The Top 10 High-risk Trends in Payment Processing and E-commerce

Updated With the Latest Trends for 2025 and Beyond

Guide

LegitScript

Successful approaches to risk mitigation in payments must take into consideration the ever-shifting nature of risk. Advancing technologies, changing regulations, criminal innovation, and new products are all factors that impact the strategy and focus of risk and compliance teams. Navigating this dynamic landscape can be both difficult and time-consuming. LegitScript keeps abreast of these trends to help our partners stay in compliance and reduce the risk of expensive card network fines.

LegitScript

In this updated guide for 2025 and beyond, LegitScript shares new high-risk trends that companies engaged in online transactions should be aware of to avoid expensive assessments levied by card networks for violations. You will also see case studies of problematic merchants and find additional resources to help answer common questions about these trends and how to navigate them.

TOP 10 HIGH-RISK TRENDS

DRUGS

Trend
1

Compounded GLP-1 Drugs

Glucagon-like peptide-1 receptor agonists, commonly referred to as GLP-1s, are a type of medication used to treat type 2 diabetes and obesity. Common brands include Ozempic, Wegovy, and Mounjaro. Their effectiveness at facilitating weight loss led to a shortage of the drugs in 2024, which prompted the FDA to allow compounders to prepare compounded versions if they met certain requirements.

While compounded GLP-1s have increased access, it has correlated to an increase in problematic merchant behavior. LegitScript tracks online activity across major platforms, and our monitoring of online ads has revealed a more than 200% increase in violative or problematic GLP-1-related ads in the first half of 2024 compared to all of 2023, and a roughly 1200% increase compared to all of 2022. This includes GLP-1 medications being promoted in jurisdictions where advertisements for prescription medicines are disallowed and, even more alarming, ads offering the medication entirely without prescription requirements.

In late 2024, the shortage ended for some brands of GLP-1 drugs, which has forced compounding pharmacies to stop manufacturing the drug in most scenarios. The cessation of these lower-cost compounded versions may drive consumers to seek cheap but potentially dangerous unauthorized versions. Already we have seen an increase in unauthorized, unapproved, and counterfeit versions of GLP-1 medications.

GLP-1 Case Study

LegitScript has seen many manufacturers and sellers of illicit peptides and anabolic steroids pivot to offering GLP-1 drugs. In this example, a rogue healthcare merchant known to LegitScript markets semaglutide under the brand names Belzempic and Beljaro, manufactured by Beligas Pharmaceuticals. While seemingly legitimate, this manufacturer states that it is the supplier of human growth hormone, peptides, and anabolic steroids to many rogue internet pharmacies known to LegitScript.

What to Watch Out For

- Check to ensure any merchant offering GLP-1s requires a prescription.
- Compounded drugs are not FDA-approved; be wary of any company claiming to have compounded GLP-1 drugs that are FDA-approved. There are also no FDA-approved generic versions of these products.
- For telemedicine websites, look for the dynamic LegitScript seal, typically located in the footer. This shows that the company has been LegitScript-certified for demonstrating compliance.
- Legitimate pharmacies and telemedicine providers generally accept standard payment methods like credit cards; uncommon forms of payment such as wire transfers or cryptocurrency may be a warning sign.

NICOTINE

Trend

2

Flavored Nicotine Pouches

The startling rise in popularity of nicotine pouches is reminiscent of the surge in popularity of vaping. The pouches, which are small and dissolvable, contain nicotine and are often marketed as a smokeless alternative to smoking. While chewing tobacco is usually placed between the cheek and lower lip near the back of the mouth, nicotine pouches are typically placed between the upper lip and the gum, allowing nicotine to absorb into the body. The pouches often contain large amounts of nicotine that can be either synthetic or derived from tobacco.

Because nicotine pouches come in a variety of flavors that may appeal to youth, they have drawn intense regulatory scrutiny. In 2024, the Food and Drug Administration (FDA) issued warning letters to more than 120 retailers that engaged in the underage sale of nicotine pouches between October 2023 and February 2024. This included online merchants, who the FDA cited for the sale of unauthorized ZYN nicotine pouches, a popular brand that sells flavors such as Espressino, Black Cherry, Lemon Spritz, and Cucumber Lime.

Nicotine Pouches Case Study

In April 2024, the FDA issued a **warning letter to EPD International S.R.O.,** the parent company of Snussie, a website engaged in the sale of nicotine products. In addition to selling nicotine pouches with flavors that may appeal to youth, the FDA noted that, under the Federal Food, Drug, and Cosmetic Act, new tobacco products — which include any tobacco product that was not commercially marketed in the United States as of February 15, 2007 — must have a premarket authorization order in effect. The letter pointed out that ZYN products lack a marketing authorization order and are therefore subject to enforcement action.

What to Watch Out For

- Always read a product's ingredient label to see if it contains nicotine. Many nicotine products today — **like pouches, gels, and dissolvable tobacco** — may be harder to spot because they don't look like cigarettes or vaping devices.
- Check to see if a nicotine product has premarket authorization. If it does not, it is likely subject to enforcement action.
- Avoid nicotine products with flavors that may appeal to youth, as these pose the greatest risk of drawing regulatory scrutiny.

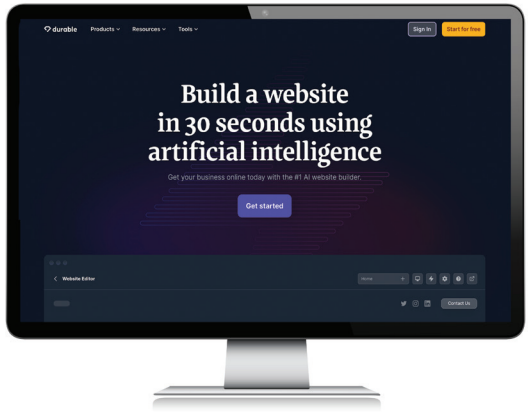
FRAUD

Trend
3

Generative AI Fraud

Artificial intelligence (AI) serves many functions. Among them is generative AI, which employs machine learning to create original content based on user prompts. The power of generative AI is in its ability to quickly create realistic content. As with any promising new technology, bad actors often direct its potential toward fraudulent and other problematic purposes.

LegitScript has been watching for fraudsters using generative AI to create realistic content to deceive payment service providers. For example, fraudsters can use AI to generate fake merchant account information and merchant applications en masse, potentially flooding payment facilitators that offer seamless onboarding. They can also use generative AI to quickly spin up realistic merchant websites for use in scams or transaction laundering



AI Fraud Case Study

AI-powered chatbots like ChatGPT can in seconds turn out text-based content, such as falsified merchant account details. LegitScript already sees **synthetic identity fraud** as a critical issue facing payment service providers, especially ones offering seamless onboarding. AI may supercharge this kind of fraud.

But that's just one concern. Web design companies like the one featured here are using AI to quickly generate custom websites in seconds. We expect to see transaction launderers making use of these websites to create detailed, more authentic-looking front businesses in record time. These highly custom front websites may be harder to discern than the clunky template-based websites we typically see.

What to Watch Out For

- The best protection against this type of merchant fraud is having strong know your customer (KYC) measures.
- It's also important to devote investigative resources to pattern detection, especially with email addresses and phone numbers. These pieces of merchant data are often more difficult to plausibly match to an identity and can be a weak point in a synthetic or AI-generated identity.
- Partner with companies like LegitScript that offer effective **onboarding tools**.

REPUTATIONAL HARM

Trend

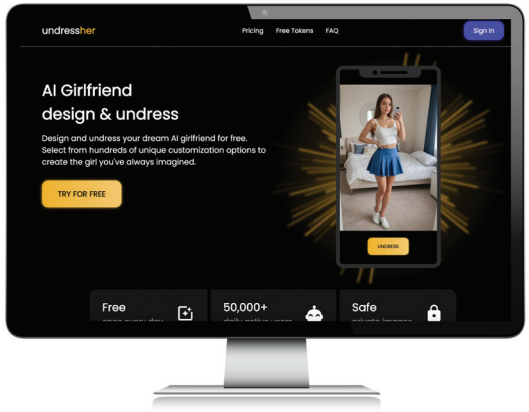
4

Generative AI Pornography

Generative AI can do more than create text. It is becoming increasingly sophisticated at creating realistic images, video, and audio. While fraud has been front of mind for most payments companies, LegitScript has also seen merchants offering generative AI solutions that may pose reputational harm.

Primarily we see this with merchants offering services that allow users to create realistic photos and videos. Without proper content moderation, customers can use these solutions to create deepfakes for misinformation, audio to impersonate people for scams, and pornographic images and videos, including child sexual abuse material (CSAM).

Computer-generated pornography is an emerging area for concern that is drawing intense scrutiny from the media, the public, and card networks.



AI Pornography Case Study

Widening access to AI technology has caused a surge in generative AI platforms geared toward creating highly custom pornography. The website featured here markets an "AI girlfriend" that users can design and undress. The reputational risk of such websites is obvious, and they can be subject to card network fines for offering non-consensual adult content that is computer generated. Not all platforms are so explicit as the merchant featured here, and so it is important to carefully scrutinize each one.

What to Watch Out For

- If a merchant is offering a generative AI solution, ask what safeguards they have in place to prevent their software from being used for fraud, IP infringement, or illicit pornography.
- Search online forums and platforms such as Reddit to look for evidence of a merchant's generative AI solution being misused.
- Read reviews of a merchant's generative AI solution to see if anyone has complained about a customer misusing it.

UNAPPROVED PRODUCTS

Trend 5

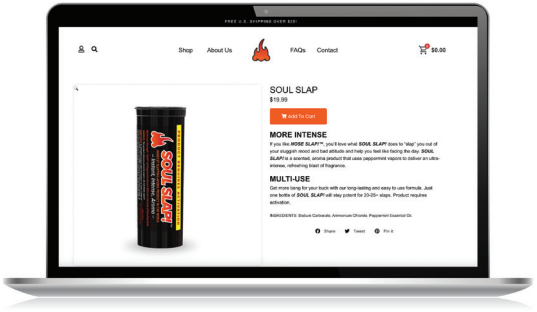
Smelling Salts

Smelling salts have a long history, with documented use going back hundreds of years. They have been used to quickly restore alertness to avoid fainting and are known most for their use on women in the Victorian era whose tight corsets were causing them to swoon. In modern times, smelling salts have also been used on athletes who have sustained head injuries.

While historical smelling salts comprised any number of ingredients, most modern products are, according to **an article** in the British Journal of Sports Medicine, "preparations of ammonium carbonate ((NH4)2CO3H2O) and perfume, sniffed as a restorative or stimulant." They are effectively scented ammonia.

LegitScript has seen an increase in merchants selling smelling salts for quick alertness, often marketing for use at the gym before exercise, at work to stave off afternoon drowsiness, and while driving to help stay alert. They are sometimes marketed as a caffeine alternative.

The FDA **has warned consumers** against inhaling ammonia for alertness and energy boosting. The agency has stated that inhaling ammonia "can quickly lead to coughing, airway constriction, and eye, nose and throat irritation." Reports of adverse events include shortness of breath, seizures, migraines, vomiting, diarrhea, and fainting.



Smelling Salts Case Study

The FDA has issued a number of **warning letters** to companies marketing these unapproved stimulants, including Nose Slap LLC. The agency described the company's products, Nose Slap and Soul Slap, as "unapproved new drugs introduced or delivered for introduction into interstate commerce in violation of section 505(a) of the Federal Food Drug & Cosmetic Act."

What to Watch Out For

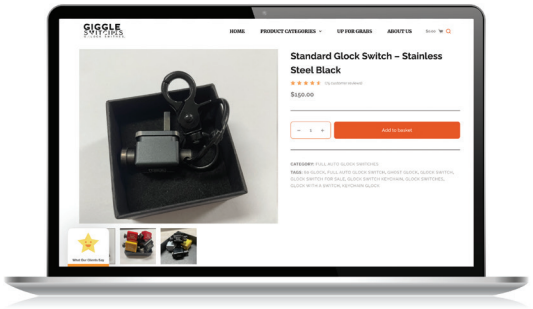
- Beware of merchants selling any inhalable ammonia product.
- If merchants offer caffeine alternatives that promise alertness, be sure to check the ingredients of the product.
- Read the marketing claims on the website and product labels to ensure there is no language indicating that the product is meant for use in the diagnosis, cure, mitigation, treatment, or prevention of disease, or intended to affect the structure or any function of the body.

Firearm Modifiers

While ghost guns have gained intense scrutiny in recent years, another firearm issue concerning payment service providers is the proliferation of accessories that turn semi-automatic guns into fully automatic ones. These can run afoul of the **rule on triggers** set by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). This rule essentially allows for only one round to be fired with each trigger pull.

Some have devised creative methods for getting around the ATF's rule. One example is a binary trigger, in which a shooter pulls once to fire one round, and then another round fires when the trigger is released. Another example is a forced reset trigger, which uses the blowback of the gun's mechanism to reset the trigger, allowing semiautomatic weapons to fire more quickly. A third example are auto sears, which jam the mechanical process of the gun and prevent it from locking the action in between rounds.

While courts battle the legality of some of these accessories, they pose reputational damage for payment service providers. Many of these accessories look innocuous and are difficult to spot. Some have even been intentionally miscategorized and sold as washing machine parts or other repair parts.



Firearm Modifier Case Study

A glock switch or glock auto sear is a small device that can be attached to the rear of the slide of a glock handgun, converting the semi-automatic pistol into a selective fire machine pistol capable of fully automatic fire. On their own, the ATF considers these to be machine guns. The merchant featured here tries to escape scrutiny by selling glock switches as keychains.

What to Watch Out For

- Know the names for various firearm modifiers. To get a fundamental understanding, watch LegitScript's **webinar on firearms**.
- If you're unsure what a merchant is selling, carefully scrutinize the description and check third-party forums to see if others are describing what the product does.
- Follow the **ATF** to keep abreast of regulatory news regarding these accessories.

SUPPLEMENTS

Trend
7

Tejocote

An FDA study of more than 700 adulterated dietary supplements over a 10-year period identified 41% as weight loss supplements containing more than one unapproved ingredient. The growing trend of tainted products in the retail marketplace has forced the FDA to intensify its efforts in supplement oversight and increase testing for impermissible ingredients. Recent testing performed by the FDA discovered a trend of products containing tejocote root (*Crataegus mexicana*). Testing revealed that products labeled with tejocote contained toxic yellow oleander, a poisonous plant native to Mexico and Central America.

Despite increased regulatory enforcement efforts and the voluntary recall of high-risk products like these from e-commerce platforms, retailers may knowingly or otherwise continue to offer these potentially dangerous products due to consumer demand and potential profits. Unsuspecting consumers may still be harmed because these adulterated supplements do not accurately disclose their ingredients.

Tejocote Case Study

In 2024, the FDA issued several warning letters concerning tainted weight loss supplements that, according to the agency, are labeled as tejocote root but are toxic yellow oleander. Brands in the recall included Eva Nutrition (featured here), Science of Alpha, Niwali, and NWL Nutra. According to the FDA, "ingestion of yellow oleander can cause neurologic, gastrointestinal, and cardiovascular adverse health effects that may be severe, or even fatal. Symptoms may include nausea, vomiting, dizziness, diarrhea, abdominal pain, cardiac changes, dysrhythmia, and more."

What to Watch Out For

- Weight loss supplements are notorious for containing unapproved ingredients; always read product labels to understand what is inside.
- Dietary supplements can also be adulterated, meaning they contain undeclared ingredients. Always check a product against the **FDA's Health Fraud Product** Database or with LegitScript's **Database Lookups**, which include recall and warning information on drugs and supplements around the world.

HEALTHCARE & MEDICAL DEVICES

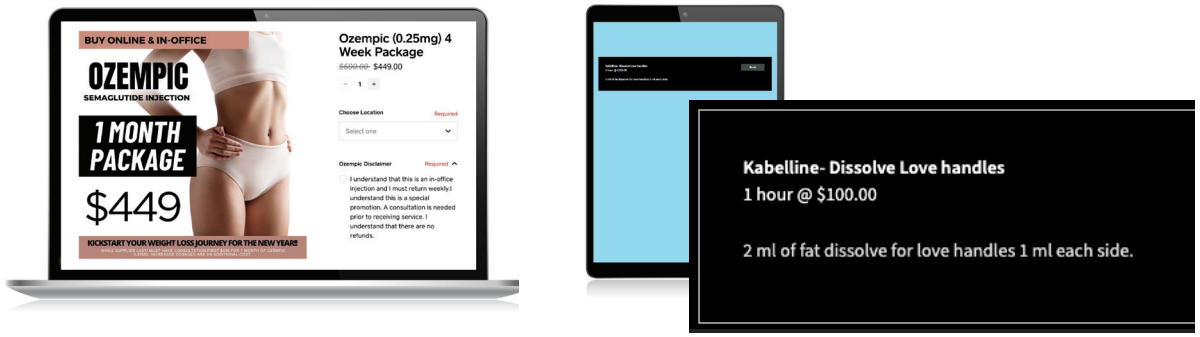
Trend 8

Medical Spas

Medical spas comprise one of the fastest-growing sectors within the healthcare industry. A report by Grand View Research estimated the market at $18.6 billion in 2023, with projections for growth at a compound annual growth rate of 15.13% from 2024 to 2030.

Med spas function as a hybrid between a day spa and a medical clinic. They offer a variety of medical cosmetic and aesthetic services such as botox injections, dermaplaning, and IV infusion therapies. Unlike traditional day spas, medical spas are typically staffed by licensed medical providers. Many have also begun to offer telemedicine services and conduct online visits with patients, expanding their market reach as well as their client base.

Because med spas are largely regulated at the state level, compliance is often confusing for med spas wanting to operate in multiple jurisdictions. Med spas often follow and implement trendier services, such as weight loss drugs, IV infusion therapies, and "vampire facials." This can open the business up to several risks, as oftentimes these services or products have not been reviewed for safety and/or efficacy by relevant regulators.



Medical Spa Case Study

The merchant feature above on the left is offering injections of Ozempic (semaglutide). At first glance it may seem like they ship the product directly. However, this page is instead used for prepayment by customers. The fine print tells customers must come into the office for it to be administered. This is considered a high-risk medical service since the merchant is accepting payment for prescription-only pharmaceuticals before the patient has had a consultation with a medical professional.

Another med spa operator, shown above on the right, is offering injectable Kabelline services. Kabelline is an unapproved drug in the United States and contains injectable deoxycholic acid for use in dissolving fat. Offering unapproved drugs in a med spa setting puts the merchant, the payment processor, and especially the customer at considerable risk.

What to Watch Out For

- Because med spa offerings vary widely, understand what services are being offered by your merchants. Be aware of the risks associated with various treatments.
- Understand where your merchants are operating. They must be compliant with the laws of the jurisdictions in which they are located and where they are providing services.
- If a medical spa is prescribing drugs and offering other telemedicine services, treat it like a telemedicine company and expect it to adhere to all telemedicine best practices.

PSYCHOACTIVES

Trend

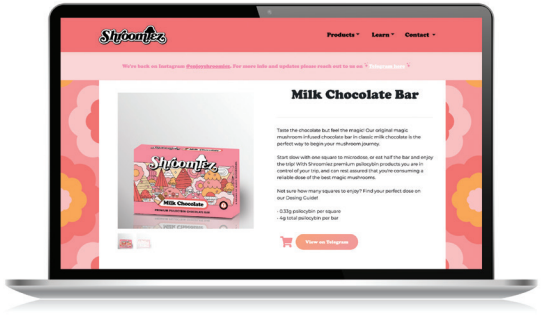
9

Psilocybin Edibles

With multiple US states and even the federal government looking at creating psychedelic medicine task forces, psilocybin is having a moment. This surge in interest in psychoactives, combined with limited legalization in places like **Oregon**, makes it important to understand the regulatory standing of psychoactive substances and the risk factors associated with online marketing and sales.

Several pharmaceutical companies have begun studying psilocybin for the treatment of various mental health conditions, and the FDA has granted Breakthrough Therapy designations to the substance for such uses, which is intended to expedite the development and review of drugs. Even so, psilocybin currently remains a Schedule I controlled substance in the US.

That designation doesn't seem to be stopping many online merchants. Psilocybin seems to be following a trajectory similar to the marijuana and CBD markets. Whereas LegitScript used to see primarily whole mushrooms and spores available for sale online, we now see a variety of psilocybin edibles, including chocolates, gummies, and other candy.



Psilocybin Edibles Case Study

The merchant featured here is offering brightly colored magic mushroom chocolate bars with a stated amount of 4g of psilocybin per bar. The chocolate comes in flavors reminiscent of mainstream candy bars with names including Crunch, M&Ms, and Cookies & Cream.

Products like these pose a number of potential problems. Unregulated manufacturing poses a greater risk to consumers since these products can be tainted or be inconsistent in their potency. Furthermore, products that may appeal to youth tend to draw greater regulatory scrutiny.

What to Watch Out For

- Look for psilocybin listed as an ingredient on product descriptions or labels.
- Carefully scrutinize edible products described as offering benefits such as euphoria, relaxation, and cerebral effects.
- Merchants engaged in the sale of other psychoactive products, such as marijuana, are increasingly like to sell psilocybin products as well.

HIGH-RISK BEHAVIOR

Trend 10

URL Shifts

URL changes are relatively common in the world of e-commerce. They may be a result of organizational shifts such as mergers or rebranding, registrar incentives, or sales of domains to an interested party. While the process is often relatively straightforward and involves transferring domain rights from one account to another, there are potential risks associated with ownership changes as failure to communicate to the merchant's payment service provider can create exposure for reputational harm and card network violations.

One of the greatest potential risks posed by an ownership change to a payment service provider is the updated website content itself. These changes in ownership carry the risk of reputational harm for the former URL's owner, as well as the potential for card brand fines for payment processors if the transfer was not effectively documented and communicated. The most frequent high-risk offenders LegitScript observes are adult or gambling content, typically on domains that may appear to be otherwise nonfunctional. Malicious actors can purchase a domain with relatively little activity and utilize it to host risky content.

URL Shift Case Study

The website featured here was previously the homepage of a US Congressional candidate, but it now drives traffic to online casinos. If this website had been processing transactions for gambling, a payment processor could be left holding the bag for chargebacks and payments processed under the original owner's account, despite the change in URL ownership.

What to Watch Out For

- It's important to regularly check merchant websites throughout the merchant's life cycle to ensure that content is not violative and that ownership has not changed hands.
- Make it a habit to monitor dormant merchants, as these are at a heightened risk of experiencing URL shifts.

Take the Next Step

Want to find out how LegitScript can help your business reduce regulatory risk, avoid fines, and keep your customers safe? Learn more about our solutions and how you can grow your business with confidence.

Merchant Risk Solutions

Marketplace Monitoring

About LegitScript

At LegitScript, we are committed to making the internet and payment ecosystems safer and more transparent. LegitScript experts proactively track high-risk trends to help keep our partners in compliance and reduce the risk of expensive card network fines. Our monitoring services provide best-in-class solutions for identifying and flagging high-risk merchants and helping our clients remove problematic vendors from their portfolios. Contact us to learn more.

Contact Us

Newsletter

Blog

LinkedIn

LegitScript