WHITE PAPER

TRANSACTION LAUNDERING – A GROWING THREAT IN THE PAYMENTS INDUSTRY

Infosys®
Navigate your next

What is transaction laundering?

Transaction laundering is an activity through which entities, unknown to a merchant acquirer, process their payments through the facilities provided by the acquirer to a known merchant. It is a criminal activity which violates the agreement that the merchant had with its acquirer.

The method of using legitimate websites as a front is being used by criminals to conduct illegal activities, such as sale of counterfeit products, drugs and weapons trade, illegal pharmaceuticals, illicit pornography, unlicensed gambling, money laundering, and terrorism financing.

It creates a situation where Merchant Service Providers (MSP – a collection of banks, acquirers, and payment processors) unknowingly become party to illegal activities and facilitate money laundering. This not only damages their reputation, but also makes them vulnerable to excessive chargebacks, legal actions, and regulatory penalties.

Transaction laundering is sometimes referred to as ‘unauthorized aggregation’ or ‘undisclosed aggregation’ or ‘factoring’. This is because of the way illegal payments from one or more unknown sites are aggregated to be processed through a single legal merchant account. However, “aggregation” is a legitimate payments model using which small and medium businesses rely upon payment aggregators to take credit and debit card payments from their customers. Thus the term ‘transaction laundering’ became popular which indicates that the payment transaction itself is altered to launder money.

The ultimate penalty is borne by the acquiring bank of a merchant indulging in transaction laundering, either knowingly or unknowingly. Regulations require the MSP to verify the legal identity of their customers and identify the Ultimate Beneficial Owner (UBO) of that entity. However, traditional Know Your Customer (KYC) still focuses on physical aspects of the legal entity as opposed to the digital aspects, making the payments area extremely vulnerable to transaction laundering.

How big is this threat?

According to EverCompliant, which is a solution provider in this space, US$155 billion was generated from online sales via transaction laundering in 2016 in the USA alone. In addition, banks are processing about six percent to ten percent of unauthorized e-commerce sites, out of which about three percent are involved in illegal activities.

G2, another solution provider who has been monitoring merchant content for the last 11 years, has found out that an average of 1.5 percent of a client's portfolio contains illegal or unknown websites.

In fact, the Charlie Hebdo terrorist attack in Paris in 2015 was aided by transaction laundering.

According to a research by pymnts.com, more than 25 percent of terminated accounts come back into the payment system in a disguised manner with nearly no change in their operations. About 50 percent of websites involved in unlawful activities do not register for merchant accounts.

Why is transaction laundering difficult to detect?

Although this method of money laundering may seem simple, it is not very easy to detect through traditional means due to the following reasons:

1. **Complexity of the payments chain:** There can be several combinations of a payment cycle involving the shopping cart, payment gateway, payment processor, and bank where the payment may go through multiple gateways or payment processors. Hence, it is very difficult to differentiate legitimate transactions from the illegitimate ones

2. **Inability to safeguard websites:** Some merchants may not realize that their websites are being used for illegal transactions either through their affiliate programs or simply by using their website as a shadow site

3. **Numerous unreported websites:** Transaction violations maybe done through hidden websites that the bank may not know and therefore may not monitor. Traditional monitoring methods do not catch unreported websites

4. **Growing use of corporate credit cards in business to business (B2B) payments:** It has seen a growth of 25 percent till 2016 and is expected to grow at least at a rate of 10 percent y-o-y till 2018. Some of these corporate credit cards offer attractive cash backs making it a more preferred option over Automated Clearing House (ACH). Therefore, it is now common to have a large payment (running into thousands of dollars) being done via a single transaction, making it difficult to single out malicious transactions.

Why it has become an increased threat in recent years?

In recent times, the threat of transaction laundering has increased due to two primary reasons – i) rapid increase in mechanisms that aid in this activity, and ii) the checks to detect them are unable to keep pace.

1. Factors that aid transaction laundering:

a. Creating a professional-looking website to sell goods along with a checkout page and credit card profile has become very easy enabling criminals to create an online marketplace swiftly. Criminals do not have to create actual brick-and-mortar storefronts to launder money. Thus, all three steps of money laundering – placement, layering, and integration can be done digitally

b. There has been a substantial growth in e-merchants and payment facilitators which provide a good degree of anonymity

c. Banks have outsourced the high-cost customer and merchant acquisition to payment service providers and facilitators, who do not have the same degree of risk management and monitoring capabilities

d. There has been a sudden surge in alternate payment methods, such as digital wallets, payment processors, and payment gateways, which do not have a very good monitoring solution, giving a fraudster newer avenues to launder money

e. It has become an attractive avenue to generate additional revenue, either through abuse of affiliate programs or by being complicit to the crime along with a launderer

2. Factors that do not deter enough:

a. Fraudsters are finding it difficult to launder money through traditional means (cash, wires, ACH) given the sophisticated and mature monitoring systems that exist for such payment methods. However for credit cards, the focus has typically been on frauds as opposed to money laundering

b. Current regulations are attuned largely to lines of business such as banking, capital markets, and insurance or products such as wires, cash deposits, and securities trading. Payments and 'card not present' credit card transactions are the blind spots in the world of anti-money laundering (AML)

c. Merchant acquirers are not governed by the same level of Bank Secrecy Act (BSA) / AML requirements as those of banks. They focus on monitoring transactions for chargebacks only, instead of money laundering

What are the types of transaction laundering?

Transaction laundering can be done in various ways and its typical growth trend is given in Exhibit 1.

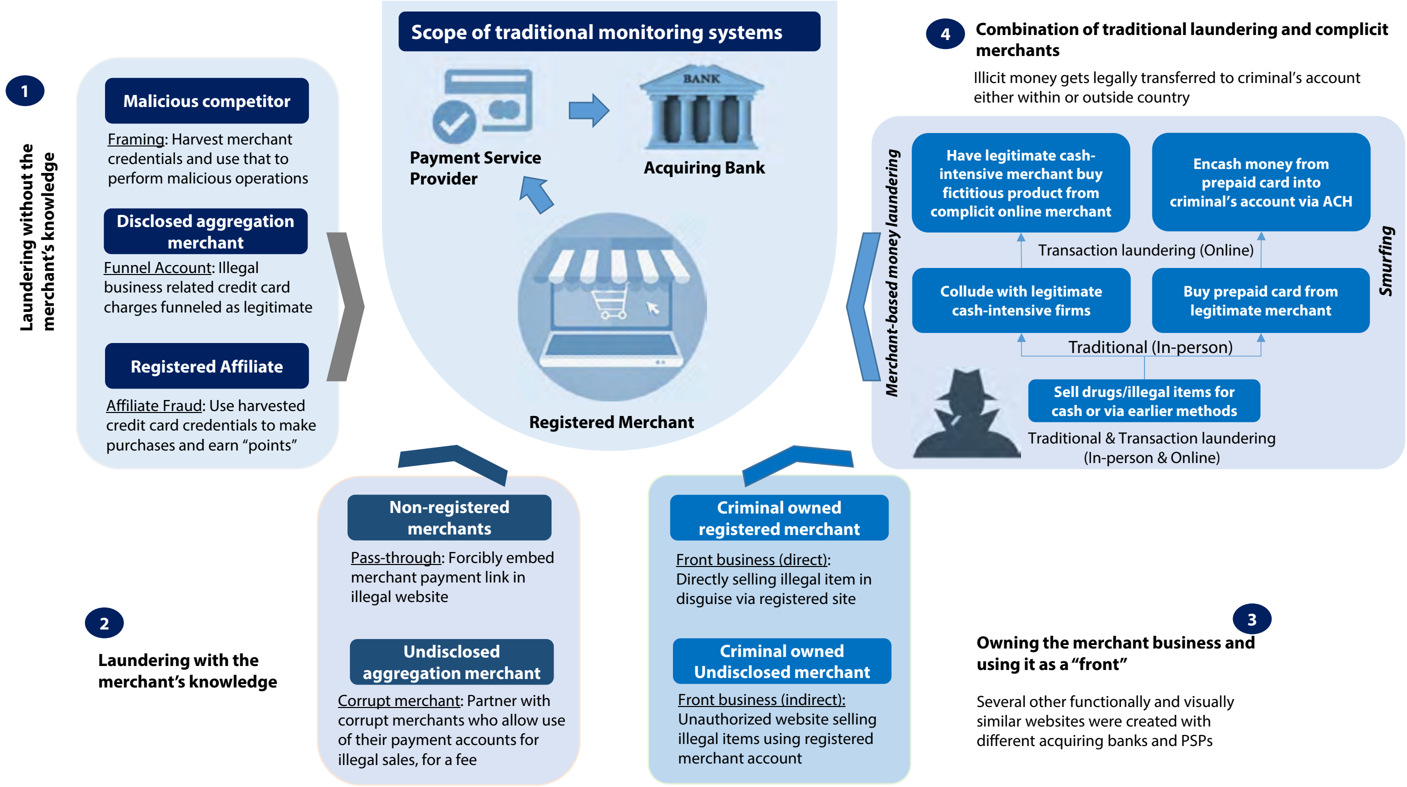
Scope of traditional monitoring systems
Payment Service Provider
BANK
Acquiring Bank
Registered Merchant
1
Laundering without the merchant's knowledge
Malicious competitor
Framing: Harvest merchant credentials and use that to perform malicious operations
Disclosed aggregation merchant
Funnel Account: Illegal business related credit card charges funneled as legitimate
Registered Affiliate
Affiliate Fraud: Use harvested credit card credentials to make purchases and earn "points"
2
Laundering with the merchant's knowledge
Non-registered merchants
Pass-through: Forcibly embed merchant payment link in illegal website
Undisclosed aggregation merchant
Corrupt merchant: Partner with corrupt merchants who allow use of their payment accounts for illegal sales, for a fee
Criminal owned registered merchant
Front business (direct): Directly selling illegal item in disguise via registered site
Criminal owned Undisclosed merchant
Front business (indirect): Unauthorized website selling illegal items using registered merchant account
3
Owning the merchant business and using it as a "front"
Several other functionally and visually similar websites were created with different acquiring banks and PSPs
4
Combination of traditional laundering and complicit merchants
Illicit money gets legally transferred to criminal's account either within or outside country
Merchant-based money laundering
Smurfing
Have legitimate cash-intensive merchant buy fictitious product from complicit online merchant
Encash money from prepaid card into criminal's account via ACH
Transaction laundering (Online)
Collude with legitimate cash-intensive firms
Buy prepaid card from legitimate merchant
Traditional (In-person)
Sell drugs/illegal items for cash or via earlier methods
Traditional & Transaction laundering (In-person & Online)

Exhibit 1: The evolution of transaction laundering

1. Merchant is unaware

a. Framing: A company / entity with malicious intent creates an illegal website and reports it to a card network to provoke a test operation. When this transaction is executed, the entity harvests the credentials and uses this to place an order from its competitor's site, thus 'framing' the innocent merchant.

b. Funnel account: The legitimate merchant accepts credit card charges from another company that does not have merchant processing accounts (regular aggregation). However, this company may be indulging in illegal business. These credit card charges are funneled into the payment processing engines as legitimate.

c. Affiliate fraud: An affiliate of a legitimate merchant may use the site to make fictitious or non-fictitious purchases using harvested credit card credentials and earn affiliate commission points.

2. Merchant is aware and complicit

a. Pass-through company: A company with legitimate business is forced to take on an illegitimate entity to use its account. This malicious entity embeds the legitimate merchant's payment link on its website using it to accept payments against sale of illegitimate goods. They may often give a certain percentage cut of the processed amount to the legitimate merchant.

b. Corrupt merchant: There could also be merchants with real businesses such as phone accessories, but have partnered with an organization to process illegal transaction to earn extra revenue.

3. Merchant owned by a criminal syndicate

A criminal syndicate can open various real businesses (often innocent and low-risk such as clothing store and a toy store) to act as a 'front' to launder illegal substances.

i. Front business (direct): This is where the 'front' business can openly sell illegal substances using a masked name through the website. For example, a food ingredient company selling banned drugs via a masked name through its website.

ii. Front business (indirect): This is where the syndicate creates a shadow site selling illegal items using the license provided for the legal 'front' business. For instance, a pharmacy in the UK obtained license to sell legitimate drugs online and displayed the government-authorized EU common logo to depict authenticity. It did not allow foreign orders to be processed since it had only UK license and also did not allow prescription drugs to be sold without valid prescription from an in-person medical evaluation. However, it also created a shadow website that sold prescription drugs without prescription and allowed such drugs to be shipped outside

UK, using the same merchant account to process customer payments. The EU common logo is displayed on both the real and shadow websites which tells the payment providers, e-commerce platforms, other intermediaries, and patients that both websites are legal.

4. Combination of traditional laundering and complicit merchants

In all the above examples, the laundering activity is largely happening online. However, in recent times, unsuspicious activities through brick-and-mortar stores combined with transaction laundering done via complicit merchants have made this activity extremely difficult to detect. This seems to be the preferred method of cross-border crimes.

a. Merchant-based money laundering [Transnational Organized Crime (TOC)]

Merchant-based money laundering is a process where goods / services being paid are either under-valued or not present at all (phantom transactions / shipments). For example, the drug mafia in Mexico actually provides a "line of credit" to wholesale buyers in the US. These wholesale dealers then sell drugs using any of the mentioned methods or via direct cash transactions. The revenue generated is then sent back to Mexico via another transaction laundering method called merchant-based money laundering.

The crime syndicate ties up with cash-intensive businesses such as supermarket, vending machine operators, convenience stores, restaurants, private ATMs, cigarette distributors, liquor stores, parking garages, and others. They either collude or coerce the cash-intensive businesses to mingle the illegitimate cash with their legitimate cash for a fee. The cash-intensive business is then instructed to make regular purchases from specific merchants in Mexico on a regular basis, via which the illegitimate money gets transferred across the border. The Mexican merchant, on its part, may not actually ship anything at all, given that the purpose of the transaction was to transfer the illicit money and not for any real business need.

b. Prepaid gift card 'smurfing'

This method is known to have been used by terror groups to fund their operations (for example, the Paris attack in November 2015). In this method, a criminal syndicate can employ some people (smurfs) to purchase low value prepaid gift cards from different stores (retailer) and then load these cards with low sums of money every day, making sure that each card is loaded after a requisite gap in time. In this way, illicit money gets loaded into prepaid gift cards which is then legalized by transferring this money to a bank account via ACH. The 'smurfs' are careful to deal with amounts below the Continuous Transaction Reporting (CTR) threshold of US$10,000.

Normally, the retailer does not ask for documentation from people who purchase or load prepaid cards with amounts equal to or lower than $500 in the US and GBP 250 in the UK.

The regulatory view of transaction laundering

- In the US, transaction laundering comes under the ambit of Financial Crimes Enforcement Network (FinCEN), Federal Financial Institutions Examination Council (FFIEC), and Consumer Financial Protection Bureau (CFPB) where they see transaction laundering as a variation of the AML themes. One aspect that FinCEN is struggling with is the way to frame rules for cross-border prepaid card smurfing. Today, open-loop prepaid cards are not subjected to the cross-border reporting requirement of US$10,000. The agency is trying to balance rules around this, with political, economic, and logistical hurdles.
- The European Union has already passed the 4th AML Directive (AMLD) and the 5th AMLD is in the process. Europe has put in measures around performing transaction and business relationship monitoring even for simplified Customer Due Diligence (CDD) cases, extending the scope of AMLD to virtual currencies and wallet providers. Standard or enhanced CDD to be performed on e-money products (prepaid cards) regardless of the amount and whether they are reloadable (simplified CDD to be done only for non-anonymous, non-reloadable under EUR150 prepaid cards) and transparency around beneficial ownership of companies and trusts.

However, one thing that all the regulations lack is a clear focus on how to implement these increased directives and rules. The regulations put more focus on unusual, complex transactions with no apparent purpose or transactions involving high-risk countries. However, transaction laundering happens in transactions that do not appear to be unusual or unlawful at first sight. Hence, the regulatory bodies also need to do more to counter this threat.

What can MSPs do better?

1. Banks tend to categorize business of their customers as high risk or low risk and base their monitoring activities on this customer risk score. However, very low-risk businesses can actually be fronts for transaction laundering. Therefore for detecting transaction laundering, non-traditional methods of monitoring and investigation are required.

2. There needs to be a way by which banks can monitor the cash deposits of a business along with its credit card activity with inputs from the merchant acquirer to be able to create a full picture of potential money laundering.

3. Focus on AML on credit cards rather than the fraud on credit cards alone. Just as there are red flags for credit card fraud, there needs to be red flags for money laundering using credit card. Some examples could be:

   a. In terms of amount, customers or items, is the transaction in alignment with historical transactions?

   b. Is the merchant procuring items internationally when they are available locally? If so then why?

   c. Are the items being purchased in line with the merchant's regular line of business? Example: Is a fruit seller trying to sell high-end electronics?

   d. Is there any hard evidence that although the payment was made, the item was indeed shipped?

4. Acquirers can take additional steps during the underwriting process to identify merchants who are indulging in or are likely to indulge in transaction laundering.

   a. Perform advanced due diligence on merchant website such as vetting backlinks to the site and identifying websites that use the same server or have common ownership to the merchant applicant

   b. Carry out click origination investigations and behavioral monitoring across the entire merchant portfolio

   c. Impart training to all departments in the organization (such as sales, chargeback, processing, etc.)

   d. Perform site visits, examine merchant balance sheets and profit and loss (P&L), seek testimonials, and conduct surveys

5. Typically, third party payment processors and merchant acquirers are not subject to formal AML regulations. They should, however, start monitoring transactions from a money laundering perspective. Acquiring (sponsor) banks should consider providing transaction laundering tools to their sponsored Independent Sales Organizations (ISOs).

6. The merchant acquirer can run analytics on the type of merchants they have and the average credit card processing volumes per month for each. They can see if there are certain outlier merchants whose prepaid card processing volumes are higher than the rest in the same category.

7. While the merchant / retailer themselves do not have rules to collect identification information of people who transact in lower sums of money on a prepaid card, there can be a system built and used where amount of money being loaded in a prepaid card is added and tracked. The destination accounts where the money on this card is used can also be tracked, so as to build a network of the way money travels on a given prepaid card.

What are the solutions available in the market today?

By and large, combatting transaction laundering will require a combination of merchant and transaction profiling solutions combined with criminal databases and human investigation. There are a few vendors with transaction laundering solutions. Largely, their solutions revolve around merchant website profiling and searching for certain characteristics and perform behavioral analytics. They could also inspect transactions conducted on suspicious-looking websites (a database that is built over time) and then try to link it back to the merchant acquirer which processed the transaction. Some of the products in the market are shown in the Exhibit 2 below.

WEBSITE & CYBER ANALYTICS BASED

EverCompliant "Merchant View" **– It is a solution to detect and prevent transaction and money launderers, hidden transaction tunnels and merchant fraud from entering the ecommerce ecosystem by leveraging cyber intelligence. In 2016, they added an additional capability in MerchantView. The new platform is now able to detect hidden mobile apps and fraudulent mobile payments being processed through legitimate merchant accounts. It also reveals related and unreported mobile applications, URLs, payment environments and provides the tools to manage risk on an ongoing basis.**

ControlScan SiteWatch (EverCompliant's US partner) - SiteWatch not only detects content violations on reported websites, but also helps detect unreported and unauthorized URLS associated with known merchants. It helps in assessing merchants, ongoing review of existing merchants, detecting web presence for merchants with no reported websites and special investigations. Its solution is cloud-based with a SaaS delivery model. It has a partnership with EverCompliant.

BEHAVIORAL ANALYTICS BASED

Zero Score - ZeroScore™ Transaction Laundering Detection service is a solution that will work without being tightly integrated with the acquirer or payment facilitator and seamlessly detect Transaction laundering. It monitors user behavior and traffic flow together which when passed through highly developed algorithms alerts the acquirer or payment facilitator of possible Transaction laundering in real time. This solution is used by MasterCard.

Trustwave's Transaction Laundering Detection **– It helps acquirers, banks, payment processors, ISOs closely monitor their merchant websites for illegal activities. It doesn't just examine the merchant's transaction summary or the site's URL and SSL configurations but also keywords, language and images on the site.**

DATABASE & WEBSITE ANAYTICS BASED

G2 Transaction Laundering Detection – This is a service that combines data, technology and expertise. It has a database called Merchant Map™ with 11 years of data on merchants and criminals. It also has tools that run analytics on transactions, website and traffic and a group of data scientists and analysts who verify violations, and continually identify patterns and fine tune detection methods.

Exhibit 2: Products in the Market

Conclusion

Merchant acquirers and major card brands do not come under the same regulatory purview as regular banks do. However, this blind spot is now being misused by criminals. There is a definite cost involved in implementing sophisticated monitoring and analytics engines. However, payments industry can actually benefit society in a much larger way if they actually start reporting suspicious activities while also improving their reputation in a proactive manner.

At the same time, there is an equally important role for the regulatory bodies to play in determining the manner in which directives are followed and the consequences to the perpetrators when caught, thus closing the loop of arresting transaction laundering.

About the Author

Kasturi Chattopadhyay

Global Delivery Partner, Financial Services Application Development & Maintenance, Infosys Limited

Kasturi has over 18 years of delivery and consulting experience in the financial services industry. Currently she is the Global Delivery Partner for a key client of Infosys. Until recently, she headed the Financial Services Risk and Compliance practice for the Americas in the Infosys' Domain Consulting Group.

Over the years, she has worked with several financial institutions to identify the pain points, and architect transformation programs and projects that involved both business process transformation and product/ technology assessment & implementation - in the areas of financial crime management (AML and fraud), regulatory compliance, and enterprise risk. She has also helped financial institutions adopt new-age paradigms such as robotic process automation, artificial intelligence, and machine learning.

References

http://www.acfcs.org/news/307150/Merchant-based-money-laundering-part-1-Phantom-Shipments.htm

https://www.acfcs.org/news/328136/Merchant-based-money-laundering-part-2-Prepaid-gift-card-smurfing.htm

http://www.lexology.com/library/detail.aspx?g=972e73e4-a663-4aff-a38a-5053b457a23f

http://evercompliant.com/transaction-laundering-new-advanced-form-money-laundering/

http://zeroscore.com/PDF/ZeroScore_TLD.pdf

https://www.g2webservices.com/cleaning-out-transaction-laundering/

https://www.g2webservices.com/acquiring/g2-portfolio-protection/transaction-laundering/

https://www.legitscript.com/wp-content/uploads/2016/07/LegitScript-Report-on-Chemist4U-Transaction-Laundering.pdf

http://www.thepaypers.com/expert-opinion/transaction-laundering-101-what-banks-and-msps-should-know/767506

http://controlscan.com

http://finance.yahoo.com/news/controlscan-helps-shed-light-emerging-130000347.html

https://ftalphaville.ft.com/2017/03/17/2186157/why-transaction-laundering-is-turning-into-a-huge-financial-blindspot/

http://www.pymnts.com/exclusive-series/2015/what-banks-and-processors-must-know-about-transaction-laundering/

https://www.linkedin.com/pulse/new-age-money-laundering-nadja-van-der-veer

https://www.linkedin.com/pulse/new-age-money-laundering-2-nadja-van-der-veer?published=t

https://www.iconfinder.com/icons/332100/buy_e-commerce_ecommerce_laptop_macbook_market_mouse_online_shop_online_store_order_purchase_shopping_store_web_shop_web_store_icon

https://www.boundless.com/sociology/textbooks/boundless-sociology-textbook/deviance-social-control-and-crime-7/the-symbolic-interactionalist-perspective-on-deviance-64/differential-association-theory-381-8939/

https://financesonline.com/15-popular-payment-gateway-solutions-one-best/

www.psdgraphics.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected SlideShare