WHITE PAPER

HOW TO PREVENT TRANSACTION LAUNDERING
Imagine you own a property that you are renting to others when not in use: a summer house, or a city apartment you purchased as income property. You take great care to make sure that your tenants are trustworthy ones; clean, respectable and financially stable. You adopt a due diligence process, in which you request documentation and references, and invest significant efforts to guarantee your tenants are reliable, honest people.

One day, you get a call from a neighbor telling you that there is noise and suspicious activity around the property. The neighbor believes that the tenants may be selling illegal drugs from your rented home. Worried, you call the police to go check in on the property and what they tell you is shocking — your approved tenant has been subletting your home, and those unknown, unapproved tenants are conducting illegal activities on your property.

Everything from the title to the utility services are registered under your name. Your failure to spot and stop the activity occurring on your property could potentially have you implicated as an accessory to these crimes.

Merchant service providers (MSPs) frequently find themselves in similar situations. They go to great lengths to ensure that the businesses they serve - and their related activities - are properly identified and legitimate. By carefully vetting their incoming merchants, MSPs strive to build a profitable business, while working to minimize the associated risk that comes with an online merchant portfolio. Yet, they repeatedly find themselves accused of facilitating illicit or illegal activity that is seemingly out of their control.

What more can they do? How can they track and prevent cyber crime that directly affects their business?

CRIMINALS HAVE SHIFTED TO ELECTRONIC MONEY LAUNDERING

---

1 For the purposes of this paper, merchant service providers (MSPs) are defined as sponsor banks, independent sales organizations (ISOs), payment service providers (PSPs), acquirers, payment facilitators, marketplaces and other entities providing services that enable businesses to accept credit and debit cards or digital wallets as a form of payment.
Electronic Money Laundering, also known as Transaction Laundering, is the digital evolution of money laundering. Initiated by the surge of online commerce, this fraud scheme has become a massive concern for the payments industry.

Transaction Laundering occurs when an undisclosed business uses an approved merchant’s payment credentials to process payments for unknown products and services, typically illicit or illegal, through a card brand network. After successfully passing Know Your Customer (KYC) checks and establishing a new account, deceptive merchants can cheat the system by simply lying about their line of business or by adopting questionable business methods once the account is active.

Rather than using the registered website - the site listed on their merchant application - corrupt merchants are now creating their own, hidden ecosystems of unreported e-commerce to sell weapons, illegal pharmaceuticals, counterfeit products, illicit pornography, etc.

As e-commerce grows, so does the threat of Transaction Laundering. According to our research, 38.1% of all money laundering is now conducted through the e-commerce ecosystem, with an increase of 8.4% year over year. We estimate that $500 billion dollars will be laundered via e-commerce in 2018.

The extent of the problem is far-reaching, as expansive as the Internet itself. As the e-commerce ecosystem grows more sophisticated and widespread, so does the threat of Transaction Laundering.
Laundering money once required a great deal of effort from the criminal’s standpoint. In many cases, they had to set up or purchase a brick-and-mortar business, ensure it was running legitimately, keep clean books, and incur considerable upfront operating expenses.

Innovation within online payments - including the surge of payment platform options, payment facilitator models, instant webstore creation technology and inexpensive hosting - has helped to make the online landscape a breeding ground for illegal activity. It is because criminals, too, are innovative in their own ways, taking advantage of the latest technologies to exploit weaknesses in the system.

In this new age, the volume of data associated with transactions is enormous, making it increasingly difficult for any player in the chain to determine the origin, target and nature of a payment. Ill-intentioned merchants can quickly and inexpensively conceal the nature of their transactions. Transaction Laundering shares the same basic principles of money laundering, as it disguising an illegal activity as a legitimate one.

**HOW TRANSACTION LAUNDERING WORKS**

The figure below is an illustrative example of a Transaction Laundering scenario, in which the acquirer registers an online flower shop as new merchant, after it passes all KYC checks and vetting requirements.
The acquirer believes it has a low-risk online business on the books, but the flower shop is serving as a false, virtual storefront for a website that sells illegal prescription drugs. As the drug shop’s transactions process through the flower shop, the fraudulent merchant makes sure to cover its trail by disguising each transaction as a legitimate purchase from the flower shop.

There are various methods for hiding the expanded ecosystems that support Transaction Laundering. 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).

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.
The global increase of new payment systems creates a significant complexity level for acquirers and payment processors to understand the true origin of a transaction. Typically, they focus on KYC procedures to comply with Anti-Money Laundering (AML) standards, but today’s evolving Transaction Laundering schemes are challenging the efficacy of these standard processes.

Additionally, the rapid increase of micro merchants creates a huge data overload for payment processors to manage. The inability to detect this activity represents a serious business risk. MSPs – including acquirers, Payment Service Providers (PSPs), Independent Sales Organizations (ISOs), Payment Facilitators and online marketplaces – can be unknowingly and unintentionally facilitating criminal activity, putting themselves at risk of potential fines, legal action and damaging their overall reputation.

Credit card brands and government regulators have placed growing demands on MSPs to and take accountability for the businesses being transacted under their watch. In the past decade, the fines imposed on financial institutions, related to their failure to conduct proper due diligence on customer and third parties, are breaking records in volume and size.

AML legislation continues to evolve under the UN’s Financial Action Task Force guidelines, most notably with the passing of the Banking Secrecy Act (1970) and the Patriot Act (2001). These developments have led regulators, including the Financial Crimes Enforcement Network (FinCEN), to enact zero-tolerance policies on banks who work with third-party processors. The “Final Rule” of FinCEN requires MSPs to verify identities of legal entity customers, or the Ultimate Beneficiary Owner (UBO). As the threat of Transaction Laundering grows in the e-commerce ecosystem, federal regulators have taken notice and have started to enact stricter policies and penalties for MSPs. However, most existing, traditional KYC programs still focus on physical, rather than digital aspects of an entity, and are not capable to address the issues related to e-commerce payments. When illegal or illicit activity does slip through the cracks, the major card brands carry a zero-tolerance policy on the relationship between the violating URL and the MSP that facilitates its payment – simply, a transactional connection is the basis for fines and regulatory action.

Understanding that this risk includes the potential of high fines, fees and legal action, MSPs have responded to these pressures by assembling resources and implementing technologies and processes to better monitor merchant risk. It's imperative for MSPs and online marketplaces to be aware of the massive blind spot in their anti-money laundering and fraud mitigation methods, as this blind spot leaves them exposed to enormous regulatory and business risks.
TRANSACTION LAUNDERING THROUGH ORGANIZED CRIME & MARKETPLACES

Through e-commerce, customers on a web site choose a product, submit their credit card or digital wallet details, input their shipping details, and wait for their product to arrive. That’s the way Transaction Laundering works as well – except that the products being sold can potentially be illicit, illegal, or downright dangerous.

August 2017 – FBI Reveals ISIS Uses Transaction Laundering

The FBI revealed that ISIS was financing their domestic terror agenda in the U.S. using popular sites, eBay and PayPal. According to the FBI statement and reported in the Wall Street Journal, Mohamed Elshinawy, an American-born ISIS operative and U.S. citizen, was arrested in Maryland after he received nearly $10,000 via PayPal for fake sales of computer printers over eBay. This money was being laundered to help fund ISIS operations on a global scale.

This revelation was important because Transaction Laundering had previously been one of the least-regulated methods of online money laundering. Now that the link to terror funding is evident, Transaction Laundering is likely to show up on law enforcement radar more frequently.

November 2017 - Money Laundering through Airbnb services in Russia

The Daily Beast and BGR - recently revealed that cyber criminals are using popular online marketplaces, specifically Airbnb, to facilitate money laundering in Russia. The scam is simple: fraudsters use stolen credits cards to launder the dirty money through complicit Airbnb hosts they meet in underground, online forums. Once the Airbnb booking transaction is processed, no one actually stays at the advertised accommodation; instead the two parties split the payment and create fake end-of-stay reviews to close the transactional loop.

Exploitation of popular peer-to-peer platforms and our online sharing economy has become an increasing threat to how we legitimately do business online.

THE RISE OF THE PAYMENT FACILITATOR

Businesses of all (virtual) shapes and sizes are entering the online payment ecosystem at a record-setting pace, creating a need for speedy merchant onboarding.

Online merchant acquisition has become an increasingly volatile business with a focus on speed and volume, pressuring MSPs to seek ways to mitigate their risk while continuing to maintain growth rates. The current market puts high demand on approving merchants in real time and building large-scale portfolios to maximize business.

The creation of the Payment Facilitator model addresses this need - designed with the intent to link MSPs to smaller, “micro-merchants” through the intermediary, or Payment Facilitator, to process payments. This model is quickly becoming the preferred method for new merchants to get up and running within a few minutes, rather than previous models that can take days or even weeks. The rise of Payment Facilitators - and subsequently, millions of small businesses entering the cyber realm leaves room for ambiguity and confusion surrounding industry standards and regulations. It also leaves the MSPs vulnerable to the unknowns that can be hiding in their portfolio.
Managing merchant portfolios involves the consideration of a large number of factors, many of which fall out of the standard KYC checks. In order to fully know your merchant, be card brand compliant, regulatory compliant, and ultimately protect your business, the following are important to understand to prevent Transaction Laundering and merchant-based fraud:

- Top-level domain list of each merchant’s website for comprehensive compliance checks
- Verification of the true goods and services advertised and sold on your registered merchant’s website
- Validation of merchant category code vs. actual category of items or services offered
- Knowledge of each and every associated website to your registered merchant
- Availability of time-stamped, archived evidence of your merchant’s violations, such as illicit, illegal or out-of-policy content
- Understanding if hidden websites are funneling transactions to your registered merchants
- Awareness of any complaints or customer issues about your merchants
- Continual monitoring of the dynamic, ever-changing status of your e-commerce universe (At any time, websites can be updated and contain new associations, goods, service, payment options, contact information, etc.)
- Case management to effectively manage all suspect merchant violators through the entire investigation lifecycle
- 100% indisputable validation of Transaction Laundering

With so much to consider and keep track of, it seems nearly impossible to build these capabilities in-house and manage risk of a large portfolio of merchants. Not taking into account these above factors puts you at risk for card fines, regulatory penalties and potential brand damage. A purpose-built platform designed to address all of the above is the most effective solution to combat Transaction Laundering.

38.1% of all money laundering is now conducted through the merchant ecosystem exceeding $200 billion globally...

and it’s increasing 8.4% year over year.
DETECTION AND ULTIMATE PREVENTION WITH TECHNOLOGY

Transaction Laundering is especially worrisome for MSPs, as it is one of the most difficult to detect and monitor. Many times, the majority of KYC efforts happens only in the signup phase of a merchant. It is important to employ these monitoring practices throughout the entire lifecycle of each merchant. Ongoing monitoring of online merchants and their transactional activity helps to provide full transparency of any-sized merchant portfolio, in order to continuously validate important details like true line of business, country of operation, appropriate content, website security, etc.

Lifecycle of a Merchant:

The migration of illicit e-commerce schemes towards Transaction Laundering now involves many more unreported websites, unknown to the MSPs, thereby disrupting the streamlined risk management processes originally created.

Not only are these merchants undisclosed, the rogue merchants are actively trying to disguise any connections to these merchants, especially around the onboarding process and initial checks. With undisclosed merchants in the mix, previous methods used to inspect and validate merchants for onboarding are called into question, and ongoing monitoring initiatives become complicated and daunting.

Online fraud is dynamic and evolving, exploiting weaknesses in the e-commerce ecosystem at every turn. If you are a MSP, it will become increasingly vital to be steps ahead of the criminals to avoid fines, fees, legal action and reputational damage and to ultimately prevent Transaction Laundering.
5 MERCHANT MONITORING MUST-HAVES TO PREVENT TRANSACTION LAUNDERING

We have determined five merchant monitoring must-haves to enhance AML practices and upgrade to include new anti-Electronic Money Laundering efforts in the digital word:

1. Automated Transaction Laundering Detection: Expose hidden transaction tunnels, launderers and merchant-based fraud schemes using proprietary technology across web and mobile channels

2. Automatic Evidence Validation: Gather conclusive evidence on suspected launderers or other unregistered/unknown merchants to track the route of the entire transaction

3. True Continuous & Automated Content Monitoring: Monitor and automatically surface violations related to obscure or hidden connections to merchants on an ongoing basis

4. Complete and Custom Risk Profile: Create a 360-degree view of each merchant’s true digital identity for a complete understanding of online associations and overall ecosystem

5. Scalability: Avoid manual and time-consuming procedures - adopt a fast, frictionless system that allows you to onboard any number of merchants and continuously monitor any size portfolio

Digital problems require digital solutions. By adding advanced, technological solutions to physical vetting procedures, Transaction Laundering risk, exposure and liability can be mitigated. Processes that rely on manual merchant monitoring simply cannot keep up, pressuring the payments industry to share intelligence and actively pursue comprehensive solutions that keeps pace with advanced technology.

ABOUT US

EverCompliant is the pioneer and industry leader in Electronic Money Laundering Detection and Prevention (known as Transaction Laundering). The company’s flagship product, MerchantView™, is the first and only dedicated solution on the market designed from its core to detect and prevent Transaction Laundering. MerchantView applies proprietary cyber intelligence technology to identify unknown and hidden merchants funneling transactions through seemingly legitimate storefront websites. EverCompliant’s technology has been adopted by large-scale financial institutions and payment service providers in Asia, Europe, U.S. and the Middle East. EverCompliant is headquartered in New York City with offices in San Francisco, Shanghai and Tel Aviv.