirmed to have originated on one of those unreported websites.
Figure 4 [below or at right, etc.] shows the ecosystem of illegal websites hiding behind the registered merchant site. URLs have been modified, but they still reveal the obvious dangerous content likely to be sold on these sites

Figure 4: Online ecosystem of associated, unreported websites with high risk content.

Case Study #2: Nutraceutical merchant's network is finally exposed.

An acquirer was conducting enhanced due diligence on a subset of its merchants in preparation for a sponsor bank audit. The acquirer had suspicions about one of its high-volume nutraceutical merchants in particular. The risk management team performed extensive research and was unable to detect any clues. The MerchantView deployment returned conclusive results: The suspicious merchant was supporting an extended network of 33 active websites selling a range of products in the nutraceutical space with multiple incidences of unverifiable claims. Equipped with this new insight, the acquirer was able to confirm that the associated sites were in fact tunneling transactions through the registered merchant account. As a result they had the proof needed to shut down the merchant.

FROM TRANSACTIONS LAUNDERING TO MONEY LAUNDERING

Starting in 1970 with the Banking Secrecy Act and the Patriot Act in 2001, the AML legislation under the UN's FATF guidelines are evolving. The fines imposed on financial institutions are breaking records on an annual basis and have reached a touching distance from the $10B barrier with BNP-Paribas's settlement agreement with the Department of Justice.

Acquiring banks and payment processors are traditionally considered low to mid risk when it comes to fraudulent activity. Their main focus is on KYC procedures to comply with group standards for AML compliance. In today's world the evolving transactions laundering schemes are turning these assumptions upside down.

The registration of illegal activity as a legitimate one, the bear essence of transaction laundering, is money laundering by definition. The underlying vulnerabilities is what creates the simplicity of transaction laundering, i.e. the easiness in which online merchants can be integrated into the payment system, can just as easily facilitate layering activities in which the merchant transactions are a wash on their own. In this situation the customer and the merchant are the same beneficiary, and no real commercial purchase is taking place.

What is just as alarming is the revelation that in the e-commerce world, the off-line KYC procedures taking place today are far from satisfying the requirements and standards imposed on the global financial system by the regulatory bodies. It becomes clearer and clearer that the usage of sophisticated cyber intelligence is critical and even essential for the validation of customer identity. The massive criminal networks identified in recent years make the case for revealing and uncovering the hidden connections between online entities a core task in the never ending money laundering prevention function.

It becomes clearer and clearer that the usage of sophisticated cyber intelligence is critical and even essential for the validation of customer identity

RECOMMENDATIONS FOR ADDRESSING THE PROBLEM

Transaction laundering activity is a significant and growing problem within the online space, further intensifying the urgency for MSPs and other payments industry stakeholders to become as agile and efficient as the fraudsters themselves. Yet in the evolution of online merchant fraud, the old tactics never completely disappear; the evolution is cumulative, with new types of fraud layering onto the old. The resulting challenge is complex and therefore requires a multi-faceted solution. The following recommendations can provide a good place to start:

Transaction laundering activity is a significant and growing problem within the online space, further intensifying the urgency for MSPs and other payments industry stakeholders to become as agile and efficient as the fraudsters themselves.

Recommendation #1: Leverage technology to expose actual merchant risk.

The transaction laundering threat requires a fundamental change in how the industry goes about vetting and monitoring online merchants. This involves moving beyond the known websites so as to detect and monitor the elaborate online ecosystems that have heretofore been invisible to MSPs. Solutions that rely on manual steps simply won't make it in this atmosphere; they must be automated so they can effectively scale.

Along with their scalability, automated technologies are ideal for discovering repeatable patterns and then reporting on them in near-real time. This speeds up the decision-making process for merchant onboarding. While current automated risk monitoring systems typically require some level of human interaction for quality assurance, the cumulative intelligence these solutions are capable of gathering will likely decrease this need over time.

Recommendation #2: Awareness and Training.

The MSP's entire business is centered on serving merchants and managing risk; therefore, all associates in the value chain have a role to play in spotting the "bad apples." Risk management is a team sport and it is imperative to raise awareness of the transaction laundering issue among stakeholders. This includes not just underwriters and risk analysts, but also sales, fraud investigators, chargeback specialists and service provider partners. For example, analyzing chargeback records can help identify problematic trends and potential transaction laundering activity. Salespeople can help by evaluating whether the merchant's forecasted transaction volume and value is rational and supported by the logical inventory and warehouse demands.

Efforts should be focused on identifying any key indicators or trends around this activity, and departments throughout the organization should receive frequent training to reinforce awareness and communicate new insights that can help flag the signs of transaction laundering

Recommendation #3: Knowledge Share and Industry Collaboration.

Shared intelligence stops fraudsters from just going somewhere else. As a community, payments industry players must work together to help each other combat scammers' moneymaking schemes and relentless pursuit of abusing their online merchant accounts for criminal gain.

MasterCard MATCH and Visa VMAS have helped industry stakeholders join forces to share information about problematic merchants. Payments associations and conferences, online fraud groups and ongoing conversations with risk management partners present additional opportunities to share information about merchants conducting illegal activity and successful detection strategies. Fraudsters have a sophisticated network and rarely operate independently. They interact with their likeminded counterparts in an effort to stay ahead of industry detection methods. Knowledge sharing and collaboration beats them at their own game.

AN EVOLVING THREAT, AN EVOLVING SOLUTION

Transaction laundering represents a new twist on the traditional online merchant fraud techniques, and has become the cause of most card brand fines. With an average of one in every five e-commerce merchants supporting extended online networks, the problem warrants increased investment in technology and attention to approval and monitoring processes.

While there is likely no "silver bullet" for eradicating online merchant fraud, merchant service providers are obligated to continue enhancing their methodologies for recognizing and putting a stop to illegal payment activity.

> "It comes down to this: When a bank allows its customers, and even its customers' customers, access to the national banking system, it should endeavor to understand the true nature of the business that it will allow to access the payment system, and the risks posed to consumers and society regarding criminal or other unlawful conduct."

The payments industry is currently faced with an opportunity to share intelligence and pursue a comprehensive solution that can keep pace with nefarious online businesses at every turn. For their part, each merchant service provider can begin by engaging and educating internal resources, building external information exchange and leveraging cutting-edge monitoring technologies to better identify and mitigate risky e-commerce merchants.

Like other fraud problems this is a dynamic and evolving one. It spreads and grows and moves around to exploit the weakest link at every point in time. If you are a merchant service provider, it will increasingly become mission critical not to be that weakest link, and strive to be a step ahead of the bad guys, and the regulators fining upon identifying such activity facilitated by the MSPs.

ABOUT EVERCOMPLIANT

Transaction laundering represents a new twist on the traditional online merchant fraud techniques, and has become the cause of most card brand fines. With an average of one in every five e-commerce merchants supporting extended online networks, the problem warrants increased investment in technology and attention to approval and monitoring processes.

While there is likely no "silver bullet" for eradicating online merchant fraud, merchant service providers are obligated to continue enhancing their methodologies for recognizing and putting a stop to illegal payment activity.