Transaction Laundering Case Study: The “Spice” Syndicate

Transaction laundering has become a confounding problem for risk managers. Sometimes referred to as “unauthorized aggregation” or “factoring,” the practice occurs when unknown, often illicit, businesses process payments through merchants both known and unknown to acquirers or their downstream partners. Transaction laundering allows prohibited goods and services to enter the payment system, violating the merchant's agreement with its acquirer, flouting anti-money-laundering (AML) laws and attracting the attention of regulators. Transaction laundering is being taken very seriously by card networks globally. By not addressing transaction laundering, acquirers are exposed to a substantial risk for fraud, brand damage, and assessments.

Transaction Laundering: Understanding the Threat

A food ingredients company selling spices and other food products was onboarded by an acquirer. It utilized a simple but effective web design that merchandised peppers, confections, rare seasonings, and other culinary items. Prices were high, but not unreasonable. At first glance it seemed to be just another new online business, and the acquiring bank had no reason to question its legitimacy.

It was soon discovered, however, that the food merchant was laundering for a site selling the drug *spice* (see *Figure 1*). This slang term refers to dried plant matter laced with synthetic (or designer) cannabinoid compounds meant to mimic the effects of high-potency THC. The chemicals used in spice have a high potential for abuse, no medical benefit, and can cause serious side effects including auditory hallucinations, paranoid delusions, and aggressive behavior.

Other risks and adverse consequences are unpredictable, with symptoms lasting several days, or even weeks in some cases. Usually our bodies deactivate a drug as it metabolizes it, but this is not the case with spice. CB1 receptors in the brain stem become overloaded, causing cardiac, respiratory, and gastrointestinal problems that result in an overdose. Reports of kidney failure and seizers are not uncommon. The drug can leave patients catatonic and listless, and result in hospitalization and death. The DEA has designated the five active chemicals most frequently found in spice as *Schedule I Controlled Substances*, making it illegal to sell, buy, or possess them. The United Nations Office on Drugs and Crime (UNODC) recently released a report reaffirming that these compounds are illegal in many countries worldwide, including England, Germany, France, Italy, Japan, and Demark.

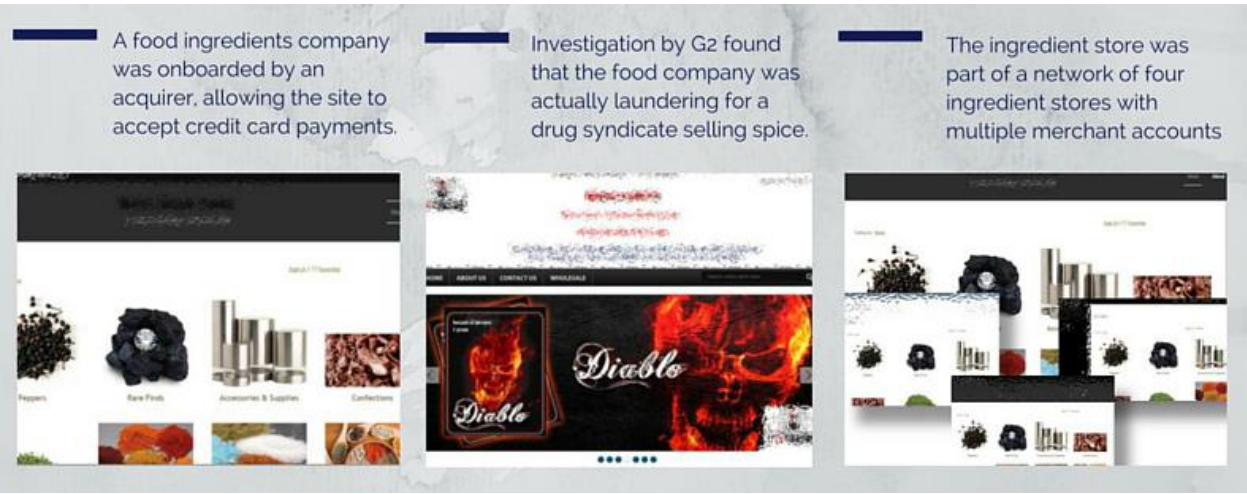


Figure 1

When G2 delved deeper, the problem was larger than originally anticipated. This ingredient store was in fact part of a network of four functionally and visually equivalent ingredient stores with multiple merchant accounts. One site was active, and three were dormant. To make matters worse, there were five additional active violating sites through which the drugs were also being advertised and sold. And three more sites ready to be activated at will *(see Figure 2)*. This syndicate had positioned itself with a safety net to ensure its criminal enterprise could carry on in the event that one or more sites were ever terminated.

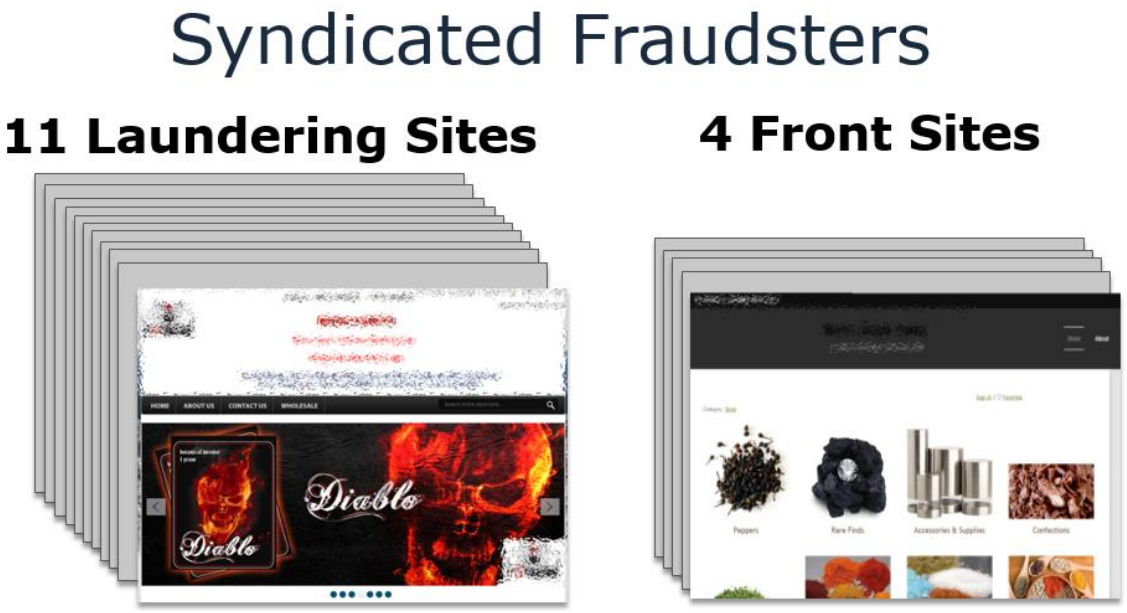


Figure 2

Spice Syndicate: One Step Back, Two Steps Forward

The merchant account was shut down immediately. The involved acquirers were pleased with the results, and they deserved to be. An illegal drug seller was denied the ability to process credit card payments online, and the acquiring bank avoided penalties from regulators and card brands. Unfortunately, the violators were not done yet. The operation came back online, processing through a separate merchant account, at first accepting one card brand. Then, two months later, they were back to accepting four cards again. This was merely a speed bump in the road for the offenders.

The syndicate also began relabeling its products as *herbal incense, Matrix, K-2, spice incense* and *potpourri*. These are other references to the drug *spice* that customers would recognize but acquirers might overlook during the onboarding process. By renaming products, the culprits relaunched without initial detection from their new acquiring bank.

The most cunning method of all was to bypass conventional authorization and the settlement processes all together on some sites by requesting that buyers enter their payment information directly into the shipping section, or request an "invoice" via email. This enabled rekeying of orders elsewhere, such as through virtual terminals.

In this specific case, the criminals won in the short term. They adjusted their tactics to continue operations, skirting detection by using both separate and new merchant accounts, and further exploring alternative routes for processing payments.

Fortunately, the illicit victory was to be short-lived. G2 had been monitoring the sites to see if the syndicate would resurface. When it did re-emerge with different acquirers, G2 informed the organizations so they too could terminate the accounts.

Spice might look similar to organic cannabis, but the potency is more than ten times greater than THC. Research has shown that our bodies have a decreased ability to deactivate the drug as it metabolizes, which damages our CB1 brain receptors.

Ever Growing Global Risk

In an effort to further present these stores as legitimate businesses, some sites list products as being 100% legal, which is untrue, and could confuse consumers who may not know exactly what is being sold. Other consumer-friendly messaging includes false claims that the products *"contain no banned chemicals"* and *"are not intended for inhalation"* to disguise the true purpose.

The offenders also utilize branding using a range of names and characters that infringe on copyrights and trademarks, which could open the door to further liability throughout the payments chain. Even worse, many of these products feature cartoons marketed at children. *Scooby Doo*, *Alice in Wonderland*, *Angry Birds*, and *SpongeBob SquarePants* are just a few that have been featured on packaging *(see Figure 3).* Further blurring the lines, these fraudsters regularly highlight products as being *limited-edition* or *collector's items*, recklessly aligning the drug with toys and collectables in the minds of unsuspecting buyers. Beyond the potential for brand damaging activity to acquirers and partners, transaction laundering of drug sales is a serious threat to overall public health, especially for children. In 2014 a rash of overdoses triggered by the use of spice prompted a state of emergency in New Hampshire. Governor Margaret Hassan stated that, "Retailers that continue to knowingly sell these illegal products are placed on notice that they could be held responsible for harm caused to users." Civil wrongful death lawsuits have been filed against manufacturers, processors, and partners involved in the selling of these drugs in many US states. Following an ABC News report that emergency calls related to the drug reached an all-time high this year, card brands and regulators alike have taken heightened steps toward identifying merchants.

Figure 3

A Web of Payments Activity

E-commerce has produced a multitude of new payment methods: e-wallets, virtual currency, mobile, wearables and more are being added all the time. Unfortunately, it has also yielded a horde of new fraud categories. An increasing number of prohibited merchants have found safe passage into the payment system by exploiting valid merchant accounts. It's important to realize the industry is not only dealing with sole practitioners. Transaction laundering can be bought and sold as a service. Violating transactions can enter in multiple places along the payments chain and use different payment methods. Life would be easier if all transactions flowed through payment systems in a consistent way, but they don't *(see Figure 4)*.

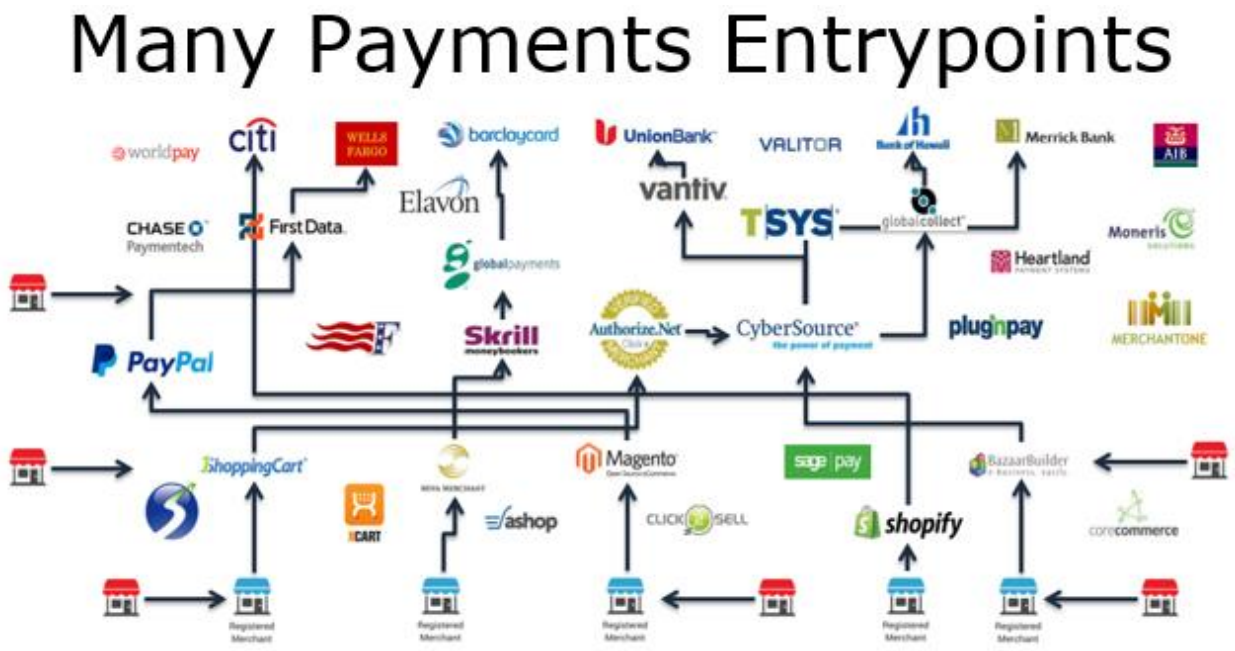
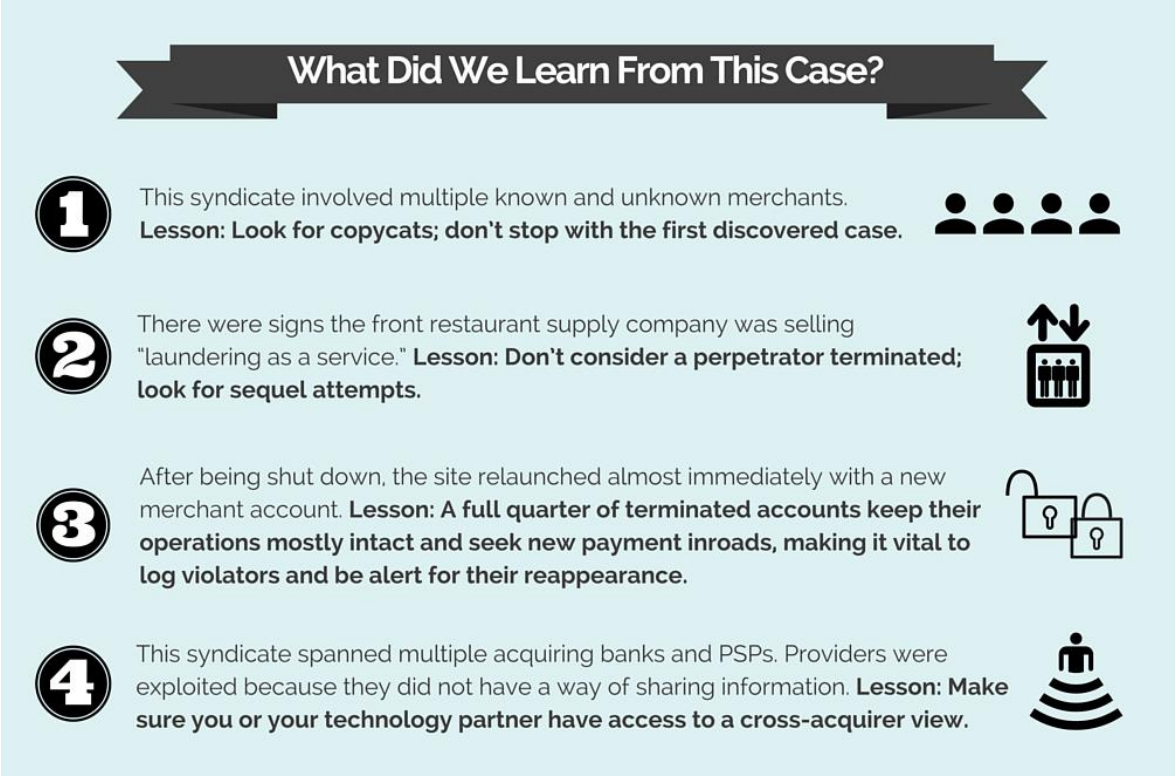


Figure 4

Due Diligence is Your Arsenal

Without transaction laundering detection, acquirers are exposing themselves to regulatory penalties and card network fines (for banks), and the loss of sponsor banks (for downstream partners). Industry best practices for identifying transaction laundering help acquirers to protect themselves from these unknown violators. Working with technology, human analysis, and a provider that offers a full view of a merchant, acquirers can work towards a complete solution to threats. Through the last 11 years of monitoring merchant content, G2 has found that on average 1.5% of clients' portfolios contain offending websites. Some will carry more, some less.

The only way to defeat launderers is to be eternally vigilant. Bad actors have evolved, broadening their capabilities to make it harder for financial and legal establishments to detect. To efficiently identify and eliminate transaction laundering in your portfolio, you must use a mixture of technology and human expertise to pinpoint the highest risk factors present in transactions. The key challenge is separating laundered transactions from legitimate transactions.



Cleaning Out Transaction Laundering

G2 Web Services is a global technology and services company that helps banks, processors and their partners ensure safer and more profitable commerce. Clients representing over half of merchant outlets globally use G2's solutions to identify bad actors and keep them out of the payments system. Widely regarded as the market leader, G2 helps clients confidently handle known and unknown threats and manage changing rules and regulations.

G2 Web Services recently released a new guide called *Cleaning Out Transaction Laundering* for risk and compliance leaders. The paper further demonstrates why transaction laundering deserves greater attention by financial institutions.

Visit G2WebServices.com for more information on transaction laundering. Contact G2 Web Services at info@g2webservices.com