LegitScript

The Online Risk Management Handbook

The Online Risk Management Handbook

LegitScript LLC

First Edition

www.legitscript.com

Print ISBN: 978-1-66784-836-5
eBook ISBN: 978-1-66784-837-2

Contents

Introduction

When John Horton founded LegitScript in 2007, major internet and payments companies faced a major problem: rogue internet pharmacies operating with impunity on advertising platforms, e-commerce websites, and in the payments ecosystem. LegitScript and others estimated that 80% to 90% of online pharmaceutical advertisements were placed by criminal enterprises selling addictive medicines without requiring a prescription. The consequences were real: youth and adults alike were dying from overdoses after making illicit drug purchases from fly-by-night online pharmacy websites.

But illicit drug sales weren't the only problem eroding trust on the internet. For all of the great things that e-commerce has brought us, there have also been child safety issues, hate groups, illicit tobacco sales, illegal gambling operations, counterfeit products — the list goes on. At LegitScript, we expanded from our initial focus on illegal drugs to tackle all types of problematic products and content in e-commerce and social media.

In working with the world's largest internet, e-commerce, and payments companies, LegitScript has made a substantial impact in reducing the incidence of these problems on all of our clients' platforms — in some cases, to nearly zero. Our approach has been a hybrid technological/human solution, led by staff who are mission-driven. While we've invested in developing an algorithmic approach capable of scaling to the needs presented by the world's largest payments and internet companies, this technology is powered by a "team of experts" with deep knowledge about laws and

regulations in the numerous countries we most actively monitor, ranging from the US to Japan, France, Brazil, Israel, and dozens more. Cybercriminals use technology, but they are human. So are we.

Along the way, our expertise in these high-risk areas led LegitScript to focus on a type of money laundering known as "transaction laundering" — an ongoing challenge for banks and payments companies. LegitScript has since become a leading authority on detecting and preventing transaction laundering, a practice that is consistently one of the most pernicious and challenging for payments risk and compliance professionals in preventing the flow of money to cybercriminals and even terrorists.

LegitScript is now 15+ years into our mission of making the internet and payment ecosystems safer and more transparent. As such, it seemed like a good time to compile the best of our collective knowledge from our "team of experts" and their years of experience. And now we're sharing that knowledge with you.

This handbook offers an overview of the most important topics that risk and compliance professionals at payments companies and large internet platforms may face in their daily work. It includes regulatory approaches to various high-risk areas, shows valuable case studies, and offers tips to help you mitigate your company's risk. We believe it's a resource you'll want to keep on hand and refer to frequently. Whether or not you're a client of LegitScript, we want to help you create an online ecosystem that the public can trust. That's our vision for the internet, and we are grateful to the internet and payments companies who help lead the way in achieving that vision.

CHAPTER 1

Drugs, Supplements, and Healthcare

Healthcare is one of the most difficult industries to navigate in the online space because of complex regulations and risks to consumers. Internet pharmacies can be particularly challenging. While many legitimate internet pharmacies exist, the ones that refuse to play by rules designed to protect patients still saturate the online space. According to LegitScript analysis, about 97% of internet pharmacies fail to adhere to drug safety laws and regulations. Growing dependence on the internet for healthcare makes problems like this increasingly urgent.

In this chapter, we look at rogue internet pharmacies — one of the internet's most pervasive problems — as well as other operators in the online healthcare and wellness space. We'll look at compliance issues around drugs and dietary supplements, and cover the basics of telemedicine, an important service that continues to grow.

1.1 Rogue Internet Pharmacies

There is a remarkable degree of consistency worldwide on three fundamental principles related to the operation of an online pharmacy. If an internet pharmacy is violating any one of the principles below it is, with rare exceptions, operating unlawfully.

Principle #1: Pharmacy Licensure Requirement

In the vast majority of countries and territories around the world, any entity shipping drugs to individual customers in a jurisdiction must be licensed, registered, or otherwise recognized in the customer's jurisdiction. (In some but not all jurisdictions, this means that the pharmacy must also be physically domiciled there.)

Reason for the requirement: The practice of pharmacy requires special training and education. There is no "right" anywhere in the world to sell prescription drugs — rather, it is a privilege granted by official licensing agencies. The mission of these agencies is to protect patients in their jurisdictions, so those agencies need to know who is dispensing drugs to patients in that jurisdiction. Licensed entities found to be dispensing drugs in a way that is unsafe, illegal, or unethical can be held accountable by those licensing agencies — but those agencies often find that foreign or unlicensed entities are physically "out of reach" and ignore regulatory directives, fines, or other discipline.

Exceptions: Some jurisdictions have reciprocity with other jurisdictions and thus recognize those other jurisdictions' licenses. Even so, these non-resident pharmacies will almost always be listed in some official roster.

Is a pharmacy license enough to prove legitimacy? By itself, no. Being able to produce a pharmacy license or similar recognition from licensing authorities where an internet pharmacy offers to ship drugs is an important start. However, it's not the end of the story. There are three main reasons that merely being able to produce a pharmacy license does not conclusively establish legitimacy:

1. Without further review, there is no assurance that the merchant is actually dispensing drugs from that pharmacy.

2. If the customer is not in the same jurisdiction as the licensed pharmacy, the pharmacy regulator loses, as a practical matter, jurisdiction to respond to complaints and regulate the transaction.
3. Similarly, if the drug transaction does not take place within a single "closed jurisdictional system," the drug safety authority, such as the US Food and Drug Administration (FDA) or UK Medicines and Healthcare products Regulatory Agency (MHRA), effectively loses jurisdiction to ensure drug authenticity and safety.

The now-offline airmailchemist.com had a license but stated that it shipped to jurisdictions where it lacked licensure, without requiring a prescription.

Principle #2: Valid Prescriptions vs. Online Questionnaires

Internet pharmacies that sell prescription drugs — any drug designated as requiring a prescription in the customer's jurisdiction — without requiring a prescription operate illegally, even in the occasional instances where the drug can be sold without a prescription in the jurisdiction where the drug is shipped from.

Reason for the requirement: If a drug is designated as prescription-only, it is because it has been determined to require an enhanced level of medical supervision to be used safely and effectively. (If it can be used without medical supervision, it is designated as an over-the- counter drug.) The requisite level of medical supervision nearly always requires that the prescribing medical practitioner have a real relationship with the patient, which in turn often requires that the prescriber have physically examined the patient prior to the prescribing (even if it was several months before).

Exceptions: In some countries and states, it is permissible in limited circumstances for an internet pharmacy to fill prescriptions based solely on an online consultation, but only to patients in those jurisdictions.

Principle #3: Shipping Directly to Patients from Foreign Suppliers

Internet pharmacies may only sell prescription drugs that have been ruled safe and effective by the drug safety agency in their customers' jurisdictions, or that have some legal exemption. Most countries have a publicly accessible list of approved prescription drugs. As a general rule, prescription drugs imported from a supplier (including a pharmacy) in one country directly to a patient in another country are considered "unapproved for sale." Thus, internet pharmacies shipping prescription drugs from Country "B" to consumers in Country

"A" are generally considered unapproved for sale merely by virtue of being imported.

Reason for the requirement: Drug safety authorities, such as the FDA (in the US), Ministry of Health, Labor and Welfare (in Japan) and the MHRA (in the UK), generally require a "closed supply chain" for prescription drugs, so that authenticity and quality can be monitored from the point of production to the end user. Simply put, when drugs from outside the prescribed supply chain come into a country, the FDA or other regulatory authority loses the ability to monitor and ensure the safety and authenticity of the drugs. (While prescription drugs may legitimately be made in foreign factories, these are inspected and allowed to be part of the supply chain, but only to a limited number of licensed distributors or wholesalers, not directly to a patient.)

Exceptions: There are a few exceptions to this general rule, and country rules can frequently change.

Tip

To see if a website is a known rogue internet pharmacy, go to legitscript.com and enter the URL in the website checker on the homepage.

1.2 Potentially Problematic Drugs

There are some drugs categories with perennial demand that comprise the bread and butter of rogue internet pharmacy product catalogs. These include drugs for pain relief, sexual enhancement, weight loss, and muscle building.

Rogue internet pharmacies may also pivot to market whatever drugs are currently in demand. For example, early in the 2020 pandemic LegitScript analysts saw an increase in websites marketing

hydroxychloroquine to treat COVID-19 even though clinical trials found it ineffective for this purpose. Later, these websites began marketing ivermectin when rumors falsely stated it was effective against COVID-19. It's important for risk and compliance teams to keep abreast of trends in dynamic areas like this to know what drugs might be potentially problematic.

A drug may be problematic for a variety of reasons. Most commonly:

- It is an approved drug sold without a prescription and/or diverted through unapproved channels.
- It is a drug that is unapproved for use in the jurisdiction where it is being sold.
- It is a counterfeit drug.

The following subsections highlight complex areas that may be of interest to risk analysts.

Homeopathic Drugs

According to the Food and Drug Administration (FDA), a homeopathic drug is "a drug product that is labeled as 'homeopathic' and is labeled as containing only active ingredients and dilutions [...] listed for those active ingredients in the Homeopathic Pharmacopeia of the United States (HPUS)." They are available in numerous dosage forms, including (but not limited to) capsules, creams, sprays, gels, granules, liquids, lozenges, ointments, pills, tablets, suppositories, and syrups.

In general, homeopathic drugs are subject to the same drug approval requirements as conventional drugs, although there are currently no FDA-approved homeopathic products. Until recently, the FDA permitted homeopathic drugs to be marketed without approval, provided they met certain requirements, such as not offering over-the-counter (OTC) products for conditions that are not amenable

to self-diagnosis. In 2019, however, the FDA withdrew this policy and reiterated that it intends to focus its enforcement authority on certain high-risk homeopathic products, such as those with reported safety concerns, those that claim to treat or prevent life-threatening diseases, and those marketed to vulnerable populations.

While the FDA's guidance on its proposed approach to homeopathic products is not yet finalized, the agency has begun to issue warning letters and take other actions against certain high-risk products, such as eye drops produced in non-sterile conditions, injectable homeopathic drugs, and those intended for use against COVID-19.

This homeopathic product was discontinued because it was found to contain varying amounts of belladonna, a potentially toxic ingredient.

Selective Androgen Receptor Modulators (SARMs)

SARMs are chemical substances designed to replicate the effects of testosterone. Though originally developed as investigational drugs by pharmaceutical companies, SARMs have quickly become popular

as performance-enhancing supplements among bodybuilders and other athletes due to the perception that there is a lower risk of side effects than anabolic steroids, as well as the fact that they are easier to obtain, as they are not controlled substances.

Though SARMs have been on the World Anti-Doping Agency's list of prohibited substances since 2008, there has been a noticeable uptick in sanctions against athletes for testing positive for SARMs in recent years.

While there are numerous products sold as SARMs, the most common are:

Name	Alternate Name(s)
LGD-4033	Ligandrol, VK5211
MK-2866	Enobosarm, Ostarine
RAD-140	Testolone
S-4	Andarine

Even though SARMs do not produce the more blatant side effects that arise from anabolic steroid use, such as acne, breast tissue development, and shrinking of the testicles, this doesn't mean that SARMs don't present significant health risks. According to the FDA, SARMs are "associated with serious safety concerns, including potential to increase the risk of heart attack or stroke and life-threatening reactions like liver damage." SARMs-like substances also present known dangers — for example, clinical development of GW-501516 was halted when the substance was found to cause fast-growing cancers in mice and rats.

Despite merchant claims to the contrary, both the FDA and Health Canada, among other regulatory authorities, consider SARMs

to be unapproved drugs that have not been reviewed for safety and effectiveness.

1.3 Dietary Supplements

The Dietary Supplement Health and Education Act (DSHEA) of 1994 transformed the FDA's authority to regulate dietary supplements. In the following decades, the relatively small market has mushroomed into an industry with hundreds of thousands of products in a market expected to reach more than $320 billion by 2030.[1] This industry is increasingly complex, both from the sheer volume of products and ongoing regulatory scrutiny.

A dietary supplement is an ingestible product that is intended to add further nutritional value to the diet. It may contain a vitamin, mineral, herb, botanical, amino acid, or other dietary ingredient. Dietary supplements can be found in a variety of forms such as tablets, capsules, softgels, liquids, or powders. In the United States, a product must be labeled as a "dietary supplement" to be compliant.

Dietary supplements most commonly run afoul of regulators for one of two reasons: impermissible ingredients and disease (marketing) claims. We'll look briefly at both of these.

Impermissible Ingredients

The FDA has identified a number of ingredients that are not permitted in dietary supplements because:

1. They are not dietary ingredients as defined by the Federal Food, Drug, and Cosmetic Act (FDCA), and/or
2. They may pose serious health risks.

1 https://www.grandviewresearch.com/press-release/global-dietary-supplements-market

Examples of impermissible ingredients include Acacia rigidula, BMPEA, DMAA, methylsynephrine, picamilon, and ephedrine alkaloids. Visit fda.gov for a comprehensive list.

Cannabidiol (CBD) has been of particular interest for use in supplements since hemp and its extracts, including CBD, became generally permissible to produce following the passage of the 2018 Farm Bill. However, as CBD is the active pharmaceutical ingredient in Epidiolex, an FDA-approved drug for the treatment of two rare forms of epilepsy, the FDA has maintained it is illegal to market CBD as a dietary supplement or otherwise introduce it into the food supply. The FDCA states that products containing a substance that is an active ingredient in an FDA-approved drug product, or which is subject to an investigational new drug application (and for which substantial clinical investigations have been made public), do not meet the definition of dietary supplement and may not be sold as such.

Sometimes dietary supplements are tainted with ingredients that are not declared on labels. Many products marketed as "miracle" weight loss supplements or sexual enhancement supplements are also marketed as herbal alternatives to FDA-approved drugs, or are marketed as having effects similar to prescription drugs. These products may contain hidden active pharmaceutical ingredients, including controlled substances, that can be harmful.

These sexual enhancement products were found by regulatory authorities to be tainted with undeclared active pharmaceutical ingredients.

Potential warning signs that a product may be tainted include:

- Promises of a quick fix; for example, "lose 10 pounds in one week"
- Use of the words "guaranteed" or "scientific breakthrough"
- Products marketed in a foreign language
- Products marketed through mass email

Marketing Claims

In general, a supplement cannot be marketed with express or implied claims to:

1. Cure, mitigate, prevent, or treat a disease (or any similar verbiage), or
2. Affect the structure or function of the body without having adequate substantiation. Products that make these types of claims are regulated as drugs under the FDCA.

A disease claim can be explicit or implied. It can be a statement that a supplement has an effect on a specific disease or class of diseases. Alternatively, a statement may not mention a disease specifically but may refer to identifiable characteristic signs or symptoms of a disease such that the intended use of the product to treat or prevent the disease may be inferred.

Disease claims also include statements that a dietary supplement can be a substitute for a product that is a therapy for a disease and statements that a dietary supplement can augment a therapy or drug intended to diagnose, mitigate, treat, cure, or prevent a disease.

If any marketing of a dietary supplement suggests that it can be used for the cure, mitigation, treatment, or prevention of disease, the FDA may find that it is a disease claim. The FDA has previously

found disease claims in the form of customer testimonials, social media posts, online videos, and meta tags used to bring consumers to websites through internet searches.

A similar type of claim is a structure/function claim, which is a statement that:

1. Describes the role of a nutrient or dietary ingredient intended to affect the structure or function of the body in humans, or
2. Characterizes the documented mechanism by which a nutrient or dietary ingredient acts to maintain such structure or function. These types of claims can be permissible if the claims are adequately substantiated.

With limited exceptions that have adequate substantiation, structure/function claims are typically problematic.

So what can supplement merchants say? According to FDA guidance, dietary supplement marketing may make claims regarding their effect on "general well-being" and make general statements about health promotion and disease prevention — as long as the statement does not imply that the product can diagnose, cure, mitigate, treat, or prevent a particular disease. For more on this, download LegitScript's Dietary Supplement FAQ at legitscript.com/dietary-supplements.

1.4 Telemedicine

Telemedicine is the practice of medicine using electronic information and communication technology between a doctor in one physical location and a patient in another. The "practice of medicine" can include diagnosing, treating, and even prescribing drugs to manage a patient's care. Telemedicine is legal, within limits, in the US, and its usage has been steadily increasing, especially since the onset of the pandemic. Almost all states have some definition of

telemedicine (sometimes known as "telehealth") and recognize it for insurance reimbursement.

Some illicit pharmaceutical merchants, particularly those selling prescription drugs without requiring an in-person examination by a medical practitioner, may claim that they are merely engaged in the practice of telemedicine. It's important to distinguish between legitimate telemedicine, in which an in-person examination may not be required, and practices that violate the law.

Telemedicine Regulation in the US

Telemedicine is regulated largely at the state level in the US. This is because telemedicine involves the practice of medicine, which is regulated through state laws and medical boards. However, federal law can also come into play, especially in regard to prescriptions for controlled substances. Additionally, dispensing any prescription drug without a prescription, even if it isn't a controlled substance, is illegal federally.

There are two issues in particular that states have focused on when it comes to telemedicine:

1. **Licensure.** Most states that recognize telemedicine require that telemedicine practitioners be licensed in the state where the patient is located.
2. **Standards of Practice.** Most states regard telemedicine as an extension of the traditional practice of medicine and require doctors to apply the same standard of care for telemedicine patients that they would for patients they see in-person.

For example, a doctor seeing a telemedicine patient for the first time is usually required to confirm the patient's identity, obtain his/her medical history and other information necessary to make a diagnosis,

and provide follow-up care — just like they would do in person. Only filling out a form rarely meets standard-of-care requirements.

Questions that can help you determine if a telemedicine website deserves a closer look:

- Are its doctors licensed in the states where the website offers to provide services?
- Is the website offering to prescribe drugs solely via telemedicine?
- Is the website offering to prescribe controlled substances solely via telemedicine?

Other Telemedicine Requirements

In addition to proper licensure, many states have specific technology requirements for providing telemedicine services. Most laws specify rules around real-time, interactive audio and video, as well as "store-and-forward" technology. Unlike live video, store-and-forward content (also called asynchronous telemedicine) is typically saved as a file and sent to professionals using a secure, encrypted internet connection. Practitioners receive the data and can then analyze it as though it were live. A third type of service, remote patient monitoring, enables a provider to track health care data for a patient in an ongoing manner, which may reduce readmission rates. Remote patient monitoring may use real-time or store-and-forward technology.

Most states do not permit the prescribing of medication based solely on an online questionnaire. While many sites emphasize the ease and convenience of obtaining prescription medications via an internet consultation, a merchant that prescribes based solely on an online questionnaire is likely not compliant with telemedicine laws in most jurisdictions.

CHAPTER 2

Cannabis and Psychoactives

The United States is currently in the midst of a massive shift in the way that psychoactive substances are viewed by both the general public as well as the law. Substances like cannabis — one of the most widely used psychoactive drugs in the United States — are becoming increasingly normalized and legalized in various forms both by individual states, as well as, to some extent, the federal government. Some cannabis products, like CBD, have enjoyed massive popularity among the average consumer. Likewise, other psychoactive substances have begun to see an upsurge in interest and may experience potential pathways toward legalization.

The term "psychoactive" is often loosely used to describe a variety of products and substances that have mind-altering effects. They have proliferated in contexts ranging from recreational to medicinal to religious use.

LegitScript generally defines a psychoactive high product as:

1. One that is used or marketed for experiencing psychoactive effects, or a street drug alternative (e.g., synthetic marijuana, herbal incense, and bath salts) regardless of legal status;
2. Or, any product that is not branded or marketed as a prescription drug, medical device, or over-the-counter drug,

> but which is manufactured, marketed, or commonly used to mimic the effect or experience of a controlled substance, irrespective of whether the product is organic or synthetic.

In short, a psychoactive high is a substance that is intended to produce euphoria, hallucinations, or altered perceptions.

With the rapidly shifting landscape around cannabis, the proliferation of various cannabis compounds, and the growing acceptance of certain psychoactive substances, it can be difficult to get one's bearings and know exactly what is allowed and what is outright illegal.

In this chapter, we will first give an overview of the landscape around cannabis, THC, and other cannabis compounds as of the publishing of this handbook, and will then touch upon some commonly seen non-cannabis psychoactive substances.

2.1 Marijuana

Cannabis is a plant of the Cannabaceae family, which also includes hops and about 170 other species. It contains more than 80 biologically active chemical compounds, the most commonly known of which are delta-9-tetrahydrocannabinol (THC) and cannabidiol (CBD). THC is the primary substance that produces the "high" associated with the use of marijuana.

While the Drug Enforcement Administration (DEA) regulates specific types of cannabis and THC as controlled substances, the Food and Drug Administration (FDA) regulates cannabis when it's used in a type of product that the FDA has jurisdiction over (e.g., drugs, foods, dietary supplements, cosmetics, etc.). The agency's website, fda.gov, is periodically updated with the latest consumer information and administration communication regarding cannabis.

Marijuana vs. Hemp

Marijuana and hemp both belong to the same species, Cannabis sativa, and the plants share a similar look. However, hemp does not contain more than trace amounts of THC, the main psychoactive substance in marijuana. Legally, hemp may not contain more than 0.3% delta-9 THC on a dry weight basis. Historically, hemp has had a wide range of practical uses, including paper, textiles, clothing, biofuel, food, and, in recent years, as a source of CBD.

Under the Controlled Substances Act, marijuana is a Schedule I substance, meaning that it has a high potential for abuse, has no currently accepted medical use in treatment at the federal level in the United States, and lacks accepted safety for use under medical supervision. Until 2018, there was no legal difference between hemp and marijuana; cannabis was a Schedule I substance, regardless of delta-9 THC levels. However, with the passage of the 2018 Farm Bill, hemp was descheduled, and a regulatory scheme for the legal cultivation was implemented by the United States Department of Agriculture. Currently, most derivatives of hemp are not considered controlled substances, so long as they contain 0.3% delta-9 THC or less.

Medical Marijuana

"Medical marijuana" refers to using the whole, unprocessed marijuana plant or its basic extracts to treat symptoms of illness and other conditions. The FDA has not approved the use of the marijuana plant as medicine. Because it is a controlled substance federally, doctors cannot prescribe medical marijuana, but in states that have legalized medical marijuana they may provide recommendations to their patients, which allows the patient to access medical marijuana in that state. Although medical marijuana is not legal at the federal level, two FDA-approved drugs, Marinol and Syndros, contain

psychoactive cannabinoid chemicals such as synthetic THC. Marinol is a Schedule III controlled substance and Syndros is a Schedule II controlled substance.

Just because some states have legalized medical marijuana does not mean there are no restrictions. Medical marijuana programs generally still regulate:

- Who may access the product, and the quantity and form of medical marijuana that patients may grow
- Purchase or use, even in states where medical marijuana is legal

These regulations vary by state. Even if a state has legalized medical marijuana, it does not necessarily mean recreational marijuana is also legal. However, an increasing number of states have also implemented recreational marijuana programs, which usually have robust regulatory schemes with detailed requirements.

Regardless of state law, marijuana remains a Schedule I controlled substance, so federal law prohibits its sale and distribution. Most financial institutions are federally regulated and insured. For this reason, the financial services industry generally does not service marijuana merchants — even ones that appear to be compliant with state law. Financial services providers could face penalties from federal regulators for processing transactions connected to federally illegal activity.

2.2 Cannabidiol (CBD)

Cannabidiol, or CBD, is a substance found in the Cannabis sativa plant and can be derived from both marijuana and hemp. Unlike THC, CBD is not psychoactive. It has become increasingly popular in recent years. Though frequently promoted as a treatment for a broad spectrum of ailments, only one CBD product, Epidiolex, is

an FDA-approved drug, which is used for the treatment of two rare forms of epilepsy.

CBD Dietary Supplements

Currently, CBD may not be sold as a dietary supplement. According to the Food, Drug, and Cosmetics Act (FDCA), it is illegal to market CBD as a dietary supplement or otherwise introduce it into the food supply. The FDCA states that products containing a substance that is an active ingredient in an FDA-approved drug product, or which is subject to an investigational new drug application (and for which substantial clinical investigations have been made public), do not meet the definition of dietary supplement. The FDA has been reviewing its policy to explore pathways for dietary supplements and/or conventional foods containing CBD to be lawfully marketed, but progress has stalled.

While substances marketed as dietary supplements or conventional food prior to FDA approval or authorization of new drug investigations may be sold as dietary supplements, the "FDA has concluded that this is not the case for CBD." The agency has issued multiple warning letters against manufacturers of CBD products for marketing their products as dietary supplements.

Since 2019, the FDA and FTC have issued scores of joint warning letters to companies making impermissible claims about CBD's ability to treat serious diseases such as cancer, diabetes, COVID-19, and Alzheimer's. Unless a product is approved as a drug by the FDA, it may not be marketed with express or implied claims that it is intended to cure, mitigate, prevent, or treat a disease (or any similar verbiage). See Chapter 1 for more on disease claims.

Vetting CBD Sales

The bottom line for now is that CBD sellers and advertisers must adhere to the many new laws around the substance and adhere to

both state and federal regulations. The most important factors to remember are:

1. For now, CBD products may not be marketed as a food product or dietary supplement.
2. Merchants may not make disease claims about CBD, including on product labels, websites, and any related social media.
3. Merchants must sell CBD in accordance with the laws of the states where they are selling.

In addition to state and federal laws, merchants must adhere to the terms and conditions of their payment service providers, which may include additional restrictions. LegitScript's CBD Certification program and Enhanced CBD Monitoring can help online sellers and payment service providers stay compliant with state and federal regulations. To learn more, visit legitscript.com/cbd.

Other Cannabis-Derived Compounds

As mentioned above, cannabis has more than 80 biologically active chemical compounds. Although THC and CBD are the most widely known, people are increasingly exploring and experimenting with other compounds found in the plant.

When people refer to THC, they are generally referring to the compound delta-9 THC. However, there are other forms of THC, including an increasingly popular compound called delta-8 THC. It is similar in structure to delta-9 THC except for the location of its double bond. Although often considered less potent, delta-8 THC is a psychoactive compound and can get users high. Delta-8 THC can be derived from either hemp or marijuana plants, but products on the market are generally derived from hemp.

Similarly, there has been a proliferation of other cannabinoids that are derived from hemp, in a wide variety of forms, including

delta-10 THC and THC-O-acetate. This is a rapidly developing space, and so it's important for payment service providers and internet companies to stay abreast of the latest compounds and the regulatory approaches to them.

2.3 Other Natural Psychoactives

Some psychoactive products are hallucinogens or psychedelics — a diverse group of drugs or substances that cause pronounced psychological, visual, and auditory changes. This includes natural psychedelics, which we will cover in this section, and fully synthesized drugs, often called "designer drugs," which we will cover in the next section.

The non-exhaustive list below primarily highlights psychoactive products that have been in the news, faced recent regulatory scrutiny, or that LegitScript has identified as being offered for sale online frequently.

Ayahuasca

Ayahuasca is an Amazonian psychoactive plant mixture. While there are many regional variations, it usually contains two parts: the stem bark of the Banisteriopsis caapi vine, and the leaves or bark of other plants, such as the Psychotria viridis bush, which contain DMT, a DEA Schedule I controlled substance. DMT itself is not orally bioavailable, but the Banisteriopsis caapi vine contains MAO-inhibiting alkaloids, which allows the DMT to be absorbed through the stomach, which can result in intense multiple-hour hallucinations.

Recent decades have seen greater awareness of ayahuasca across the Western world, including an exploration of potential medical benefits. Although there have been clinical trials using ayahuasca for the treatment of treatment resistant depression, results had not been published by the time this book was released.

Though DMT is a Schedule I controlled substance in the United States, ayahuasca itself is not controlled, as not all variations of ayahuasca necessarily include DMT. However, even ayahuasca that contains DMT may be used in specific instances in the United States. One exception is for religious ceremonial purposes under the First Amendment. As a sacrament, ayahuasca is a central element of some healing ceremonies in the Amazon basin in South America, and its ritual consumption has become common among communities stemming from that region. It's important to note that many merchants operating spiritual retreat centers in the US may claim religious exemption to use ayahuasca in ceremonies when in fact they often do not meet the requirements.

Kratom

Kratom is a naturally occurring psychoactive plant. It is made from the leaves of the tropical Mitragyna speciosa tree, which is primarily located in Southeast Asia. Depending on the dose or amount of kratom ingested, it can have either a stimulating or a sedating effect. According to the National Institute on Drug Abuse, the chemical compounds found in kratom leaves "interact with opioid receptors in the brain which produce sedation, pleasure, decreased pain — especially when consumed at a high dosage." Kratom shops, which are increasingly ubiquitous across the US, market the substance as an energy booster, mood enhancer, and pain reliever. Some even propose to use it as an opioid withdrawal aid, which the FDA finds problematic.

Kratom is unapproved for medical use, and the FDA has repeatedly issued warning letters to companies promoting kratom to treat disease. Even so, it is easy to order on the internet, and it is often sold as a green powder in packets or in pills. It is also sometimes sold as an extract and even a chewing gum or taffy. Marketing of kratom is common in places like cannabis dispensaries and smoke shops.

In August 2016, the DEA announced its intent to temporarily place the two main active ingredients in kratom as Schedule I controlled substances, but the notice of intent to schedule it was withdrawn after intense opposition from advocates. Nonetheless, the DEA has listed kratom as a Drug and Chemical of Concern. Even though kratom has not been scheduled at the federal level does not mean it is permissible to sell. Several states have banned kratom, and the FDA has issued a warning to consumers that the agency is "concerned that kratom, which affects the same opioid brain receptors as morphine, appears to have properties that expose users to the risks of addiction, abuse, and dependence." The agency has also issued an import alert for kratom products, and regularly seizes kratom being imported into the US.

Mescaline

Peyote, also known as buttons, cactus, and mesc, is a type of cactus, small and spineless, with mescaline as its main psychoactive ingredient. While this species of cacti varies greatly in size and shape, the crown has disc-shaped "buttons" that harvesters cut out, dry, and then typically chew or soak in water to produce an intoxicating liquid. Peyote extract is bitter, which is why users often prepare a tea by boiling the plant for several hours or grind the dry cactus into a powder that can be funneled inside a digestible capsule or smoked in a similar way to cannabis or tobacco, according to the Drug Enforcement Administration. While traditionally from a natural source, mescaline can also be produced through chemical synthesis.

Mescaline is, according to the NIH, a substance that has played an important role in religious ceremonies by indigenous people of northern Mexico and the southwestern United States for generations. Peyote and mescaline are both Schedule I controlled substances under the CSA. However, similar to ayahuasca, they are exempt

from control when used in a ceremonial context by certain religious groups under the American Indian Religious Freedom Act of 1978.

Psilocybin

Psilocybin, also known as 4-phosphoryloxy-N,N-dimethyltryptamine, is the psychoactive substance in "magic mushrooms." These types of mushroom grow widely in the Western Hemisphere, especially in tropical and subtropical regions of South America, Mexico, and the United States. Psilocybin use has a long cultural history; the mushrooms were ingested by indigenous cultures from Mexico and Central America during religious ceremonies. Common methods of ingestion include dried or fresh mushrooms on their own, mushrooms mixed with food, and tea made from brewed mushrooms. Psilocybin is naturally occurring and is not commonly produced synthetically.

In the United States, psilocybin is also a Schedule I controlled substance. According to the DEA, there is no currently accepted medical use for psilocybin, and it lacks accepted safety for use under medical supervision. Even so, psilocybin advocates have been shifting public perception in recent years through greater media coverage, clinical interest, and local ballot measures meant to decriminalize the substance. Oregon was the first US state to legalize psilocybin for therapeutic use in November 2020.

Over the last few years, 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.

Salvia

According to the National Institute on Drug Abuse, "Salvia (Salvia divinorum) is an herb in the mint family found in southern Mexico. The main active ingredient in salvia, salvinorin A, changes the chemistry

in the brain, causing hallucinations." Both salvia and extracts of salvinorin A are commonly sold as "legal" psychoactive highs in states where there are no restrictions.

While salvia is not illegal at the federal level, many states, such as Florida and Wisconsin, and other countries have laws that prohibit or regulate its use. Furthermore, the DEA has listed salvia as a Drug of Concern, and it has no approved medical uses.

Sonoran Desert Toad

Not all natural psychoactive substances are plant-based. A species of toad produces a substance that is similar to DMT, the psychoactive substance commonly found in ayahuasca. According to a study published by the National Center for Biotechnology Information, "5-methoxy-N,N-dimethyltryptamine [5-MeO-DMT] is a psychedelic substance found in the secretion from the parotoid glands of the Bufo alvarius toad. Inhalation of vapor from toad secretion containing this substance has become popular in naturalistic settings as a treatment of mental health problems or as a means for spiritual exploration." In recent years, spiritual retreats offering 5-MeO-DMT secreted from the Sonoran Desert toad have become an increasing trend.

5-methoxy-N,N-dimethyltryptamine, whether derived from the Sonoran Desert toad or from other sources, is also a Schedule I controlled substance. While at one point the compound was considered a sacrament used for religious purposes, it has never been granted any explicit exemptions under any Religious Freedom Acts of the United States. In all states where the Sonoran Desert toad is native, the possession and sale of it is prohibited.

Tips Regarding Merchants Marketing Psychoactive High Products

- Websites marketing psychoactive high products are generally blatant about their offerings.
- Be sure to check where merchants are located and where they offer shipping since laws may vary by country. For example, the Netherlands has more permissive laws around certain psychoactive products.
- Some online merchants selling to the US may claim products are legal because they are for "religious use" or "research purposes," but these claims are generally untrue.
- LegitScript has seen a rise in merchants offering spiritual retreats at which substances such as ayahuasca are provided. Though many of these retreats are located in countries where such substances are not prohibited, these websites could still present reputational risks, and result in heightened regulatory scrutiny or card brand fines.

2.4 Psychoactive Designer Drugs

Synthetic psychoactive products, sometimes called designer drugs or street drugs, are ones created in a laboratory. While not all designer drugs are psychoactive, ones that are include LSD, MDMA (ecstasy), methamphetamine, ketamine, and GHB. In this section we provide information about bath salts and herbal incense, two new forms of psychoactive substances that have gained prominence in recent years.

Bath Salts

The term "bath salts" is slang for synthetic drugs chemically related to cathinone, a stimulant found in the khat plant. Chemically, cathinones are similar to amphetamines such as methamphetamine and

MDMA. Common man-made cathinones found in bath salts include 3,4-methylenedioxypyrovalerone (MDPV), mephedrone, and methylone. Bath salts usually take the form of a white or brown crystal-like powder and are sold in small plastic or foil packages conspicuously labeled "not for human consumption," "for novelty use only," or "for research purposes only."

These products are often marketed as "research chemicals" but are used to create designer drugs. They have been nicknamed "bath salts" because of their visual similarity to soaking products that are actually used during bathing. These two products are unrelated in their chemical makeup, and true bath salts have no mind-altering ingredients.

Bath salts have gained notoriety in recent years because of highly publicized incidents in which a person under the influence of the drug has acted out violently, sometimes injuring or killing others. They are sold under a variety of pseudonyms, including research chemicals, jewelry cleaner, plant food, plant fertilizer, hookah cleaner, phone screen cleaner, and party powder.

Herbal Incense

Herbal incense is a slang term for another type of designer drug. To create herbal incense, drug manufacturers spray synthetic cannabinoids (such as AB-FUBINACA or THJ-2201) onto dried plant matter (usually damiana leaf or mugwort). Some "incenses" are sold as liquids to be vaporized and inhaled in e-cigarettes and other devices. Herbal incense is usually available packaged in colorful foil packets, adorned with bright colors and cartoons.

Some have speculated that the epidemic of injuries related to vaping may be a result of vaping cartridges that have been laced with undeclared synthetic cannabinoids. Herbal incense is also sold as aromatic potpourri, K2, Spice, herbal potpourri, herbal smoking blends, liquid aroma, synthetic marijuana, and liquid incense.

Dangers and Regulations of Designer Drugs

While the risks vary by type, designer drugs can cause a variety of side effects including heart attacks, insomnia, agitation, anxiety, delusions, hallucinations, muscle spasms, seizures, severe paranoia, and aggression. Psychotic symptoms are common, and people under the influence may be a danger to others.

These products are generally illegal. Bath salts and herbal incense contain either controlled substances or analogues of controlled substances. Three common bath salt ingredients – methylenedioxypyrovalerone (MDPV), 4-methyl-N-methylcathinone (mephedrone), and 3,4-methylenedioxy-N-methylcathinone (methylone) – have been classified by the DEA as Schedule I controlled substances.

Many synthetic cannabinoids, including AB-FUBINACA, 5F-APINACA, and THJ-2201, have also been added to Schedule I of the Controlled Substances Act.

Tips for Spotting Designer Drugs

- Bath salts and herbal incense are commonly sold in bright packaging and labeled very obviously as "not for human consumption."
- When sold as "research chemicals," bath salts are often marketed in simple bags or as chemical structures.
- Bath salts and herbal incense are sold online and in drug paraphernalia stores ("head shops").
- Common brands of bath salts include Cloud Nine, Vanilla Sky, White Lightning, Ivory Wave, Ocean Burst, and Red Dove.
- Common brands of herbal incense include Scooby Snax, Diablo, Joker, Wanted, K2, and Spice.

CHAPTER 3

High-risk Business Models

Certain business models pose inherently more risk because they can more easily take advantage of consumers. While many of these merchants may be legitimate and operating in good faith, these business models warrant extra scrutiny because they have a history of abuse and problematic activity. In this chapter, we focus on three of the most common high-risk business models: negative-option billing, drop-shipping, and no-value-added services.

3.1 Negative-option Billing

Negative-option billing merchants use a customer's failure to reject an offer or cancel an agreement as confirmation that they want to be charged for goods and/or services. This method benefits sellers by lowering costs and increasing revenue, thereby generating higher profits. By shipping products to consumers on a predetermined schedule, sellers can stock the appropriate inventory and avoid costs related to renewals.

This type of selling, however, is heavily regulated by the Federal Trade Commission (FTC) because of the high risk for deceptive practices. Typically, the problematic versions of these merchants offer a product for free, or at a reduced cost, then continue to bill the consumer for an ongoing subscription that the consumer was unaware they consented to. This structure can increase the risk of chargebacks. Both the FTC and major card brands such as

Mastercard have strict rules about how negative-option merchants must operate.

How it Works

Negative-option billing, also known as continuity marketing, is a practice in which the consumer's failure to reject an offer or cancel an agreement is interpreted as confirmation that they want to be charged for goods and/or services. Essentially, these merchants may be misleading their customers into signing up for subscriptions or recurring purchases without customers' express consent. Merchants engaged in this practice pose risk for regulatory and card brand scrutiny, as well as elevated risk for chargebacks.

Congress has stated that it is illegal for merchants to sell online using a negative-option feature unless certain conditions are met regarding transparency, informed consent, and easy cancellation practices.

Comparing Fraudulent and Legitimate Subscription Models

Merchants engaged in negative-option billing differ from merchants offering a simple subscription or recurring service. Indicators that a merchant is offering legitimate subscription services include:

- They disclose material terms in an understandable manner.
- They make the appearance of the disclosures clear and conspicuous.
- They disclose the terms of the offer before payment is made.
- They obtain affirmative consent for the offer.
- They never impede the process of cancellation.

Negative-option billing hinges upon deceptive practices to obfuscate the true nature of the business model. There is nothing problematic

about subscription-based services that are forthright about their billing and obtain consent for recurring offers.

Anatomy of a Negative-option Billing Merchant

While the FTC has shared some basic guidelines that can help in determining compliance for a negative-option billing merchant, there are often other simple indicators to be on the lookout for that may also be used to conduct a quick "sniff test" of a merchant's operation. For instance, because this problematic business model hinges upon deception rather than quality of offerings to return a profit, many merchants seek low overhead costs, usually in the form of hastily made template-based websites.

These websites often feature products — typically dietary supplements or cosmetics — under the guise of "free trial" promotions paired with aggressive "act fast" marketing in an attempt to hasten the customer's purchasing time. Rushed customers don't want to miss out on a deal, and merchants don't want them to identify the true terms of the purchasing agreement, which are often intentionally buried on the website. Other negative-option billing merchants may offer a limited array of products with sparse descriptions, high price points with unrounded numbers, and/or product bundling options. In employing these tactics, negative-option billing merchants bank on the chance that consumers won't notice or think twice to check their bank statements for recurring subscription charges.

Card Brand Rules Around Negative-option Billing

Mastercard has standards for merchants engaged in recurring or subscription-based billing to require more rigorous checks on negative-option billing. These standards present a more holistic definition of negative-option billing, and prescribe ways to mitigate consumer harm and reduce credit risk, such as the curtailment of

negative-option merchants who attempt to spread chargeback risk through load balancing.

Negative-option Red Flags

Although negative-option billing merchants market various products and services, dietary supplements and cosmetics are common product offerings. Typically, the merchant's website will feature a prominent call to action while providing little information about the products themselves. Common characteristics of negative-option merchants include:

- The merchant obfuscates its billing terms (for example, by using small print or making the terms difficult to find).
- The merchant provides complex and potentially misleading billing terms (for example, the customer must cancel within 18 days, four days of which are shipping days, to avoid a charge of $99.95).
- The merchant's website uses a common template that provides little information about the product offered and focuses on encouraging customers to sign up for a "free trial" that may result in a substantial follow-up charge.

Rebranding Methods

The regulatory scrutiny and deceptive nature of negative-option billing is in and of itself a high-risk commercial activity, prone to chargeback risk and consumer dissatisfaction. As such, merchants operating in this space recognize their practice as a short game, hoping to capture as many sales as possible before drawing too much critical attention.

Negative-option billing merchants remain nimble in their ventures by rebranding and relocating, often setting up shop with a new name and website within weeks of a closed former account.

Using a template-based design for their new websites helps minimize the impact of account turnover considerably, and merchants rely heavily on private label manufacturers and fulfillment centers to relabel and ship products with their new name and branding to sustain their schemes.

Multiple negative-option websites for weight loss supplements display the same template with seemingly identical products that are branded differently.

Load-balancing Risk

Another method merchants may use is load-balancing transactions. Merchants may create multiple accounts in an attempt to spread transactions and chargeback risk to avoid drawing scrutiny. A sole operator may open several accounts for the same website URL to help facilitate this.

A merchant may also create a wider network of websites to help further spread transaction activity. These websites may share some of the same characteristics noted in the previous sections, and may feature similar or alternative products with generic or absent name recognition. Alternatively, these websites may be even more functionally derelict and unchanged from a template, serving instead as a shell company designed to shoulder the processing of more active accounts under ownership.

Examples of FTC Action

Negative-option billing can take many forms. To prevent consumer harm, regulatory authorities have specific rules regarding negative-option plans, such as the FTC's requirement that merchants clearly disclose terms of an offer and never impede the cancellation process. Companies that run afoul of regulatory agencies may face monetary judgements.

In one case, the lingerie company AdoreMe offered VIP memberships for a monthly fee. It allowed subscribers to skip months and issued a credit for $39.95 when they did. However, when customers canceled their subscriptions, they lost the stored credits they had accrued. The FTC determined this to be a deceptive practice, and the company was required to refund customers.

In another case, NutraClick, a nutritional supplements and beauty products merchant, faced a fine of $350,000 for failing to fully disclose the billing terms behind its "free" samples. When consumers signed up, they were automatically registered for a membership costing $29.99 to $79.99 per month. This violated Section 4 of the Restore Online Shoppers Confidence Act (ROSCA).

The AdoreMe website (left) offered subscription credit, but then wouldn't let some customers redeem it. NutraClick's Force Factor (right) offered free samples that unwittingly signed customers up for a subscription.

3.2 Drop-shipping

Drop-shipping may not be a practice familiar to many consumers, but this business model is becoming increasingly popular for online merchants. Starting a drop-shipping business is relatively easy and affordable, allowing many merchants to launch these businesses from their homes. Although there are many benefits to this model for merchants, drop-shipping can cause complications for e-commerce marketplaces and other internet companies trying to mitigate risk.

Drop-shipping Explained

Drop-shipping is a business model that allows merchants to sell products without having a physical inventory of the items they sell. The products sold go directly from the manufacturer or wholesaler to the customer without utilizing the typical distribution channels, such as a storefront or reseller warehouse.

Drop-shippers do not own or possess the inventory of products listed on their website — they simply help facilitate the sale. These merchants (or retailers) make a profit on the difference between the wholesale and retail price.

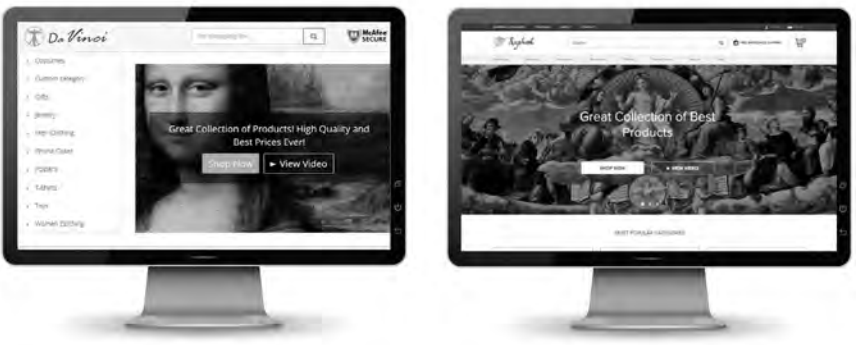
Large e-commerce platforms such as Amazon and eBay typically allow drop-shipping, but have policies around it.

Legitimate Uses of Drop-shipping

Drop-shipping has become increasingly popular because it allows a merchant to launch a business without having to invest a large amount of money in a product. Merchants can create a successful e-commerce business from a home or small office with little funding.

The drop-shipping model also cuts out traditional responsibilities, such as storing items in a warehouse, performing packing and shipping, processing returns, and managing inventory.

Additionally, drop-shipping merchants frequently do not have to create their own websites from scratch. There are many templates available online, such as the ones shown in the following images, offered through drop-shipping services companies.



Drop-shipping templates, which are often free, make setting up a drop-shipping business quick and easy.

Risks Associated With Drop-shipping

There are risks involved with drop-shipping, which is why some e-commerce marketplaces discourage these merchants from entering their platforms. One risk is that drop-shippers never own or control their inventory. This makes problems with fulfillment and shipping far more common than traditional retailers. Chargebacks are more common and complex because, with more people involved in the sale of an item, it is sometimes difficult to determine who is responsible if something goes wrong.

Furthermore, drop-shipping websites are sometimes used to mask illegal activity through transaction laundering. Criminals will set up drop-shipping websites, seeming to sell innocuous products but actually processing transactions for products such as illicit pharmaceuticals or psychoactive high products.

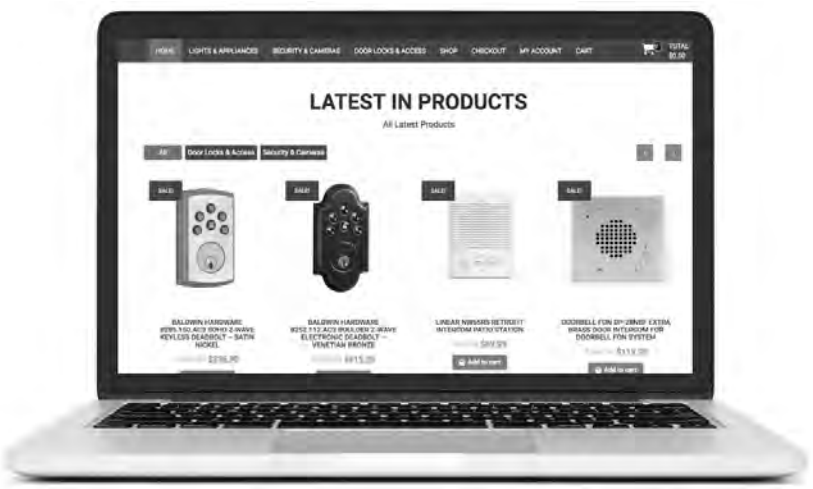
Characteristics of a High-risk Drop-shipper

Although many drop-shipping websites share similarities, there are some red flags that stand out regarding possible illicit activity. These include:

- Overly generic website templates with no unique information regarding the business. Some may even display the original template text and contact information.
- A random or erratic selection of products for sale.
- Oddly broad or narrow product lineups.
- Nonsensical pricing for the products being sold.
- Obvious neglect, such as broken links or inactive social media accounts.

Case Study: A Drop-shipping Transaction Launderer

At first glance, the retail website in the following image appeared to be selling locks and alarm systems. They were using a common drop-shipping template and included unique contact information. However, upon further review, there were multiple red flags that stood out.



Although this merchant stated that the business was located in the United States, the phone number listed on the webpage was not formatted correctly for the US. Additionally, the phone number matched that of another company offering payment processing services for high-risk businesses.

There were inactive links to social media and customer service pages. Furthermore, many of the products had seemingly haphazard pricing (e.g., $336.90). This price structure can be fairly common for drop-shipping website templates that have yet to be populated with original content.

LegitScript confirmed transaction laundering for this website via a test transaction. This seemingly innocuous lock and alarm website was set up to run transactions for the illicit pharmaceutical website Legal Medicines Online, as shown in the following image.

This rogue internet pharmacy markets a variety of prescription drugs, including pain medications such as hydrocodone, morphine, and

oxycodone. The website appears to ship worldwide and does not appear to require a prescription.

Because drop-shipping is a common typology for transaction launderers, LegitScript recommends paying close attention to these merchants. For more on transaction laundering, see Chapter 7 of this handbook.

3.3 No-value-added Services

Merchants involved with no-value-added services generally offer to facilitate government applications or other services that consumers could complete on their own for free. LegitScript has seen an increase in no-value-added services, ranging from phony driver's license renewals and travel authorizations to fraudulent immigration services.

No Value Added Explained

"No-value-added" merchants are described as such because they quite literally offer no value to their customers; worse still, they may prey on vulnerable populations, such as immigrants or the elderly. There has been ongoing regulatory action against such businesses in the United States, and these merchants pose considerable risk, especially considering the potentially sensitive nature of consumer information involved with government applications. Additionally, they pose a high credit (chargeback) risk because they often mislead customers about having government affiliation but ultimately have no influence.

Commonly Targeted Industries

One of the most common targets for no-value-added merchants is reselling the US Department of Homeland Security's Electronic System for Travel Authorization (ESTA). Since 2009, citizens of

countries participating in the visa waiver program have been required to obtain this authorization prior to entering the United States. Originally free of charge, ESTA costs $14 as of 2022, but many scammers lure unsuspecting travelers into paying significantly more. These websites frequently attempt to make their websites appear official, and often claim to review or submit customers' applications.

Websites that copy the official ESTA website, such as official-esta.com, charge as much as $95 for the $14 application. Not only is this deceptive, but consumers receive no added benefit whatsoever, and the merchant nets more than $80 of profit per transaction. Worse than being overcharged, customers in rarer instances may never receive their travel authorization. Despite international media attention about these scams, they still persist.

Official ESTA website

Virtually any government service can be a target for these scammers. LegitScript analysts have observed problematic no-value-added services centered on the sale of state fishing and hunting licenses, business incorporation and licensing, visa processing, birth or marriage

certificates, and more. In short, any merchant offering to facilitate access to readily obtainable government services warrants scrutiny.

The homepage and domain name of official-esta.com make it appear like the official website.

No-value-added Red Flags

No-value-added merchants often attempt to play up their alleged government affiliations. Keep an eye out for misleading similarities to government websites, especially the use of official symbols or logos, which may warrant additional scrutiny when coupled with fine print and disclaimers about the merchant's lack of government affiliation.

These merchants also commonly use domain names that bear striking similarities to that of the official website, or that could be easily mistaken for an official government website or service. Keep an eye out for domain names that are within a character or two of their official counterpart.

Take notice of the cost breakdown: these merchants will often disclose that the government paperwork is available for free, or costs nothing to file when displaying their fee. For example, any

merchant charging $99 to file a free form with a government agency is a red flag.

While not authoritative in itself, checking for a pattern of poor online reviews can help establish a pattern of a business's habits. Confirming the merchant's greater internet presence can be another important step to verifying the legitimacy of a suspicious merchant's services.

The Importance of Persistent Monitoring

In LegitScript's experience, merchants terminated for offering no-value-added services often quickly disappear and then reappear with a new, fully rebranded scheme, ready to open new merchant accounts using fresh concealment tactics. Payment service providers should dedicate resources to continuous monitoring, re-review, and network research to identify new websites in connection to known networks.

As part of its merchant monitoring service, LegitScript continues to actively monitor known network data points such as email addresses, merchant names, DNS information, and many other unique identifiers to quickly identify new no-value-added schemes and detect transaction launderers. This kind of proactive detection and monitoring for emerging threats enables our analysts to keep clients informed of newly confirmed high-risk accounts and their constantly changing patterns.

Case Study: An Infamous No-Value-Added Merchant

After lost fortunes and a series of lucrative online scams, Canadian serial entrepreneur Jesse Willms turned his eye to no-value-added schemes. In 2011, the FTC took enforcement action against Willms for his involvement in creating a vast affiliate network of websites marketing supplements and cosmetics with negative billing options and deceptive marketing. According to the FTC, Willms collected

hundreds of millions of dollars from consumers around the world with these scams, and eventually consented to a $359 million settlement with the FTC.

Following the FTC action, Willms moved into offering no-value-added services. His offerings are extensive and include numerous template sites, such as publicrecords.us.org and police.us.org. These websites claim to offer customers access to police records and publicly available information for a fee. Such offerings are red flags for no-value-added services to begin with, but based on Willms' prior activities, consumers may face an elevated risk of being ensnared in a recurring billing scheme for services they never actually receive.

Example of two strikingly similar no-value-added website operated by Willms

In addition to these websites, Willms also operates sites that claim to offer a number of other government services, including DMV-related services.

For example, while dmv.us.org discloses the fact that it is not associated with the Department of Motor Vehicles; however, the URL and overall internet presence is set up in a way that could easily confuse consumers, especially those from less internet-savvy demographics.

An official-looking Willms-operated website offering DMV services

Recent FTC actions against the operators of the similarly deceptive dmv.com underscore the risk posed by this type of scheme. The operators of dmv.com and associated websites sold sensitive personal data from the customers who fell for their deceptive marketing. According to the case, by their nature, "the websites were patently misleading." Once a consumer's information is available online, it can proliferate in unexpected ways. For example, Willms' extensive database fell victim to hackers, and as many as 4 million customer records were sold on the dark web.

CHAPTER 4

Financial Trading Platforms

Online investing has seen a substantial increase in popularity and access due to new and emerging trading platforms that allow users to bypass traditional brokerages. With the rise in traffic to mainstream trading websites such as Robinhood and E*Trade, the number of platforms offering increasingly complex trading opportunities — and sometimes even facilitating fraud — is proliferating online, including on websites that accept credit cards.

As the market expands and evolves, regulators are struggling to keep up with all of the fraud. IOSCO, the International Organization of Securities Commissions, maintains a database of thousands of warnings and alerts that have been issued by regulators all over the world involving investment scams. These trading opportunities often present significant risk to customers and attract attention from government regulators, law enforcement, and card brands.

This chapter provides a high-level overview of some of the more common and popular complex financial instruments — including forex trading, contracts for difference, and binary options — to help payment service providers and internet platforms learn key points to consider when facing these types of merchants or platform users.

4.1 Forex Trading

Forex Trading Explained

"Forex" is shorthand for "foreign exchange" and is the global currency trading market (e.g., selling US dollars and buying euros). Ordinary forex trading is not necessarily any more problematic than any other types of investing, though it can carry additional risk, and there is no centralized international market or exchange where all trading takes place. While forex trading used to be reserved for banks, corporations, and other entities trading in high volume, the proliferation of internet trading platforms has allowed individuals known as retail investors (individuals who do not have a high net worth or significant experience trading in the market) to open accounts with relatively small amounts of money and engage in forex trading.

Forex trading is much more complicated than simply swapping US dollars for Japanese yen, like a tourist might do at a bank while traveling. Most trading platforms permit customers to use what is known as leverage or margin trading, which allows customers to place a small amount of money down in order to control a large amount of currency. In the US, regulated forex trading permits a cap of 50:1 leverage; however, other countries permit up to 100:1 leverage, and some jurisdictions do not provide any cap on leverage whatsoever. While this allows for greater profits when a trade is successful, it also means that losses are amplified as well.

In some situations, investors on the wrong side of a trade may lose more money than is available in their account, eventually owing a debt to the trading platform. Platforms operating legally in regulated jurisdictions generally have to limit these losses, but those operating illegally, or in places where regulations are less robust,

place no limit on potential losses and will take the opportunity to draw additional "owed" funds directly from customers' credit cards.

Risks and Problematic Actors

In addition to the inherent risk in forex trading, governments have warned about fraudulent scams involving the forex market. US regulators have identified scams in which forex "dealers" simply steal money from investors outright and never actually place any trades. Additionally, some brokers have been found to artificially manipulate data on platforms to make certain investments more attractive to customers. Finally, many of these trading platforms may not be fraudulent, but are engaging in unlicensed activity. The UK Financial Conduct Authority (FCA), maintains an active list of unauthorized firms and individuals, including many offering forex trading, with several new firms being added daily. Additionally, it is important for both potential customers and acquirers to know that in many jurisdictions forex trading is almost completely unregulated, so those who are victims of fraud or unscrupulous tactics may be completely without recourse in many cases.

Forex Case Study: Luxis Trade

Luxis Trade was a platform that, according to the UK Financial Conduct Authority, was engaged in unlicensed activity, which can increase the risk of customer exploitation. The FCA website stated that consumers should be wary of dealing with Luxis and similar platforms that have not been vetted by the government: "Almost all firms and individuals offering, promoting or selling financial services or products in the UK have to be authorised by us. However, some firms act without our authorisation and some knowingly run investment scams. This firm is not authorised by us and is targeting people in the UK. Based upon information we hold, we believe it is

carrying on regulated activities which require authorisation." The platform now appears to be offline as of the writing of this handbook.

4.2 Contracts for Difference

CFDs Explained

CFDs, or contracts for difference, are popular on online trading methods. A CFD is an agreement between a buyer and seller to exchange the difference between the current price of an asset (like a stock) and its price when the contract is closed. In general, if a stock's value goes up during the contract period, you make money; if it goes down, you lose money. Traders do not actually purchase the stock. CFD trading usually involves the use of leverage, and only requires a small deposit on the total amount of the trade, so gains and losses are amplified. CFDs are another type of investment that was previously only utilized by major institutions but are now being traded by retail investors on online platforms.

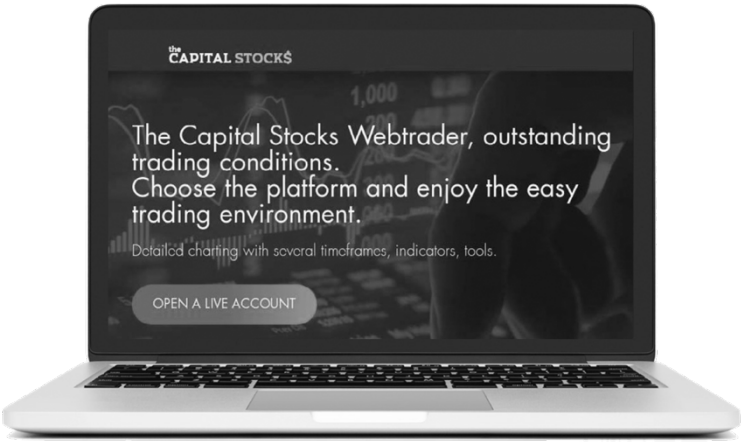
CFDs are not permitted in the United States and are subject to strict regulation for retail investors in many countries such as the UK and EU member states.

Risks and Problematic Actors

Like forex trading, in addition to the inherent risk of investing, fraud is a significant risk with CFDs. Fraudulent brokers may offer unrealistic deals to get customers to transact on their platforms but may refuse to let customers withdraw earnings. If the platform is unregulated, there may be little recourse for consumers.

CFD Case Study: The Capital Stocks

BaFin, the Federal Financial Supervisory Authority of Germany, issued a warning about The Capital Stocks, a platform that entered into CFDs based on forex products, shares, indices, commodities, and cryptocurrencies. According to the notice, the parent company, Kleinman Enterprise Limited, did not hold authorization from BaFin, as required under the German Banking Act, and so the government ordered the immediate cessation of its unauthorized proprietary trading activities.



4.3 Binary Options

Binary Options Explained

Binary options are a bet on whether an asset (usually a stock) will trade higher or lower than a certain price at a certain point in time, usually very close to when you make the bet. They have drawn a lot of regulatory attention in recent years in countries such as Brazil and India. Other than the name, they have almost nothing to do with "traditional" options, and the bettor never actually buys the stock they're betting on. If the bettor is correct, they make a pre-established percentage of their bet. If they're wrong, they lose all of the money they bet. Other names for binary options include: "all-or-nothing options," "bet options," and "one-touch options."

Binary options are either banned or strictly regulated in a number of jurisdictions such as the United States, Canada, EU member states and, most recently, Australia.

Risks and Problematic Actors

A study by the Australian Securities and Investments Commission found that about 80% of retail clients lost money trading binary options, and that binary options are likely to result in cumulative losses to retail clients over time because of their product characteristics: the "all or nothing" payment structure, the short contract duration, and the negative expected returns.

In addition to the risks associated with trading binary options, the US Securities and Exchange Commission has identified common frauds associated with binary options trading platforms, including refusal to credit customers' accounts, software manipulation to show that customers lost money when they actually "won," and widespread identity theft. Prior to the practice being banned in Canada, binary options fraud was so rampant that the Canadian Provincial

Securities Administrators created an entire website devoted to binary options scams.

Binary Options Case Study: Blue Bit Analytics

The US Commodity Futures Trading Commission (CFTC) issued an order requiring New York resident Glenn Olson to pay more than $1 million for his role in a fraudulent binary options scheme. According to the CFTC, Olson admitted that he and others misrepresented the profitability of trading through the company Blue Bit Analytics. They also reportedly manipulated or fabricated trades in customer accounts to the customers' disadvantage, prevented customers from withdrawing funds, and misappropriated customer funds.

4.4 Financial Trading Platforms Risks and Warning Signs

Red Flags

Consumers, internet platforms, and payment service providers should carefully scrutinize any online trading platform they interact with. The following red flags may present elevated risk and warrant additional scrutiny.

- Promises of very high returns in a short period of time
- Platforms that offer very short trading periods, such as minutes or hours
- Offers of "free" money or other incentives to start trading
- Automatic investing options (e.g., "let the computer do it for you!")
- Language suggesting that customers open an account in another country to get around government regulations
- The option to use credit cards. While accepting credit cards is not unheard of or outright prohibited in the industry, most reputable, regulated brokers will require cash (debit card or bank transfer) to establish an account to trade, and never accept credit cards.

Risks for Internet Platforms

Operators of problematic financial trading platforms often recruit customers through social media, which can cause reputational damage to the social media platform and negative media exposure. To help prevent users from marketing these types of financial services, it's important to watch out for red flags in user-generated content, including:

- Promises of very high returns in a short period of time
- Platforms that offer very short trading periods, such as minutes or hours
- Offers of "free" money or other incentives to start trading
- Automatic investing options (e.g., "let the computer do it for you!")
- Language suggesting that customers open an account in another country to get around government regulations

- The option to use credit cards. While accepting credit cards is not unheard of or outright prohibited in the industry, most reputable, regulated brokers will require cash (debit card or bank transfer) to establish an account to trade, and never accept credit cards.

Risks for Acquirers

Consumers aren't the only ones at risk. Acquirers and payment service providers face risks related to financial trading platforms:

- Because the platforms offering these non-traditional investment products are heavily regulated and have drawn significant attention from government agencies, card brands typically consider operating financial trading platforms to be a high-risk activity, placing additional scrutiny on acquirers who onboard these types of merchants.
- The prevalence of fraud in the market presents significant chargeback risk, a risk of card brand fines, or possible regulatory or legal action.
- Even if financial trading platforms are operating legally, the significant risk to investors increases chargeback risks if customers lose money when trading.

Increasingly, consumers are being targeted by investment scams carried out through online trading platforms where fraudsters offer trades in foreign exchange, contracts for difference, binary options, and crypto assets such as Bitcoin. These are often promoted via social media.

Important Takeaways

- **Regulation is complicated.** In the world of financial regulation, both where you conduct the activity and where

the customer is located can determine which laws apply. Generally, a platform does not have to be based in a given country to be subject to its laws.

- **Some platforms may appear to be licensed.** Many websites offering exotic trading options may have valid licenses in certain jurisdictions such as Malta or Cyprus, and claim that these licenses allow them to operate worldwide. In most cases this is not accurate, as most regulated markets require a license to operate in a given jurisdiction.
- **The market is often ahead of the regulations.** As agencies move in to regulate some of these financial instruments, the market creates new ones to replace them. Some platforms offer a variety of trading options — binary options on forex, forex trading involving cryptocurrency, CFDs on forex, etc. — and they often call them by different names, which makes it difficult to determine whether it falls within a country's specific laws. For more on cryptocurrency, see Chapter 8.

CHAPTER 5

Deceptive Practices

Consumers don't always get what they pay for — especially in the online space. Deceptive marketing techniques and SEO manipulation tactics on the internet are both pervasive and ever-changing as scam artists, hiding behind the anonymity that the internet affords, develop new and creative ways to lure consumers into well-orchestrated schemes.

This chapter discusses the regulatory bodies that govern unfair and deceptive practices, and gives examples of some of the industries that pose an elevated risk for deceptive marketing, including health and wellness, lending, fake job opportunities, risk-free trials, credit repair, debt collection, and more. We then describe common tactics used by merchants to trick consumers, game the system, or evade the detection of enforcement bodies.

5.1 The Federal Trade Commission

Both the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) are focused on stopping unfair and deceptive practices. The FTC is primarily concerned with protecting consumers from fraud in the marketplace, regardless of the product or service. The CFPB, despite its broad authority, generally concerns itself with deceptive claims regarding consumer financial products or services.

About the FTC

The Federal Trade Commission, or FTC, was created in 1914, with a mission to combat anti-competitive trade practices as a response to massive monopolistic trusts that arose in the late 19th century. Since then, the scope of its authority has continued to grow; it now acts as the primary enforcer against unfair and deceptive trade practices, and administers such consumer protection laws as the Equal Credit Opportunity Act, the Restore Online Shoppers' Confidence Act (ROSCA), and the Telemarketing Sales Rule.

To accomplish its mission, the FTC conducts in-depth investigations, brings lawsuits against violative companies, and pushes consumer education initiatives.

While the FTC's authority is broad, its two primary areas of focus are (1) the elimination of anticompetitive business practices; and (2) protecting consumers from unfair and deceptive trade practices.

Unfair and Deceptive Trade Practices

The Federal Trade Commission Act (FTCA) prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC considers "deceptive" practices to be those that involve a material representation, omission, or practice that are likely to mislead consumers acting reasonably in the circumstances." Unfair acts or practices, on the other hand, are those that cause or are likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." False advertisements that are likely to cause a consumer to purchase food, drugs, medical devices, services, or cosmetics are explicitly prohibited by the FTCA (see 15 USC § 52).

The Responsibility of Payment Service Providers

For years, the FTC has viewed enforcement actions against payment processors as a "critical component" in its fight against fraud. From 2013 to 2017, the FTC targeted payment processors as part of an initiative called "Operation Choke Point," focusing on actions where the payment processor had reason to know of a merchant's deceptive practices and continued to provide services. This focus was prompted by the FTC's view that payment service providers are vital gatekeepers against fraudulent activity, and that enforcement action against complicit or negligent payment processors could address a broader range of violative behavior than action against individual merchants. In recent years, the FTC seems to have renewed its focus on payment processors, bringing multiple enforcement actions and entering into consent orders to settle claims of unfair or deceptive acts or practices.

In a 2020 statement, FTC Commissioner Christine S. Wilson maintained that the FTC will "pursue appropriate law enforcement 'when a payment processor helps a fraudulent merchant take money from consumers – either by actively helping the merchant hide its fraudulent conduct from acquiring banks and payment networks or by turning a blind eye to the merchant's fraud.'"

The Impact on Internet Platforms

The FTC has more recently turned its attention to problematic behavior on social media platforms, particularly deceptive scams. According to an FTC report released in 2022, more than one in four people who reported losing money to fraud in 2021 said it started on social media with an ad, a post, or a message.[2] The data in the report indicated that social media was far more profitable to scammers in 2021 than any other method of reaching people.

2 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021

About 95,000 people reported roughly $770 million in losses to fraud initiated on social media platforms in 2021, which the FTC noted was an eighteenfold increase from just four years earlier. While enforcement action has generally not yet focused on internet platforms themselves, the reputational damage it causes can affect user numbers, user engagement, stock prices, employee retention, and more.

Products and Services Presenting a High Risk of FTC Scrutiny

The FTC has broad jurisdiction to combat deceptive practices regardless of the business type, with minor exceptions. However, businesses that have historically drawn the FTC's attention include:

- **Dietary supplements and cosmetics.** The FTC regularly pursues supplement and cosmetics sellers — including everything from fish oil to skin serums — for promoting their products with false claims as to their effectiveness or with other deceptive tactics. Beyond fraudulent marketing claims, though, dietary supplement and cosmetics sellers also present an elevated risk of deceptive sales techniques, such as negative-option billing and deceptive "free trial" offers. The FTC has actively pursued actions against payment processors that were found to be aiding fraudulent supplement merchants.
- **CBD.** Similarly, CBD merchants are frequent targets of the FTC for marketing their products with unsupported claims about their ability to treat serious diseases.
- **COVID-19-related.** The FTC has been doggedly pursuing sellers of fraudulent COVID-19 products and services. With expanded authority over these types of merchants, the agency is likely to continue its focus in this area.

- **E-liquids.** The FTC recently stated that it considers the failure to disclose material health or safety risks, such as the risk of addiction, on e-liquids to be a prohibited unfair or deceptive practice.
- **Alternative lending.** Merchants offering loans present a high risk of FTC scrutiny. The FTC has previously brought actions against lending companies with deceptive claims and practices, such as falsely promising loans would come with "no hidden fees."

5.2 UDAAP and the Consumer Financial Protection Bureau

In wake of the 2007-2008 financial crisis, the US government implemented several monumental pieces of regulatory legislation, most notably the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The Dodd-Frank Act created the Consumer Financial Protection Bureau, which is charged with protecting consumers against abuses related to credit cards, mortgages, and other financial products.

Included in this act are guidelines designed to protect American consumers, notably the prohibition of "unfair, deceptive, or abusive acts or practices" (UDAAP).

Defining UDAAP

The Dodd-Frank Act considers a practice as **unfair** when:

- It causes or is likely to cause substantial injury to consumers.
- The injury is not reasonably avoidable by consumers.
- The injury is not outweighed by countervailing benefits to consumers or to competition.

The Dodd-Frank Act considers a practice as **deceptive** when:

- The act or practice misleads or is likely to mislead the consumer.
- The consumer's interpretation is reasonable under the circumstances.
- The misleading act or practice is material.

The Dodd-Frank Act considers a practice as **abusive** when:

- It materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service.
- It takes unreasonable advantage of:
  - A consumer's lack of understanding of the material risks, costs, or conditions of the product or service.
  - A consumer's inability to protect his or her interests in selecting or using a consumer financial product or service.
  - A consumer's reasonable reliance on a covered person to act in his or her interests.

High-risk Businesses for UDAAP Violations

While any company could engage in UDAAP, certain business areas receive more scrutiny from regulatory agencies for violations than others. Following are some examples of high-risk business areas.

- **Credit repair.** Credit repair businesses often charge advance fees, mislead consumers about the benefits and actual costs of their services, and misrepresent the terms and limitations of their services.
- **Debt collection.** Actions typical of many debt collection agencies are specifically mentioned as UDAAP by the CFPB, including falsely representing the amount or legal status of debt, revealing the consumer's debt to their associates and

family without consent, and threatening actions that the service provider does not have authorization to pursue, such as arrest or prosecution for nonpayment.

- **Payday lending.** Businesses offering short-term loan solutions with excessive rates of interest sometimes obfuscate the terms of their loans, mislead consumers about the actual interest accumulated, or even attempt to collect on loans that are considered void.
- **Lead generation and sales.** Lead generators and sales people sometimes use deceptive marketing and language when describing the benefits and effectiveness of their leads, or even provide leads that are knowingly fraudulent and/or based on inaccurate information. Additionally, lead generators are responsible for verifying the legitimacy of businesses to which they sell information.
- **Extended warranties and service contracts.** Service centers have been the subjects of many CFPB UDAAP suits. Typically, the CFPB targets these businesses for intentionally misrepresenting both the price and scope of maintenance included in service contracts.

Tips to Avoid UDAAP Fines

Companies working with merchants, sellers, or advertisers can take several internal steps to avoid UDAAP violations and accompanying fines. These include:

- Properly responding to consumer complaints
- Performing internal policy audits
- Educating staff
- Practicing proper underwriting
- Reviewing existing UDAAP policies

Spotting Potential UDAAP Violations

In addition to internal steps, processors and acquirers should also know how to spot and detect potential UDAAP violations when onboarding and reviewing merchants. Relevant questions to ask of any merchant include:

- Are the advertised terms of the merchant services factually based and described accurately?
- Do they clearly inform customers of any and all fees associated with their services?
- Does the merchant unfairly target vulnerable demographics?
- Do customers receive the specific product or service that they request?
- Does the merchant charge for products and services that the customer has specifically agreed to?
- Does the profitability of the product offered by the merchant depend significantly on penalty or back-end fees, rather than upfront fees?

5.3 Deceptive Marketing

Marketing is one of the key practices susceptible to deceptive techniques. Online advertisers must abide by the same rules as any other advertiser and be not only truthful, but also be able to substantiate claims with applicable evidence. Merchants and online advertisers offering services with deceptive marketing may put internet platforms and payment service providers at a higher risk of regulatory scrutiny, and companies that run afoul of regulatory agencies may face monetary judgements.

For example, in 2020 a Latvian payment processor settled a complaint with the FTC that it enabled a deceptive "free trial" offer

scheme. The FTC alleged that Transact Pro illegally maintained merchant accounts that enabled a company offering "risk free" trials to evade credit card chargeback monitoring programs.

Identifying Potentially Deceptive Marketing

To protect their personal information and avoid predatory businesses, consumers can take steps to help determine if a product or service is engaged in potentially deceptive marketing. Scammers will often exploit a vulnerable or targeted group with products and/or services tailored to their specific needs. These businesses frequently market products or services that seem too good to be true, and may employ a sense of urgency or other high-pressure techniques to encourage consumers to act quickly.

Operators of these types of businesses may have multiple websites or social media profiles offering the same or similar services in the event one is shut down. Because the products or services offered may not be obviously problematic, these operators are often able to take advantage of online advertising to direct traffic to their websites. Below we go into detail about three examples of deceptive marketing for vulnerable or targeted groups.

Fake Job Opportunities and Résumé Repair Services

Looking for work can be a stressful experience, and many job hunters seek out resources to better position themselves with prospective employers. Some have turned to online career-building services that promise not only to improve their résumés, but even guarantee high-paying job placement afterward. However, if a job opportunity sounds too good to be true, it probably is.

In February 2019, the FTC charged two companies and their owner for participating in a fraudulent job-placement and résumé-repair operation that utilized misleading claims about high-paying positions that didn't exist. According to the FTC, the companies "...

deceived job seekers with false claims that those who used their services had a 100 percent interview rate and over an 80 percent placement rate."

After messaging targets through LinkedIn and other social media platforms, the operator persuaded people to pay up to $2,500 to get access to "unadvertised, highly paid executive positions" that did not exist. Many of these customers were subsequently lured into paying an extra fee for résumé repair services. According to the FTC statement, customers were told that their original résumés failed to meet the high standards necessary for the bogus position, and in order for them to be eligible for job placement, they first needed to fix their résumés — using the services of a company under the control of the same operator. The defendant operated multiple DBAs, a technique that may have been used to avoid detection and regulatory scrutiny.

Examples of websites presenting an elevated risk for deceptive job and résumé-repair services.

Red Flags: Job Opportunities and Résumé Repair

- They request money from individuals to access job listings or interviews.
- They require customers to pay upfront for job placement services.

- They have a common website template and list fake-looking positive reviews.
- They have many negative consumer reviews on third-party platforms, such as bbb.org or ripoffreport.com.
- They will often be associated with one or more websites set up with similar services.
- They will often use implied endorsements by well-known brands and/or celebrities.

"Risk Free" Trial Offers

As mentioned in Chapter 3, negative-option billing, also known as continuity marketing, is a practice in which the consumer's failure to reject an offer or cancel an agreement is interpreted as confirmation that they want to be charged for goods and/or services. Essentially, these merchants are misleading their customers into signing up for subscriptions or recurring purchases without customers' express consent.

Merchants engaged in this practice pose risk for regulatory and card brand scrutiny, as well as elevated risk for chargebacks. Furthermore, Congress has stated in its Online Shopper Protection statute that it is illegal for merchants to sell online using a negative-option feature unless certain conditions are met regarding transparency, informed consent, and easy cancellation practices.

"Risk-free" trials are a common technique used in negative-option billing models. As shown in the following image, websites often try to create a sense of urgency by describing supplies as limited or listing countdowns for offers. This can push consumers to act before they have read the fine print.

Example of a negative-option billing merchant offering cosmetics.

In November 2019, the FTC announced it was mailing 79,771 refund checks totaling more than $1.8 million to consumers who thought they were signing up for risk-free trial offers but were actually enrolled in negative-option billing for seemingly popular skin care products. By providing their payment information to cover the cost of shipping fees, consumers were unwittingly signing up for unauthorized recurring monthly charges.

In this particular case, seven individuals and 15 companies selling Auravie, Dellure, LéOR, and Miracle Face Kit skin care products were charged for "risk free" trials alleged by the FTC to be deceptive. Additionally, the defendants were also charged for implied endorsements by misrepresenting themselves as accredited by the Better Business Bureau, in violation of the FTC Act.

For more information on negative-option billing, see Chapter 3.

Assistance Animal Documentation

According to the US Department of Housing and Urban Development (HUD), an assistance animal "is an animal that works, provides

assistance, or performs tasks for the benefit of a person with a disability, or that provides emotional support that alleviates one or more identified effects of a person's disability." Unlike a service animal, it is not required to be trained.

In November 2019, HUD Secretary Ben Carson sent a letter to the FTC requesting the commission to investigate websites offering certificates or other documentation for assistance animals. According to the Secretary, some online advertisers have been taking advantage of individuals with disabilities who may not know what is required as proof of reasonable need for their assistance animals. Furthermore, these companies may be cashing in by misleading consumers into believing they need to spend hundreds of dollars for a sham piece of documentation to keep their assistance animals in their homes. In order to appear legitimate, these operators will often use language that implies an endorsement by the federal government, or design their website to look and feel like an official government website.

In addition to misleading individuals with disabilities, online scammers may also facilitate the sale of bogus documentation to individuals who do not actually have a disability, for the purpose of enabling pet owners to evade pet fees and/or breed restrictions for travel or other public situations in which pets are typically restricted.

The online verification process often entails a questionnaire that ostensibly is evaluated by a mental health provider. However, according to HUD's letter to the FTC, "These certificates are not an acceptable substitute for authentic documentation provided by medical professionals when appropriate."

Furthermore, according to the US Department of Justice's Civil Rights Division on Disability Rights, "There are individuals and organizations that sell service animal certification or registration documents online. These documents do not convey any rights under

the [Americans with Disabilities Act] and the Department of Justice does not recognize them as proof that the dog is a service animal."

Examples of websites presenting an elevated risk for deceptive animal assistance documentation.

Red Flags: Animal Assistance Documentation

Potentially deceptive websites offering animal assistance documentation often advertise through internet platforms. Their websites may use designs to make them look official or affiliated with the government.

Marketing that may trigger regulatory scrutiny includes:

- "No More Unfair Pet Deposits"
- "Avoid Breed and Size Restrictions"
- "No More Unfair Airline Fees"

5.4 Typosquatting

Typosquatting is a deceptive tactic typically intended to trick internet users into visiting websites they believe are operated by a trusted entity. Instead, the websites may attempt to steal a user's information, sell counterfeit products or services, or engage in other forms of illicit activity that can harm consumers and damage brands.

What is Typosquatting?

Typosquatting refers to the registration of a domain name intended to mimic another domain name to entice internet users to click the link. Typosquatting takes advantage of various ways to imitate an existing domain name, such as intentional typos or visual deception intended to mimic the appearance of a domain name. Sometimes, this practice is also referred to as URL hijacking, brandjacking, or cybersquatting.

Typosquatters capitalize both upon genuine typographical errors that an unwitting user might enter — for example google.cm or golgle.com — as well as visually deceptive domain names an internet user might not immediately recognize as falsified.

Typosquatting may infringe on trademarks and can deceive consumers into believing they are visiting websites operated by a trusted entity. Typosquatting is used commonly as a phishing tactic. It allows fraudsters to send email messages to internet users under the guise of a trusted entity such as a social media brand or a bank, when in reality the domain name registrant is a malicious actor intending to abuse consumer trust to steal sensitive information.

To combat this activity, proactive registration of typosquat domain names is a key brand protection tactic. For example, faceboook.com is registered to Meta, and automatically redirects to the primary website, facebook.com. This proactive registration prevents the domain name from being registered by a malicious party. Sometimes, registrants will essentially hold the domain names ransom, offering to sell them to a brand holder at an exorbitantly high price.

Methodologies of Typosquatting

Typosquatting can take many forms that vary substantially in sophistication. Some are ham-fisted and low-effort, while others are highly

sophisticated. Below are some of the techniques LegitScript analysts commonly encounter:

Typographical errors and misspellings: The most straightforward way to typosquat is to mimic a typo that an internet user might genuinely make, such as twittter.com. This generally is intended to redirect traffic from internet users who are manually typing in domain names.

Abuse of TLDs and ccTLDs: More than 200 country code top-level domains (ccTLDs) exist — providing the possibility for hundreds of variations on a domain name. The most commonly used TLD in the world is .com and, as such, similar domain extensions have increased potential for abuse. For example, .cm — the ccTLD for Cameroon — is widely abused by cybercriminals to mimic their .com counterparts. In 2018, the cybersecurity blog krebsonsecurity.com found that millions of visits to .cm-registered typosquat domains (including espn.cm, aol.cm, and itunes.cm) occurred within only a few months. Another ccTLD abused for its similarity to .com is .om, which is the ccTLD for Oman. Extensions such as .co, .co.uk, and .ca are also sometimes exploited for their relative visual similarity to .com.

Adding trailing text: One method cybercriminals sometimes rely on includes adding additional text to a well-known domain name. For example: netflix-user.com. Because many brands do, in fact, have special domains for specialized purposes, this may mislead users. Brands can protect themselves from this by consolidating activity to their root domain, and primarily relying upon subdomain for specialized purposes; for example, user.netflix.com.

Adding in preceding text: Attackers are one step ahead of the use of subdomains and will often mimic the appearance of a subdomain with a hyphen; for example: user-netflix.com.

Adding in www, http, or com: In a common "preceding text" variant, attackers will add in common pieces of the URL as part of the domain root; for instance: www-apple-id.com.

IDN homograph attacks: A potentially tricky typosquatting variant is the Internationalized Domain Name (IDN) Protocol homograph attack, which exploits similarities in characters belonging to different writing systems. For example, the Cyrillic "o" is nearly indistinguishable from the Latin "o."

Domain names that do not contain Latin characters are represented by Punycode, which allow conversion of Unicode characters to the limited character set supported by the DNS, and are used to encode internationalized domain names. Punycode sequences have the prefix "xn—." The following example — in which the Latin "o" in "icloud" is replaced with a Cyrillic "o" — demonstrates the difficulty of visually distinguishing these characters.

Domain Name (Unicode)	Destination
icloud.com (Latin "o")	icloud.com
icloud.com (Cyrillic "o")	http://xn--iclud-o29a.com

Most web browsers have certain measures in place to make these deceptions more apparent to the user. For example, pasting a domain name containing characters from multiple writing systems into Chrome or Firefox will result in the punycode being displayed in the URL bar.

Other homograph attacks: Attackers can also use Unicode characters to mimic other Unicode characters. The characters "a" and "o" can be interchanged; for example: opple.com. Similarly, a

lowercase "l" is sometimes interchanged for an "i;" for example: appleId-apple.com.

Preventing Typosquatting

Typosquatters are both prolific and creative, and there is no one-size-fits-all solution to protect yourself or your customers. However, consumers, rightsholders, internet platforms, and payment service providers can protect themselves by following basic protocols:

- For payments companies, watch out for merchants applying for merchant accounts with domain names that are suspiciously similar to well-known brands. For social media platforms, watch out for users promoting these domain names.
- Carefully scrutinize merchants or users promoting domain names that include common typosquatting techniques, such as starting a domain name with "www-."
- Invest in monitoring services, such as those provided by LegitScript, to quickly flag suspicious merchants who may be engaged in phishing, IP infringement, or other problematic activity.

5.5 Geo-targeting, Technology Targeting, and Cloaking

Most internet users are familiar with how services such as search engines and business directory services use geo-targeting to deliver the most relevant content to users based on their locations. For instance, people searching for pizza online likely want search results near where they live. Geo-targeting is therefore extremely useful in search engine optimization (SEO).

However, illicit operators also use these techniques to evade enforcement and hide their illicit activity from internet companies and payment service providers.

Geo-targeting, Technology Targeting, and Cloaking Explained

Geo-targeting and technology targeting are useful tools that enhance the browsing experience, typically based on characteristics of the user.

- **Geo-targeting** refers to the method of delivering different content to consumers based on their geographic locations.
- **Technology targeting,** or user-agent targeting, targets users based on their specific browsers, operating systems, or devices.
- Finally, **cloaking** is the method of delivering different content or URLs to human users and search engines.

These technologies have legitimate and important uses. Almost anyone operating online — from local businesses, internet search platforms, websites, and phone apps — uses geo-targeting and technology targeting to deliver what they believe is the most relevant data to users based on their locations and demographics. For example, to maximize user experience and ease, a website can display different languages and currencies based on visitors' geographic locations.

Geo-targeting can also be used to manage intellectual property content. One of the classic examples of such intellectual property content is streaming television. Due to licensing rights, services such as Hulu and Netflix may not provide streaming services, or only provide certain content, to customers outside of the US.

Online websites selling products that might be restricted or prohibited in certain countries may also use location detection to restrict shipping based on a visitor's geographic location. Websites may also geo-target and display different results based on the availability of shipping locations.

Illegitimate Uses of These Technologies

Bad actors can also use geo-targeting and technology targeting to evade enforcement. Websites engaging in questionable or even illicit behaviors may only show high-risk content to visitors in certain geographic locations or users with specific device types, while showing innocuous content to visitors from another specific geographic location or using another device type.

For example, the now-defunct website zh-jhjs.com, shown below, appeared to be a legitimate packaging supplier on a desktop browser (although sharp eyes will notice the IP-infringing Alibaba logo at top).

On a mobile device, however, the website showed misleading news content marketing high-risk supplements. The website pretended to be a legitimate news website and even featured celebrities who

likely did not endorse the products being sold. The "news" content is lathered with outrageously misleading weight loss claims such as "30 lbs of stomach fat loss in just 1 month." Similar marketing tactics have been cited by the FTC as deceptive.

Another example is the now-defunct arizona19.club, shown in the following image on the left, which appeared to be a website showing generic information about the state of Arizona to crawlers. However, LegitScript was able to detect that the website redirected to a rogue pharmacy website belonging to the PharmEmpire network, shown below on the right.

Cloaking Uses

Cloaking — a controversial practice that is sometimes called "transaction laundering of the advertising space" — is typically considered

a form of "black hat" SEO. In fact, cloaking is considered a violation of many search engines' and social media platforms' policies because it can serve users with different results than they expected. Furthermore, in many cases, cloaking can also be used to affect search engine rankings by fooling the search engine's algorithm. Illicit advertisers engaging in questionable behaviors may also use cloaking to evade detection by crawlers and/or ad reviewers.

When a website is hijacked (see Section 6.6), the hijackers can also use cloaking to make it more difficult for the primary website operator to detect the intrusion. Violative content may only show in particular instances. This can make it difficult for search engines to catch and enforce hijacked content.

How These Technologies Are Implemented

Geo-targeting, technology targeting, and cloaking can have similar but different methods. A geolocation can be detected via a website visitor's IP address, device ID, GPS signals, and more. Some of the methods cloakers use may include:

- Collecting and recording IP addresses that visit the page, and blocking questionable ones;
- Detecting a visitor's referral URL and/or user agent HTTP header and blocking ones that look as if they might be coming from a content reviewer or a crawler;
- Banning or showing different content to visitors in a specific geographic location where content reviewers or enforcement agencies may be located; and
- Oftentimes, these websites utilize scripts such as PHP scripts, which are the components embedded in HTML codes, to make their websites behave dynamically, including delivering different content to different users.

5.6 Website Hijacking

Hijacked websites are ones whose primary purpose appears to be obfuscated or compromised without the registrant's consent, and which display or redirect users to clearly unaffiliated content. In other words, a hijacked website shows signs that the merchant has either lost control of their website, or that third-party content has been injected or uploaded without consent, and is contrary to what reasonably appears to be the domain name registrant's intended purpose.

Risks to Payment Service Providers

Although website hijacking may not be explicitly prohibited by payment processors, compromised merchant accounts are the primary concern when LegitScript uncovers active hijacking behavior. In addition, such merchants carry additional general reputational risk due to the proximity of the potentially illegal activity to the payments relationship.

Since illicit e-commerce merchants are prohibited from participating in most mainstream forms of online marketing, many resort to malicious takeovers of innocuous websites. Hijacking is a technique typically used by criminals to further their criminal activities, and hijacked websites become "hosts" or "facilitators" of illicit content once malicious code is introduced. These techniques not only corrupt the user experience, but they can also manipulate internet search platforms into vehicles for illegal activity, thus increasing the risk for payment providers, e-commerce platforms, and the general public.

Identifying Hijacked Websites

One of the clearest indicators of a hijacked website is that it will display illicit content only when accessed via an internet platform's

search results but appear innocuous when accessed by typing the URL into the address bar. As many websites rely on search visibility to attract visitors, the inclusion of problematic content can devastate legitimate visitor traffic and ward off potential customers. The effect on individual websites also impacts the internet platforms themselves, as contaminated search results can confuse and discourage users.

Redirection Hijacking

The two most common types of hijacking are a **redirection hijack** and a **content injection hijack.** A redirection hijack is when a hacked website is used as a springboard to automatically redirect to an illicit website.

Fake webpages are embedded into the website, typically with filenames that mimic the genuine content as a way to evade detection. If those pages are accessed via search results, visitors are taken to the legitimate website before being quickly redirected to an illicit one. However, visitors who access the root domain name of the website may never see the illicit content.

For example, a French-language medical supply website displayed illicit content in search results. From the search results alone, it appeared that the site hosted several webpages marketing drugs for sexual enhancement. Visitors who clicked on one of those webpages were taken to the correct URL initially, but then quickly redirected to a rogue internet pharmacy website.

Google search results (left) redirected users to a rogue internet pharmacy (right).

Although the redirect was executed in a fraction of a second, while the browser was loading, the source code on the webpage provided indicators that the website was hijacked.

Content Injection Hijacking

Rather than redirecting to another website, some hacks insert code into an existing website so that the illicit content appears within the hijacked website. This is the second common type of hijacking, a content injection hijack. Content injection can take the form of random links or drug-related keywords peppered into the genuine website text, or it can appear as though an illicit website itself is hosted within the innocuous website.

For example, Google search results for a private social club showed a rogue subpage promoting erectile dysfunction drugs. The content of the subpage didn't appear to be related to the rest of the website. However, when accessing the page from the search results the browser remained on the innocuous website, even though it displayed content that looked like a complete internet pharmacy website within the page. The false website appeared to be an image. When clicked, it directed visitors to the actual internet pharmacy website, mymedicstar.com.

The website for a social club (left) displays problematic injected content that when clicked directed users to a rogue internet pharmacy (right).

As search engines, social media platforms, and other internet businesses get better at stopping legitimate avenues of promotion for illicit businesses, merchants and payment service providers are likely to see an increase in hijacked websites.

CHAPTER 6

Fraud and Scams

E-commerce is gaining an ever-larger share of the retail market, with more than $4.2 trillion in online sales occurring worldwide in 2020 alone, according to the Adobe Digital Economy Index. Alongside the boost in legitimate sales are scammers who hope to take advantage of this growing market. According to the FTC, consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 percent over the previous year.

Fraudsters are drawn to the internet by the increased anonymity and relative ease and cost with which they can enact their scams. Fake identities, bogus social media accounts, and premade website templates are just some of the tools in an online scammer's toolkit. In this chapter, we highlight some of the most common and pervasive scams occurring in merchant portfolios and on e-commerce platforms.

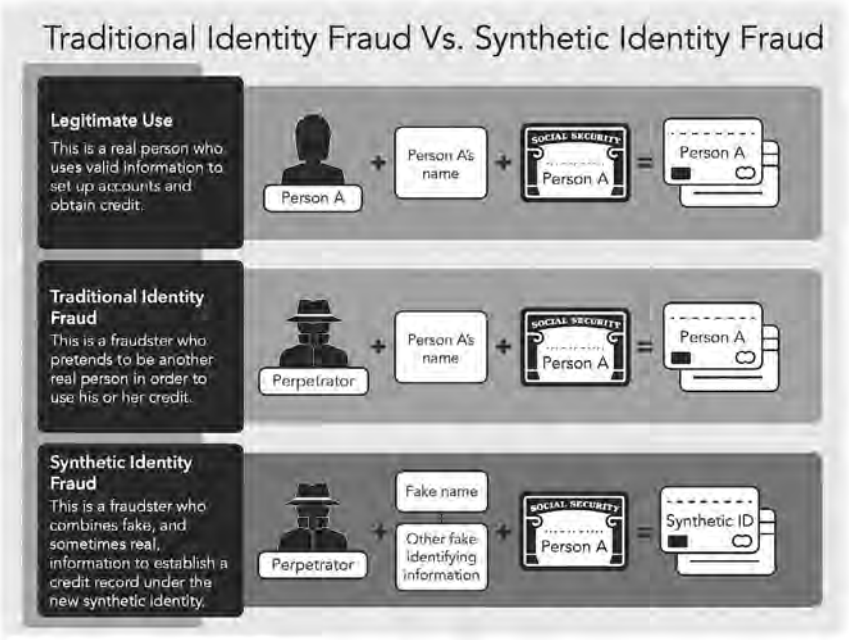
6.1 Synthetic Identity Fraud

In recent years, a novel form of fraud has emerged: fraudsters combine elements of stolen identities and wholly fabricated information to create patchwork "synthetic" identities to obtain access to financial services, such as credit, loans, and merchant accounts. This combination of genuine and fabricated details render these identities increasingly difficult to detect as fraudulent, putting the payments community and the public at risk.

How Synthetic Identity Fraud is Evolving

Synthetic identity fraud differs from traditional identity fraud in a few key ways. With traditional identity fraud, a criminal pretends to be another person — using all the victim's stolen information — to gain access to his or her credit. With synthetic identity fraud, a criminal uses a blend of real and falsified information to establish a credit record under a new synthetic identity.

See the following illustration to better understand the difference between traditional identity fraud and synthetic identity fraud.



While synthetic identity fraud has previously been most commonly associated with credit fraud through the banking industry, a similar pattern has been developing in the online payments industry. Fraudsters now use these same synthetic identity creation techniques to open online merchant accounts en masse.

These merchant accounts can be highly profitable for fraudsters, who can use them for transaction laundering, card testing,

card cashing, and other forms of fraud. These parallel forms of fraud are interrelated: fraudsters have fraudulently opened credit cards to buy nonexistent goods through merchant accounts they control.

Methods of Synthetic Account Creation

The primary innovation behind synthetic identities that renders them so difficult to detect is that elements are derived from real identities rather than being entirely manufactured. Synthetic identities contain elements of truth, and in some cases may even appear to be connected back to verifiable people, enabling them to more effectively trick existing KYC controls.

Several recent developments have paved the way for a surge of synthetic identity fraud in the US, including many advancements that have had unexpectedly problematic consequences:

- **Increased automation of financial services.** In the payments industry, the frictionless onboarding process, coupled with the wide availability of e-commerce templates, mean that fraudsters can spin up a large number of accounts with relative ease and speed.
- **Randomization of social security numbers** (SSNs), beginning in 2011, made it more difficult to verify SSNs and thereby simplified mass generation.
- **Large-scale data breaches,** such as the 2017 Equifax breach, exposed enormous amounts of consumer data that is now cheaply available on the dark web. Drivers licenses have sold for as little as $20 each, and social security numbers have sold for as little as $1 each.

"Aging" Synthetic Accounts

Real people have real histories and leave a trail of established records that contribute to a deeper, established identity. By contrast, a

synthetic identity, cobbled together from disparate data points, has nowhere near this level of depth or verifiable history. To create the appearance of legitimacy or trustworthiness, fraudsters frequently "age" their fraudulent merchant accounts or synthetic identities to establish history and the facade of legitimacy. Fraudsters and bad actors dramatically increase an account or identity's value by developing its history and apparent trustworthiness over time before using it to commit fraud.

With changes being implemented to online SSN verification (eCBSV) in 2022 and beyond, LegitScript expects fraudsters will have created a significant number of accounts and synthetic identities to age before the enhanced verification procedures are fully adopted.

Risks of Synthetic Accounts

According to recent analysis from Juniper Research, losses from online payments fraud are expected to exceed $200 billion between 2020 and 2024. In the world of online payments, the use of synthetic account data to create online merchant accounts is also a significant emerging risk.

Some of the specific financial risks include:

- **Transaction laundering.** Fraudsters' ability to create merchant accounts en masse poses significant risk for transaction laundering by enabling them to easily spread charges for violative products and services across a wide range of camouflaged merchant accounts. The potential for obfuscating violative activity makes this a significant challenge for the payments industry. See Chapter 7.
- **Card testing.** With access to nearly unlimited merchant accounts, fraudsters can easily test stolen credit card

information, paving the way for large payouts and creating large financial losses.

- **Card cashing.** Fraudsters can make cash withdrawals from their victims' credit lines, or can alternatively use the stolen cards to pay themselves by purchasing non-existent products from merchant accounts under their own control.
- **Chargeback spreading.** An account's chargeback rate is a common risk indicator, but synthetic identity theft enables fraudsters to operate a large enough number of accounts that they may not draw elevated scrutiny for chargeback rates.

Additionally, there are significant risks to consumers from rampant identity theft, particularly to vulnerable populations, such as children and the elderly.

Characteristics of Synthetic Accounts

Synthetic accounts can be difficult to identify since they are an amalgamation of real and fabricated personal information. At a cursory glance, many of these accounts may appear genuine. However, under careful scrutiny, the facade begins to melt away. Focusing on individual data points of synthetic accounts is unlikely to yield useful results, as many of the data points have been co-opted from real identities. But if we zoom out and observe these data points as pieces of a larger picture, fraud patterns often become apparent.

Fraudsters tend to open many accounts at once to minimize their loss in the event of detection and to spread the risk over multiple payment access points. In the name of efficiency, these fraudsters often take shortcuts while opening a large volume of accounts, which creates patterns of identifiable fraud. Such patterns include numerous accounts opened under the same merchant name or email address. Some similarities can also exist around shared merchant descriptors or a common physical business address.

Another common tactic used by synthetic accounts is to provide falsified URLs and names of businesses that have long been established to appear legitimate.

Impersonating an existing company makes it possible to quickly set up accounts with merchant processing providers to begin running transactions with stolen card information. Free email services such as ProtonMail and Tutanota allow fraudsters to create accounts without requiring two-factor authentication, and can even allow them to spoof their email addresses so that they appear to be associated with the established organization they're using to apply for a merchant account. Slight typographical errors in spoofed email addresses or a mismatch between the merchant's name, email, and the URL on the merchant application can be hallmarks of synthetic accounts. Further red flags should be raised if the contact information of the merchant account does not match the contact information listed on

the merchant's website. Observing anomalies in identity elements and the payments behavior can expose these accounts.

Mitigating the Risks of Synthetic Accounts

Synthetic account creation is a significant threat to the financial services industry, and can be used to precipitate numerous financial crimes that can touch every sector. The fraudsters move quickly, usually create accounts in groups, and may obscure themselves behind semi-plausible combinations of real and fake identities. Risk and compliance teams can get ahead of the threat through a combination of strong know your customer (KYC) measures and devoting investigative resources to pattern detection.

Knowing these accounts are not set up using genuine identities, KYC measures are the first natural line of defense. The use of genuine personal information sourced from data breaches can make this more challenging than it would first appear. Names, addresses, SSNs, and business names can be easily sourced from public records, but email addresses and phone numbers are often more difficult to plausibly match to the identity and can be a weak point in the synthetic identity.

This is because phone numbers and email addresses are so commonly used for account communications and two-factor authentication. The attacker is, of course, disincentivized from using the person's real phone number or email address because they don't control it. So the contact telephone number and email address are, on balance, more likely to be controlled by the attacker.

Email address patterns to look for can include:

- Email addresses containing a personal name with no apparent relationship to the provided merchant name;

- Email addresses followed by a long string of numbers, which is often a default configuration of email service providers;
- For accounts apparently belonging to large companies or organizations, the use of personal email addresses may be a risk factor, particularly when other risk factors are also present;
- Email addresses that are created using free email services, including mail.com clones.

None of these factors alone is necessarily indicative of synthetic identity fraud, but these are all important KYC considerations. Similarly, merchant phone numbers may provide clues. Are there records of that phone number being associated with the merchant? Is the phone number a Voice-over-Internet-Protocol (VoIP) number?

LegitScript's approach to synthetic identity fraud is primarily based in network analysis and pattern detection. An anomalous account is usually tied to many more following similar falsification patterns. For this reason, we recommend devoting investigative resources — whether from an investigative analyst team, technical solutions, or both — to make sure KYC is not the only control in place.

6.2 Crowdfunding (Aggregation) Scams

Crowdfunding is the practice of funding a project, new idea, or business venture by raising typically small amounts of money from a large number of people. Campaigns are commonly set up to collect donations for charities, entrepreneurial projects, and individuals' personal needs. While crowdfunding websites are the most obvious platforms for raising money online, problematic crowdfunding campaigns can also appear on social media and virtually any platform that accepts user-posted content.

Crowdfunding scammers frequently pose as a legitimate charity, business, or individual to lure donors and investors. Their

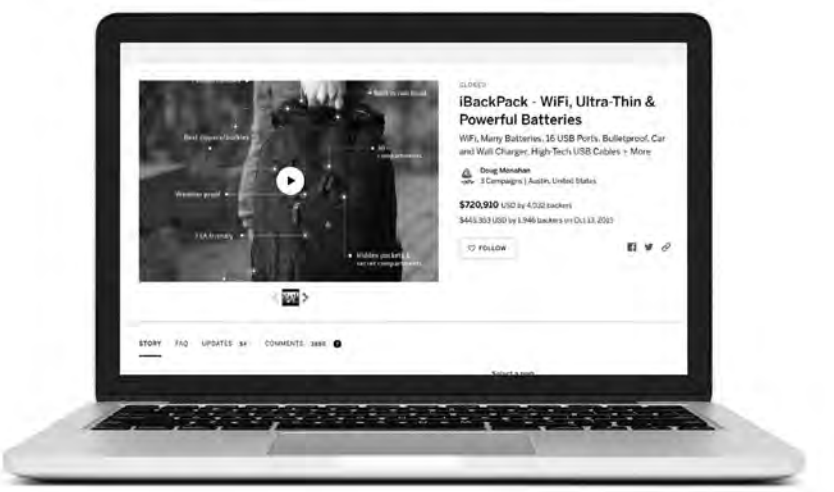
pitches vary widely: some promise fantastical products, some solicit donations for fake charities, and others appeal for help for fabricated plights — such as medical bills, college funding, loved ones in need, etc.

While the pitches are different, the result of these scams is often the same: fraudsters eventually disappear, leaving donors and consumers without a promised product or with the uncertainty that their contributions helped in the way they had hoped.

Crowdfunding Case Study: iBackPack

In 2019, the FTC filed a complaint against the operator of crowdfunding campaigns who was purportedly raising money to develop a high-tech backpack known as iBackPack. Douglas Monahan first started his campaign on IndieGoGo in 2015, pitching a backpack that would include built-in batteries for charging mobile devices, RFID-blocking pouches, a USB hub, a Bluetooth speaker, and a mobile hotspot for portable wifi connection. Monahan raised more than $720,000 from this first campaign, yet investors claimed they never received the backpacks promised them. Monahan raised an additional $76,000 in 2016 after creating another crowdfunding campaign on Kickstarter, this time called iBackPack 2.0, which also failed to deliver a completed version of the project to its backers.

While investors in new products on crowdfunding platforms assume the risk that their investment may never come to fruition, the FTC alleged that Monahan used a large portion of the nearly $800,000 he had raised for personal expenses. In 2020, Monahan reached a settlement with the FTC, which permanently banned him from engaging in crowdfunding activities in the future.



According to the FTC, the creators of the iBackPack campaign made representations to Indiegogo's staff that the product was being produced and delivered, in an effort to continue their fundraising efforts. The creators purportedly told Indiegogo's staff that they were in the "full production and shipping phase" and had already shipped the iBackPack to "hundreds if not thousands" of contributors while at the same time telling backers that production of the iBackPack had been delayed nearly a year.

Problematic Crowdfunding Red Flags

- The pitch for the product, service, or event sounds too good to be true.
- The organizers are unclear or purposefully vague about how donations to the campaign will be used.
- The person/company/charity has initiated numerous crowdfunding campaigns in the past. Review the outcomes of those campaigns.
- The campaign is raising money for urgent causes, such as disaster relief. While many of these may be legitimate, scammers frequently exploit people's desire to help in a crisis.

- Comments from backers express dissatisfaction at the progress of a campaign or raise concerns about its legitimacy.

6.3 Counterfeits

One of the most pervasive problems for online marketplaces and e-commerce platforms is the sale of counterfeit goods. Virtually any item is at risk of being faked, but the most popular targets include designer clothing, sports jerseys, footwear, cosmetics, small electronics, and popular brand-name toys. Scams such as these frequently appear on discount marketplaces, but are also marketed on social media and other forums. Counterfeiters may take a variety of approaches in marketing their products. Some list their products as authentic, including fake documentation to prove the product's "authenticity." Others may appropriate a trademarked logo but explicitly market their products with terms such as "UA" (unauthorized authentic), "clone" or "replica." While scammers typically market these products with prices far below the market rate to entice consumers, some customers have paid full price for presumably authentic items that are in reality cheap knockoffs.

Counterfeit Case Study: everymemorabilia.com

In May 2021, a Maryland man pleaded guilty to federal charges alleging that he sold fake autographed memorabilia online. Douglas Duren allegedly ran the websites everymemorabilia.com, neautograph.com, and awesomememorabilia.com between 2010 and 2019, through which authorities alleged he sold products such as sports equipment, book and movie posters, and photographs with "celebrity autographs." In reality, authorities alleged Duren bought these retail items before forging the autographs himself and reselling the memorabilia at high costs, such as a Miami Heat basketball jersey ostensibly signed by Lebron James that was listed for $375.

Duren's websites included language asserting authenticity of the products for sale: "We have inexhaustible sources and unique professional contacts throughout Hollywood and the entire movie industry, such as working industry professionals, managers and agents, rare memorabilia traders, movie premiere attendance's [sic], and information on personal signings. This avenue of contacts insures we can find and acquire your memorabilia treasures. Each poster comes with a Certificate of Authenticity. This certificate insures the signed item to be genuine, and accompanies the item if you ever want to re-sell it, in the future."

Counterfeit Product Red Flags

- Brand-name products are listed at suspiciously low prices.
- The website has an unprofessional design or poor user experience.
- The domain name includes a brand name or an iteration of one but does not appear to be an official website.
- Product descriptions use keywords that denote a replica's quality, such as "AAAA," "AAA+," and "1:1."

- The website offers no option to pay with credit or debit card.
- The business has poor customer reviews or complaints on third-party platforms.
- The website has unclear refund policies.

For more in intellectual property infringement, see Chapter 8.

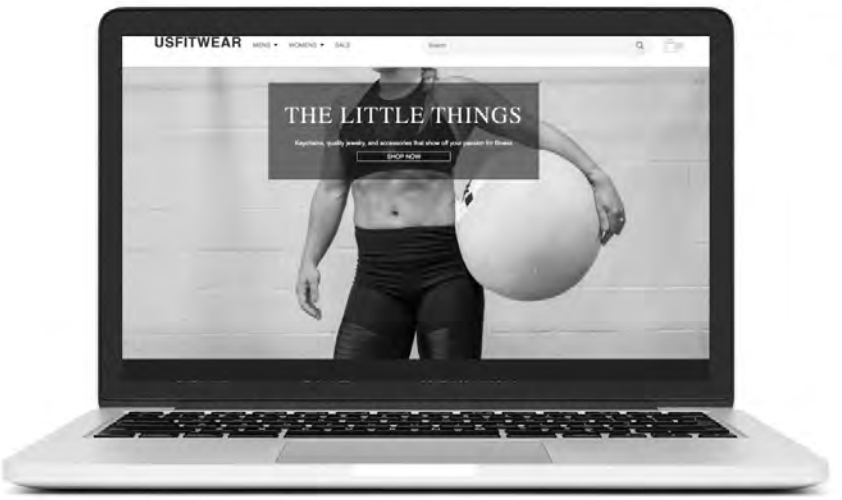
6.4 Nondelivery Schemes

Nondelivery scams occur when a consumer purchases a product that is never delivered (and which the merchant typically never has possession of in the first place). These scams can be difficult to spot because oftentimes consumers don't realize they've been scammed until long after their payment has been processed. Nondelivery scammers market their products across social media and e-commerce platforms, typically redirecting consumers to their own websites. Products can include anything, but these websites most frequently market drugs, luxury items, popular electronics, exotic or highly sought-after pets, and other in-demand or hard-to-find products.

Nondelivery Case Study: usfitwear.com

In May 2020, the Better Business Bureau (BBB) released a consumer warning regarding the online retailer usfitwear.com. BBB reported more than 100 complaints and several Scam Tracker reports pertaining to nondelivery of goods purchased from the website. According to BBB, complainants alleged that they never received their purchases — which ranged from exercise apparel to products as large as above-ground pools and trampolines — and reported that they were unable to reach anyone through usfitwear.com to lodge their complaints. BBB noted several red flags on the website, including limited payment options and conflicting contact information. The contact phone number on usfitwear.com corresponded to a New York area code, but the physical address listed on the website placed

the company at a seemingly unconnected residential address in Alabama, according to BBB. At the time the consumer warning was released, none of the complainants reported having received their orders, and the website is now offline.



The domain name usfitwear.com was registered in February 2020, just a few months before the BBB's consumer warning. The registrant's name and information were hidden using privacy-protection services, which makes it difficult to know who is operating a website. The operator was using a major payment facilitator to accept payments.

Nondelivery Red Flags

- The website has limited payment options, in particular methods that offer little recourse for refunds such as Western Union, money orders, gift cards, and cryptocurrency.
- Products are priced far below market value.
- There is a "kitchen sink" product lineup that includes an incongruous assortment of offerings.

- The website looks hastily thrown-together, with little or no contact information.
- The contact information and/or address provided on the website hold no connection to the supposed business, and the business has no other internet presence.
- The domain name has been recently registered.
- There are pervasive complaints on third-party review platforms.

6.5 Easy-Money Scams

Easy-money scams (also called get-rich-quick schemes) offer the promise of fast cash with little to no work required, typically through jobs such as mystery shopping, multilevel marketing, or "investment opportunities." These scams most commonly appear on advertisements and social media offering quick ways to make money from home. Consumers are lured in by the promise of fast payouts; however, many of these postings are scams that can yield significantly less than the promised compensation, provide no compensation at all, lead consumers into debt by requiring them to invest in "amazing opportunities," or unwittingly rope consumers into more serious forms of fraud.

These schemes are especially problematic because they may prey on vulnerable populations, such as the poor and the elderly. With some so-called "investment opportunities," victims have lost thousands of dollars; in other circumstances, victims have divulged personal data that scammers then used to establish merchant accounts used for transaction laundering.

Easy Money Case Study: My Online Business Education (MOBE)

In 2018, the FTC filed a complaint against an international business coaching program known as My Online Business Education (MOBE),

accusing them of swindling US consumers out of hundreds of millions of dollars. According to the FTC, the business claimed to have a proven 21-step system "for making substantial sums of money quickly and easily from internet marketing," in which consumers would pay an initial fee of $49 for access to the program. However, participants alleged that after the original $49 payment, they were bombarded with sales pitches for high-cost membership packages that were supposedly required in order to progress through MOBE's 21-step program. The complaint cited misleading advertising by company affiliates on social media such as, "How a Baby-Faced 22-Year-Old College Dropout Just Crossed $1 million" and "... even people in their 80s are making money by following 21 simple steps." The actual purpose of the program, according to victims, was to teach them how to sell MOBE's classes and memberships to their own friends and family rather than to train as entrepreneurs as promised. MOBE ultimately reached a settlement with the FTC in 2020, agreeing to pay more than $17 million.

The FTC alleged that operators of this scheme also made it difficult to receive refunds: "In addition to their false and unsubstantiated claims that consumers will earn substantial income by joining

the MOBE program and purchasing these costly memberships, Defendants also make false and misleading refund and money-back guarantees to induce consumers to purchase MOBE memberships. After consumers pay, however, Defendants require these consumers to sign post-purchase agreements that seek to impose onerous conditions for obtaining a refund, or that claim in other instances that the purchases are non- refundable and final. Defendants often cite to the language in these post-purchase agreements to deny refund requests or dispute chargebacks."

Easy Money Red Flags

- The promised compensation sounds too good to be true.
- The company asks people to pay upfront for a job opportunity.
- Unsolicited emails promise quick payouts for little effort.
- The business has many negative reviews on third-party complaint websites.
- The company asks to use a consumers' personal data and/or credit.

6.6 Romance Scams

Romance scammers typically adopt fake online persona with the purpose of gaining their target's trust and affection, which they manipulate in order to extract money or other gifts from their target. They are one of the most popular and quickly growing scams on the internet, with the FTC reporting a 50% increase in romance scams between 2019 and 2020, and an estimated $304 million lost to these scams in 2020 alone. These scams most commonly appear on dating apps; however, the FTC has also reported a significant rise in scammers approaching their targets through fake social media

accounts. Anywhere there is user-posted content, romance scammers may be a threat.

The most sophisticated scams involve criminal rings of fraudsters who together operate many different fake profiles. They assume the personas of both men and women of all sexual orientations. Frequently, the persona's stated location is far from the victim to avoid meeting in person. Scammers often describe circumstances that tug at heartstrings — such as a struggling single parent or a lonely military member deployed overseas — to lure victims and then solicit money, often to help with a fabricated problem or to ostensibly pay for travel to visit the victim.

Romance Scam Case Study: A "Marine" in Maryland

In May 2021, a Maryland man pleaded guilty to fraud in connection with an online dating site romance scam. According to the US Department of Justice, the scammer used fake profiles and personas on dating sites to connect to several women, claiming he was a widowed US marine with a young son. According to the DOJ, he declared to each woman that he wanted to get married, buy a house, and raise children together. Shortly afterward, the complaint said he would ask victims to send him money for a variety of fake pressing financial situations such as car, legal, or health problems. The women were instructed to do so through interstate wire transfers and bulk cash shipments, making the payments difficult to track or recompense. The Justice Department said he was able to obtain at least $276,361 from at least eight female victims across three different states.

Romance Scam Red Flags

- The person asks for gifts or money, claiming a family emergency, medical expenses, travel expenses, etc.

- The person asks that the money be sent by wire, gift cards, or cryptocurrency.
- A reverse image search suggests that the photos used in a profile belong to someone else.
- The person has no other internet presence, or their personal details reveal other, disparate profiles.
- They agree to meet in person but always break plans, usually at the last minute.
- Conversations seem stilted and generic, as if used from a template.

6.7 Pet Adoption and Rehoming Scams

Pet adoption soared during the COVID-19 pandemic, and as a result pet rehoming and adoption scams have flourished, luring users with promises of cheap fees on popular or designer animal breeds such as Yorkies, Golden Retrievers, Poodle mixes, and Huskies. In this niche version of a nondelivery scheme, scammers often post ads on social media or classified platforms meant to redirect consumers to their fraudulent websites. Oftentimes, the pictures of animals used by these scams have been stolen from other websites or social media and used to advertise animals they don't possess.

Victims typically place a deposit on an animal, but then find out that the seller has disappeared with their money or, worse, that the seller is demanding additional compensation for shipping costs, veterinary supplies, or other fabricated problems. Because of the emotional attachment a pet can create, scammers can often continue to milk the buyer over time. Consumers may find themselves out hundreds or even thousands of dollars before they realize they've been tricked.

Pet Adoption Scam Case Study: petscityzone.com

The website petscityzone.com, which is offline as of the publishing of this handbook but previously offered online adoption for various dog breeds, was reported in early 2021 as a possible scam on both the International Pet and Animal Transportation Association's (IPATA) warning list and on petscams.com. Although unconfirmed by LegitScript, the website had the hallmarks of a scam: it gave little information about their available puppies, provided only a WhatsApp contact number, and required payment for the animals to be in the form of Zelle, Cash App, Walmart MoneyCard, or Western Union.

A search of the website's phone number revealed several other now-offline pet adoption websites for different breeds using the same contact information: craffenheimpuppies. com, wonderland-goldenretriever.com, and royalchowchowpups.com.

A reverse image search of some of the pet photos revealed one of a Golden Retriever puppy that had been posted to the social media site Reddit several years earlier by someone who purported to be the puppy's owner. Several other puppy photos also appeared to have been originally posted on the internet two to three years before the domain name was ever registered. Additionally, the testimonials from customers listed on the related websites shared nearly identical language, some with identical spelling errors.

Pet Adoption Red Flags

- There is limited information offered about the animals for sale.
- The website markets popular breeds available immediately even though they typically require a waitlist.
- There are suspicious photos, descriptions, or contact information.

- The seller uses forms of payment that offer little recourse for refunds (e.g., money wire, cash apps, gift cards, etc.)
- Animals are deeply discounted and available immediately for purchase.
- The domain name has been recently registered, and/or DNS data connects it to other defunct domain names that appear to have been related to pet adoption.

CHAPTER 7

Transaction Laundering

Transaction laundering offers a backdoor into the regulated financial system for cybercriminals who want to offer credit card payments to their customers. Even as payment processors implement best practices to identify and stop transaction laundering, illicit merchants find new ways to operate and adapt over time. In this chapter, we look at common typologies and associated risk factors, evolving transaction laundering methodologies, and key principles you can implement to interrupt and prevent transaction laundering and its associated crimes.

7.1 Defining Transaction Laundering

At a high level, transaction laundering is a way to game the payments compliance system. The illicit merchant obtains a merchant account for a seemingly innocuous business, then uses it to process risky transactions for the true underlying operation.

In many ways, this is analogous to more traditional forms of money laundering, where a front company posing as a genuine business isn't really selling anything, and the payments it takes are actually for something else. A transaction laundering website, commonly referred to as a bank page, is the online equivalent of a storefront that — despite never being open, offering strange products that nobody would ever buy, and appearing to have no customers — somehow manages to stay in business.

The increased volume and speed of e-commerce has given rise to frictionless onboarding, which enables people to obtain merchant accounts quicker, with less information required up front about the merchant and their business. This is good news for people who are looking for a quick and painless way to get set up with selling online, but it can increase the risk of abuse. Transaction laundering can be challenging to detect even with a more thorough underwriting process, but expedited and frictionless onboarding makes it much easier for illicit actors to exploit the payments ecosystem.

7.2 Why Cybercriminals Use Transaction Laundering

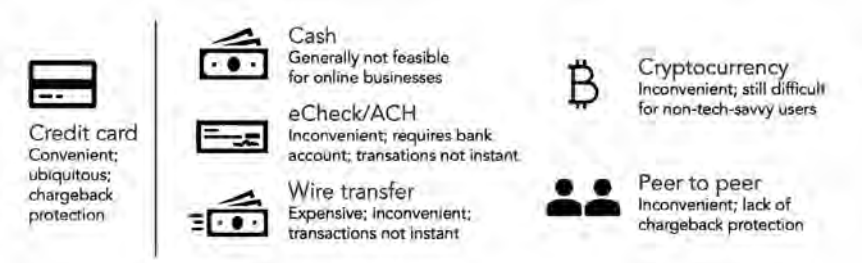
More than ever, people are buying online. E-commerce accounts for an increasing share of total retail sales, growing from 4.2% in 2010 to more than 13% in 2021, and the trend is likely to continue. The internet makes it easy to perpetuate financial crime because it affords anonymity, access to services on the operator's end, and a much larger pool of customers.

At LegitScript, we often say that illicit sellers are rational economic actors. What we mean is that merchants engaged in illicit activity, just like legitimate merchants, are striving to succeed in business. They are making the best possible decisions to ensure their businesses thrive — including a well-built e-commerce website with an easy payment flow. For that reason, problematic merchants want to accept credit card payments.

There are many ways to process payments online, but credit cards are, in most cases, the gold standard. Lacking credit card processing, illicit merchants are forced to offer other payment options that are far less desirable for both them and the average customer.

Alternative forms of payment such as eChecks, ACH, or wire transfer are often quite costly to the seller and can take several days

to complete the transaction. Customers are increasingly savvy on using cryptocurrency or peer-to-peer payment methods, but what these options offer in increased anonymity and instant processing, they lack in refund and chargeback protections. And, of course, paying cash for an online purchase is virtually unheard of these days.



7.3 Transaction Laundering Methodologies

Not all transaction laundering looks the same. There are many ways to launder a transaction, and cybercriminals have become increasingly sophisticated in their methods. Let's look at some of the most common ways illicit merchant launder transactions.

The Standard Transaction Laundering Account

More entrepreneurial illicit merchants may decide to take transaction laundering into their own hands by setting up "bank pages" marketing innocuous goods, but the merchant account information includes their real name or business information. This is the type of transaction laundering most of us think about.

The "Stealth" Transaction Laundering Account

Increasingly, cybercriminals are offering transaction laundering as a service, where an illicit merchant pays to use the payment processing capabilities of a transaction launderer. These types of transaction laundering accounts are sometimes referred to as "stealth accounts," as it's an easy way to launder under the radar.

These transaction launderers typically employ synthetic identity fraud — that is, accounts are created with stolen information. It's "synthetic" because the personal identifiable information (PII) is a mix of random but often authentic information such as birthdays, social security numbers, employer identification numbers, and more. Although real, the information doesn't necessarily align with any one real person, and it likely comes from data dumps from a variety of breaches. People make these synthetic accounts in bulk and sell them on forums and purpose-built platforms. Read more about this in Chapter 6.

Semi-willing Identity Theft

LegitScript has seen many instances in which members of the public are recruited online as part of Independent Business Owner (IBO) schemes. People lend their identities in the creation of LLCs, which bad actors then use to obtain accounts for processing. IBOs are marketed as "passive income" in the form of commissions on sales from these merchants, but unwitting members of the public typically do not have visibility or understanding into what the accounts are actually being used for. We see IBOs targeting vulnerable populations of US citizens such as the elderly and other fixed- or low-income individuals.

Potentially Complicit Payment Processor

In this scenario, a payment processor may knowingly process payments on behalf of fraud merchants. The processor may not necessarily know the exact nature of the problematic activity but is either permissive or willing to overlook suspicious activity. This type of transaction laundering is rare.

Regardless of the method, illicit merchants processing payments using transaction laundering are resilient and typically have techniques to adapt when caught. The most common responses include:

1. Creating more transaction laundering websites. Recent domain name creation dates may be a clue for merchants who are operating on the fly.
2. Setting up an arsenal of transaction laundering accounts for load balancing, and to protect against the possibility of accounts being closed.
3. Taking other payment methods such as peer-to-peer and cryptocurrencies as a stopgap until the merchant regains credit-card processing.

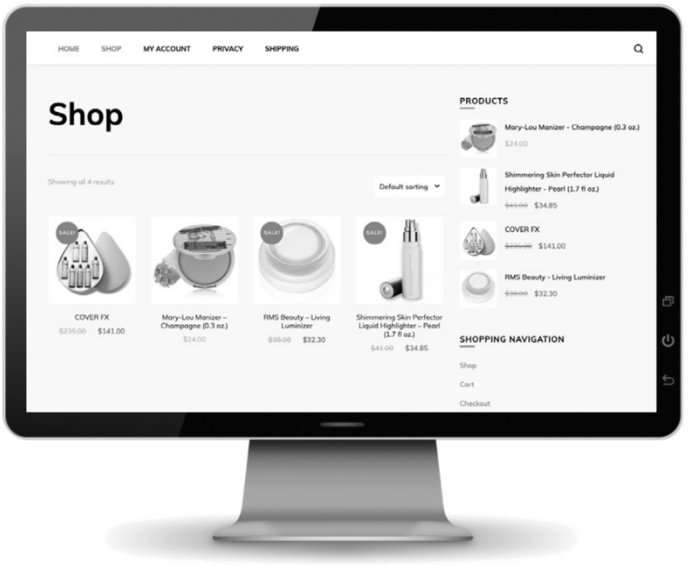
7.4 Transaction Laundering Typologies

Transaction laundering is a technique employed by a variety of cybercriminals, from merchants selling illicit drugs to ones offering illegal gambling. It's helpful to understand that each type of illicit merchant tends to act in a particular way and employ common techniques that may help you to more quickly identify them. For example, cybercriminals selling IP-infringing streaming entertainment often set up merchant websites for vague computer services, such as web hosting or technical support.

Let's look at some of the most common typologies of transaction launderers and how each type tends to operate.

Rogue Internet Pharmacies

Rogue internet pharmacies are ones that offer pharmaceuticals illegally — that is, selling drugs without a valid prescription requirement, selling in a jurisdiction where they are unlicensed, and/or selling unapproved drugs. The following screenshot shows a cosmetics website that was transaction laundering for a merchant offering controlled substances and opioids via email solicitations. For more about this merchant, see the case study in section 1.6.



Tips

- Common typologies include health- and wellness-related websites selling supplements or cosmetics, enabling the merchant to have a plausibly related merchant descriptor.
- Conducting research on the domain name system information (DNS), such as Whois information and IP address, may reveal affiliated websites.

Illicit Gambling

A common type of laundering seen with gambling merchants is the use of intermediary payment forms, or payment aggregation methods, to obscure illicit transactions. Merchants are blocked from accepting credit cards for gambling in some jurisdictions, so they will direct users to pay for an e-voucher, or will route them through a cryptocurrency exchange that takes payments via credit card. As shown in the following screenshot, risky stored value or aggregation services are often used.

It's not unusual for us to see a highly integrated payment processing flow. For example, upon attempting a deposit on a gambling website with a card, we are redirected to a crypto exchange for the same amount, and then routed back to the gambling website when the exchange is complete. Although it's possible that some of these exchanges are genuine cryptocurrency marketplaces, most that we encounter with gambling website integration appear purpose-driven for laundering.

Tips

- Common typologies include risky stored value products such as e-vouchers or aggregation services.
- Laundering can occur through credit cards used on a cryptocurrency wallet integrated with a gambling website.
- Online gambling is also used for money laundering.

IP-infringing IPTV

Illicit IPTV is persistently one of the most common services to make use of transaction laundering. According to the International Trademark Association, the total estimated value of counterfeit and pirated goods, including digital piracy, is nearing $3 trillion, with illicit streaming entertainment responsible for an increasing share. See Chapter 8 for more on IPTV. Merchants offering IP-infringing IPTV often use web hosting or VPS services as a laundering guise for IPTV resellers, as shown in the following screenshot.

Rights holders are also fighting back against piracy, and payment processors may be left on the hook for sizable fines associated with helping to facilitate these sales. Both Visa and Mastercard prohibit illegal transactions involving copyright infringement, and work diligently with rights holders to investigate allegations of infringing behavior. Regulatory agencies may also hold internet companies

accountable if they show gross negligence in allowing these merchants to market or conduct business on their platforms.

Tips

- Common typologies include subscription-based fronts such as web hosting for IPTV processing.
- Web hosting is particularly common for this type of transaction laundering.
- Automatic redirects may occur at checkout.

Negative-option Billing

A potentially deceptive approach to selling, negative-option billing can ensnare consumers in ongoing subscriptions without their express consent. See Chapter 3 for more on this business model. The Federal Trade Commission has highlighted the practice as a major focus of enforcement, and Mastercard updated its standards regarding the registration of negative-option merchants. These merchants operate a bit differently in that they often create multiple innocuous-seeming storefronts so that they can engage in load balancing. The following screenshots show websites offering everything from handbags to pets, but all of them were processing payments for a website marketing high-risk sexual health products.

Tips

- Common typologies include a variety of websites that look innocuous but with offerings that may seem strange under closer scrutiny.
- Merchants engaged in deceptive recurring billing schemes also pose a high risk for chargebacks.
- To prevent detection, merchants will create many storefronts to rotate their payments through to engage in load balancing.

Transaction Laundering for Fraud and Scams

Increasingly, LegitScript sees merchants engaged in various forms of fraud making use of transaction laundering. These include brand impersonation fraud, tech support scams, and nondelivery schemes, which occur when a consumer purchases a product that is never delivered (and which the merchant typically never has possession of in the first place). These scams can be difficult to spot because there is often lag time between when consumers make a purchase and when they realize they've been scammed. These merchants also frequently rotate through many shell accounts, making them hard to pin down. Transaction laundering for fraud is increasingly attractive because it helps distance the payment processing from the violative website, making it harder to connect the two and more likely that the merchant account remains active longer.

Detection Strategies

- Customer complaints and, increasingly, law enforcement action can offer useful details during the analysis of potential transaction laundering merchants and websites.
- Undercover calls or other undercover contact with the merchant can help test theories and confirm transaction laundering.

- Data collected from transactions, phone calls, social media, and news articles can help build out networks of fraud websites using a combination of Whois information, website content, and unique source code identifiers.

7.5 Transaction Laundering Red Flags

Although transaction launderers are pernicious because of their ability to evade detection, certain types of business models inherently pose elevated risk for transaction laundering because they are so easy to abuse. They include:

- Drop-shipping
    - Especially consumer goods such as clothing, electronics, and knickknacks
- Generic technical services such as web design, hosting, or SEO
- Generic professional services such as graphic design
- Lower-risk healthcare products such as supplements and cosmetics

For these types of businesses, a face-value analysis can offer important clues about whether a website warrants additional scrutiny. There are ways to differentiate incomplete websites from potential bank pages. Some of these include:

- Use of a generic template-based website with little modification
- Website copy and design that is not consumer-friendly, lacking expected dynamic features
- Lack of a greater web presence, such as social media profiles and consumer reviews

- Website configurations that prevent web crawlers from indexing the page

If a face-value analysis raises red flags, a network-mapping analysis can help reveal if the website is connected to anything else of note. This can be done with open-source information alone, such as searching for contact information published on the website that shows up elsewhere.

Other points of inquiry can include website infrastructure and technical data analysis, as it's not uncommon for merchants to reuse the same services for their transaction laundering websites as well as those offering violative products. Merchant application details can also prove valuable since many merchants are unaware that investigators may have visibility into this data, and so they may leave obvious clues. So, remember to research:

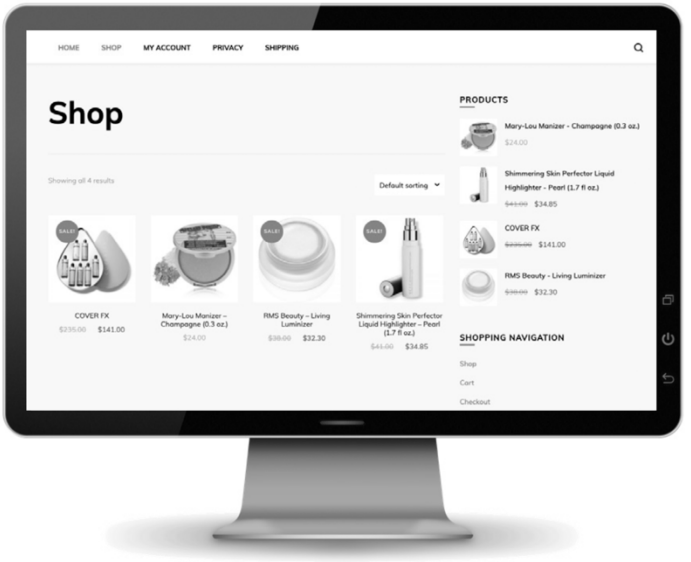
- Published contact information on the merchant's website
- Merchant application details
- Technical data such as Whois, web hosting, and DNS for connections to other websites
    - This might reveal connections directly to the underlying violative website, or, alternatively, to a ring of transaction laundering websites.

7.6 Transaction Laundering Case Study: Drugs Via Email

Large transaction laundering schemes can be uncovered through a single bad actor. This case study provides an example of how a transaction laundering investigation can begin with a single website or merchant account, and grow to include a full network of illicit activity.

LegitScript received an email solicitation to an undercover account from a merchant offering prescription opioids, such as tramadol, for sale to consumers in the US. The rogue pharmacy operation provided a URL in the body of the email that was inaccessible through the root domain, but allowed customers with a link to a specific web page to place orders.

A test transaction returned a merchant descriptor corresponding to a generic cosmetics website. This website bore hallmarks of transaction laundering, such as a bare-bones product listing and incongruous product pricing. That is to say, the face-value analysis raised red flags.



Next, we performed a network-mapping analysis. Details and published contact information on the website were generally unattributable. Whois registration information provided an additional avenue for investigation. More than 20 additional domain names pointing to websites with hallmarks of transaction laundering were registered using these contacts.

Several websites stood out as outliers, including one offering high-risk merchant processing, and another offering an "investment opportunity" wherein individuals could provide their identity and credit to "partner in" a merchant account for unknown businesses. (This was the IBO scam mentioned in section 1.3.)

One domain name actually bore the business name listed in the Whois; the other website offered access to high-risk merchant accounts — suggesting that this was an integrated operation that sought IBOs for merchant accounts, set up fake bank pages, and then offered the accounts to merchants looking to process cards for all manner of things (including, to our knowledge, illicit pharmaceutical sales).

While websites in this network have been taken down, the operation itself was still active as of the publishing of this book. LegitScript continues to track this network of transaction laundering websites and illicit businesses to help our clients steer clear of this activity.

CHAPTER 8

Other High-risk Areas

In addition to the topics covered in the previous chapters, LegitScript tracks dozens of other highly regulated industries and categories. The following sections touch upon topics that are seeing new developments, experiencing increasing consumer interest, or facing noteworthy regulatory or card brand scrutiny.

8.1 Cryptocurrency and NFT Fraud

A 2022 study by Finder.com found that about 27 million Americans own cryptocurrency, 44.5% of which own Bitcoin. Although this is less than 10% of the total US population, cryptocurrency adoption has been on a steady incline since the inception of Bitcoin in 2009.

Sellers offering or promoting cryptocurrency or other virtual credits offer a type of unregulated, intangible money or good, whose value is issued and controlled by its developers, and whose use is accepted among the members of a specific virtual community. In particular, virtual credits lack legal tender status in any jurisdiction and official connection to the real economy.

Processing payments for cryptocurrencies can carry substantial risk due to the speculative and highly volatile nature of cryptocurrency markets. Furthermore, it can be difficult for payment service providers to trace what a customer is purchasing. Since this is the case, virtual credits are easy mechanisms for money laundering.

Criminals have been known to purchase virtual items using their real money, then send these virtual goods to associates in their virtual form, which the associates then convert back into real money.

Crypto Scams

The movement toward mainstream cryptocurrency acceptance has drawn problematic actors looking to exploit the public. In recent years, billions of dollars have been lost in crypto-related scams and theft, including the hack of Bitfinex, a virtual currency exchange, which led to the theft of an estimated $4.5 billion.

Cryptocurrency-related scams are often promoted via social media accounts, and are reaching ever wider across more diverse audiences. These scams often involve fake cryptocurrencies, fake wallets, online phishing scams, or a "rug pull," which is a malicious act in which crypto developers abandon a project and take off with the project funds, similar to "pump-and-dump" schemes.

Crypto Scam Case Study: Squid Coin

Squid Coin was ostensibly a digital token inspired by the popular South Korean Netflix series Squid Game. At the end of October 2021, Squid Coin skyrocketed in value as investors who had been lured by flashy promotions on social media platforms purchased Squid Coin. Between October 26, 2021, and October 29, 2021, the listed value of a Squid Coin rose from a little more than one cent to more than $2,800. Soon after, however, the currency collapsed to zero after a rug pull by the coin's creators, who appear to have abandoned the project and made off with investor funds worth $3.3 million.

Cryptocurrency observers and media outlets warned investors about Squid Coin after numerous red flags surfaced: its social media accounts did not allow followers or subscribers to comment; its developers published a sloppy whitepaper with obvious spelling and grammatical errors; and investors were prevented from reselling their

tokens. CoinMarketCap, a data provider, urged potential traders to take "extreme caution" after Squid Coin buyers told the platform that their coins could not be sold.

Non-fungible Tokens

Non-fungible tokens (NFTs) are virtual assets that exist on the blockchain and can be purchased with fiat currency. These unique digital assets — which are usually photos, videos, or audio — can be sold and traded. When a customer purchases an NFT, they are purchasing what can be thought of as certificate of ownership or authenticity.

NFT sales volume totaled $24.9 billion in 2021, compared to just $94.9 million the year before, according to DappRadar, which collects data across blockchains. NFTs made headlines in 2021 when a single NFT by the artist Beeple sold for $69 million.

The idea that NFTs can quickly increase in value have made them easy conduits for fraud. Common scams include phony NFT artwork, fake platforms utilized to steal credit-card information from unknowing consumers, and hackers exploiting security gaps in rapidly growing marketplaces. For example, one victim reportedly lost $480,000 after sharing his screen with scammers posing as customer service representatives of a popular NFT marketplace.

Like all forms of artwork and other items of value, NFTs can be used for money laundering, though there have been no proven cases of this happening to date. However, one of the main differences between NFTs and other expensive items such as property or original artwork is that purchasers of these digital assets can more easily remain anonymous.

Furthermore, NFTs may have significant copyright-related implications, especially as well-known brands are getting involved. Fashion brands are emerging as players in the NFT world. Nike, for

example, patented a system enabling customers to receive a virtual version of custom shoes they buy.

This creates an enhanced risk of intellectual property infringement. There is a possibility that infringers may create tokens for an image they do not own.

NFT Case Study: NeoPets

An efficient way to sell NFTs is to make thousands of unique items at a time, often by subtly changing their color or pattern. When the virtual pet website Neopets launched a line of NFTs, some of the digital assets used patterns that were allegedly exclusive art from creators on the unaffiliated Neopets fan site "Dress to Impress." No legal action has been filed against Neopets as of the publishing of this handbook, and it's unclear what rights these creators may have when it comes to NFTs. Because there has been no clear legal precedent to clamp down on NFT counterfeiters or those that infringe upon original artwork or a brand's intellectual property, this is an area in which the legal framework is still developing.

8.2 IP Infringement

According to the International Trademark Association, the total estimated value of counterfeit and pirated goods, including digital piracy, has reached nearly $3 trillion annually. Many social media and e-commerce platforms have been cited as hotbeds of intellectual property (IP) infringement because of the internet's worldwide reach, the increasing ease of online payments, and the relative anonymity that e-commerce affords bad actors.

IP infringement can put consumer safety at risk and facilitate more serious forms of wrongdoing, which is why it is a threat and liability to e-commerce marketplaces, social media platforms, and payment service providers facilitating online sales.

Types of IP Infringement

IP infringement is the infringement or violation of an intellectual property right. There are several types of IP rights, including copyrights, patents, and trademarks. Infringement can take many forms, but the most common ones appearing online include:

- **Unauthorized goods or services:** a merchant that is offering the unauthorized sale or resale of brand name or designer products or services; a merchant that is offering the sale of goods or services that are illegally imported or exported without the rights holder's permission; or a merchant that is offering unauthorized licensed materials, most frequently music, movies, TV shows, or software. In this scenario, the asset may be genuine but has been illicitly obtained, reproduced, and/or distributed.
- **Counterfeit goods:** a merchant that is offering a product that copies a genuine one and uses branded designs or logos, regardless of whether the product purports to be a replica or the genuine item.

Common unauthorized and counterfeit goods include luxury items such as jewelry and accessories; apparel such as shoes and clothing; and electronics such as mobile phones, smart watches, and other gadgets. However, unauthorized and counterfeit goods can apply to any branded product.

Merchants often do not state whether they are authorized to offer the intellectual property they are selling, making it difficult to discern whether the offered goods/services are legitimate or infringing. Additionally, a merchant may make false claims of authorization.

As such, it is an industry best practice for e-commerce marketplaces and payment service providers to request evidence of

permissive use from merchants that do not clearly own the rights to the intellectual property they sell.

Dangers of IP Infringement

IP-infringing websites may appear legitimate at first glance, which can make them difficult for internet companies and payment service providers to spot. Take, for example, the following image marketing luxury accessories. Counterfeit merchants like these pose not only a danger of fines from credit card companies, but the threat of litigation from the brands that are the victims of counterfeiting.

Furthermore, counterfeits can risk consumer health because they often are made without regard to health and safety standards. For example, British police warned of the dangers posed by counterfeit electrical devices that can cause fires or electrical shocks. Items such as counterfeit mobile phone chargers, which may undergo no safety checks, have been the cause of house fires and burn injuries.

In another example, Chinese investigators broke up an organized crime gang said to have made as much as $7 million by selling repackaged, used condoms to hotels, vending machine operators, and supermarkets.

Consumers have been harmed by counterfeit cosmetics found to contain hazardous substances including cyanide, arsenic, mercury, and lead.

Red Flags of Counterfeit and Unauthorized Goods

- Domain names that are similar to a brand's genuine flagship domain name
- Websites with obvious misspellings or other blatant language errors
- Websites offering popularly counterfeited brands such as Nike, Gucci, Disney, Star Wars, Adobe, and Microsoft
- Items described as replicas, imitations, or "our version" of a product if the item uses the original brand's design and/or logo
- Products made in the "same factory" as high-end brands.

Internet Protocol Television

Perhaps the most common form of IP infringement LegitScript encounters is internet protocol television (IPTV), a service that enables consumers to access TV via the internet. These services, both legitimate and illicit, have risen in popularity in recent years as more consumers gain access to high-speed internet and desire cheaper, à-la-carte alternatives to traditional cable TV. Typically, IPTV providers offer subscription access to streaming content, or provide devices pre-loaded with applications intended for the same use.

The relatively quick adoption of IPTV has made it a prime target for criminals. Piracy has risen in conjunction with the popularity of IPTV services, often at great cost to rights holders.

A recent Notorious Markets List, published by the United States Trade Representative, estimated that unlicensed video providers, hosting services, and device sellers stood to bring in $840 million a year in revenue from the sale of their products. According to the report, the cost to the entertainment industry is estimated to be between $4 billion and $5 billion.

While IPTV providers argue that they are not violating the law because they only provide access to streaming content, and are not offering downloads or hosting any content themselves, courts disagree. The European Court of Justice ruled that fully loaded IPTV devices are illegal, and sellers of these devices have found themselves on the receiving end of large fines.

Rights holders are also fighting back against piracy, and marketplaces and payment service providers may be left on the hook for sizable fines associated with helping to facilitate these sales. Both Visa and Mastercard prohibit illegal transactions involving copyright infringement, and work diligently with rights holders to investigate allegations of infringing behavior. Regulatory agencies may also hold internet companies accountable if they show gross negligence in allowing these merchants to market or conduct business on their platforms.

Red Flags of IPTV

- Merchants offering an extraordinarily large number of channels for a suspiciously low monthly fee
- Merchants providing access to premium channels, such as HBO, as part of their flat fee structure

- Services that include pay-per-view content as part of their subscription package
- Services that allow customers access to a broad range of international channels
- Language stating that consumers can use the product or service to eliminate their cable bill

8.3 Vaping and ENDS

Vaping has been in the spotlight because of reported health risks associated with its use and because of what the Food and Drug Administration has called an epidemic of youth e-cigarette use. This scrutiny highlights the elevated risk e-cigarette products pose for legal violations. Although many internet platforms and payment service providers prohibit online e-cigarette merchants because of reputational risk and the risk of selling to underage consumers, online merchants may attempt to obfuscate their business models to circumvent a company's terms and conditions.

Vaping Defined

Vaping has become ubiquitous in recent years, particularly among teens and young adults. A user who vapes inhales vapor through the mouth, typically from a battery-operated electronic device (such as an electronic cigarette) that heats up and vaporizes a liquid or solid. This is different than smoking, wherein a user inhales the smoke of a combusting substance, such dried tobacco leaf.

Vaping devices can be used to inhale nicotine, THC (the psychoactive ingredient in cannabis), cannabidiol (CBD), and even non-traditional substances such as essential oils. The substance vaped is typically called vape oil, vape juice, e-liquid, or e-juice.

Vape oil comes in hundreds if not thousands of flavors, some of which have drawn regulatory scrutiny from the FDA for appearing

to target younger populations. Flavors cited include ones mimicking the taste of Kool-Aid, SweeTarts, Hawaiian Punch, gummi bears, Froot Loops, Skittles, and more.

E-cigarettes

Defining e-cigarettes can be surprisingly complicated. The FDA considers e-cigarettes, e-liquids, and related accessories to be components of an electronic nicotine delivery system (ENDS). For simplicity's sake, we refer to these, collectively, as e-cigarettes. They are subject to increased regulatory scrutiny by the FDA and are subject to review by authorities.

The final rule issued by the FDA in 2016 deemed products meeting the statutory definition of "tobacco product," except accessories of the newly deemed tobacco products, to be subject to the Federal Food, Drug, and Cosmetic Act. This includes e-cigarettes and their components and parts.

Electronic Nicotine Delivery Systems

These systems are often sophisticated pieces of technology that comprise many parts. The FDA lists the following example components:

- E-liquids
- Cartridges
- Atomizers
- Certain batteries
- Cartomizers and clearomizers
- Tank systems
- A glass or plastic vial container of e-liquid
- Digital display or lights to adjust settings
- Drip tips

- Flavorings for ENDS
- Programmable software

Any component intended for use as part of such a system counts as part of it, even if it is sold separately.

In many respects, these products are currently regulated like tobacco products. These parts, especially if sold separately, can be difficult for internet platforms and payment service providers to identify on an online seller's website, account page, or social media post. Furthermore, e-cigarettes come in many shapes and sizes, which can make them difficult to spot; some of them have been confused for pens or external flash drives.

Other Vaping Substances

THC, the psychoactive ingredient in cannabis, is still controlled at the federal level in all forms, making vape liquid that contains THC a high-risk product. (See Chapter 2 for more.)

While the FDA has yet to promulgate rules specifically addressing CBD in e-cigarettes or vape products, they have released warnings regarding the potential safety hazards of vaping unapproved and untested products. As there is no way for the average consumer to know what additional ingredients are contained in a particular vape product, the FDA has warned these products may trigger laryngospasm and bronchospasm and may be toxic to the tissues in the upper or lower airways. However, the FDA has not yet taken enforcement action against CBD vape products without problematic claims. Internet platforms and payment service providers should pay special attention to e-cigarettes or vape products that are marketed with claims to treat or cure diseases — as CBD vape juices often are — as that is where the FDA has focused its enforcement action for these products."

More recently, some merchants that used to sell tobacco-derived nicotine have recently switched to synthetic NTN ("non-tobacco nicotine") to avoid FDA regulation. Makers of synthetic nicotine products usually state that their nicotine is developed in a lab and is not derived from tobacco leaf. New legislation enacted in March 2022 makes it clear that the FDA has regulatory control over products containing nicotine derived from any source, including synthetics. According to the FDA, "manufacturers of NTN products who wish to market their products are required to submit a premarket application and obtain FDA authorization to market their product, or they will be subject to FDA enforcement."

A 2022 paper from Stanford University identified six manufacturers of synthetic nicotine and 98 brands claiming to contain synthetic nicotine. According to Truth Initiative, a nonprofit dedicated to ending the use of tobacco and nicotine, the disposable e-cigarette Puff Bar and oral nicotine products Bidi Pouches, NIIN, and Rush have all been marketing synthetic nicotine products that have not been through the required regulatory review and approval processes. These products come in flavors often used to attract youth.

8.4 Adult Content

With the rising popularity of user-uploaded content, the landscape of online adult content has become more complex, which can make it difficult for internet platforms and payment service providers to navigate. Adult content distributed online will generally fall into two categories: first, studio-produced content, which is typically controlled, solicited, and/or produced by an adult content provider; and second, user-uploaded content, in which users typically share directly through a mechanism offered by an online platform.

Although both content areas may pose significant risk, user-uploaded content likely poses a greater level of inherent risk because

compliance with applicable laws and regulations is dependent on the platform's ability to monitor and self-regulate content, including performer age and consent verification, through content moderation. Adult live-streamed content also falls under the umbrella of user-uploaded content, and may pose an even greater level of inherent risk because the content is streaming in real time and cannot be subject to the same level of vetting as an uploaded image or video.

In late 2021, in an effort to prevent child sexual abuse material (CSAM) and other non-consensual content, Mastercard imposed revised rules for adult content websites that use of its credit card or payment options. These rules include requirements such as pre-approving all content before publication, forbidding certain search terms, and keeping records of age and identity verification for all performers.

FOSTA/SESTA

Another challenge is the appearance of adult content on social media and other platforms where this type of content is unintended and often prohibited. The manner in which social media platforms (the majority of which are based in the United States) regulate and police adult content is informed by US legislation that was passed in April 2018. Officially known as the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, it is popularly referred to as the FOSTA/SESTA package. The nominal overall purpose of the law is to curb illegal sex trafficking online by "holding websites liable for user-generated content that facilitates sex trafficking [...] and to make intentionally hosting such material a federal crime," which significantly weakens the immunity granted to online platforms under Section 230 of the Communications Decency Act.

In response to FOSTA/SESTA's passage, social media underwent significant shifts in its approach to regulating adult content. Among the more notable examples, classifieds website Craigslist

shut down its personals section entirely two days after the law came into effect. Tumblr, once home to a thriving not-safe-for-work community especially valued by LGBTQIA+ and other marginalized people, soon after issued a blanket ban on all adult content, including illustrations depicting sex acts. However, other platforms have taken a far more lenient approach to moderating and removing adult content. Some platforms and forums make use of extremely lenient registrars and internet service providers, which have made them havens for largely unrestricted adult content. 4chan is an example of such a forum.

Adult Content Best Practices

Internet platforms, payment processors, and sellers engaged in the distribution of adult content online can follow certain best practices that may reduce the risk of noncompliance:

- Ownership or control of the entire process of content creation, publishing, and distribution is the surest way to reduce the risk of distributing illegal or violative content.
- Following all required procedures of 18 USC § 2257, regardless of the jurisdiction in which content is produced, will help mitigate the risk of underage performers. Given the prevalence of online adult content in the United States and Section 2257's applicability to content in the United States regardless of the country of origin, strict adherence to Section 2257's requirements will help ensure compliance.
    - Properly affix a statement on all pages hosting adult content that describes where the records required by Section 2257 may be located.
- Display template age verification and consent agreements on the websites with a self-certification that all performers on the site have executed these agreements.

- Refuse to accept any user-uploaded content. Absent complete control over the content creation process, platforms that accept user-uploaded content, even content from so-called "verified users," subject themselves to enhanced risk of distributing impermissible content.
- Perform frequent, independent audits of all verification and compliance records.

8.5 Illicit Massage

In 2018, the federal government seized backpage.com, a website critics say was notorious for enabling prostitution and human trafficking through the classified adult ad space. Because of this closure, individuals who advertised their services on the website were forced to find other ways to market their businesses online.

One resulting trend has been an influx of illicit massage merchants, who pose as massage professionals but are actually using their businesses as a front to provide sexual services.

Illicit Massage Defined

LegitScript has seen an increase in illicit massage merchants in our clients' platforms since the seizure of backpage.com. Illicit massage refers to any merchant who is offering sexual massage services. These services typically violate a company's terms and conditions, and in many cases also violate local laws.

Overtly illicit massage websites are typically easy to spot because they include suggestive photos of the massage providers or describe explicit services, such as "happy endings." However, many merchants attempt to pose as legitimate massage businesses, making them difficult to detect. This guise allows them to widely market their business while offering sexual services.

The Impact of Illicit Massage

In addition to potential violations of terms and conditions as well as local laws, the trend in illicit massage businesses presents risks for not only prostitution but also human trafficking.

Polaris, a nonprofit, non-governmental organization, released a report in 2018 titled "Human Trafficking in Illicit Massage Businesses." The report uncovered alarming rates of human trafficking related to illicit massage parlors. In 2017, 2,949 of the 32,000 human trafficking cases Polaris analyzed were connected to illicit massage parlors, which was, according the report, second in prevalence only to trafficking in escort services.

Red Flags of Illicit Massage Merchants

LegitScript's expert analysts look for a number of key indicators that present a heightened risk for illicit massage merchants. Common risk indicators include but are not limited to:

- Massage merchants who stay open late or even boast 24-hour service
- Physical descriptions of staff, such as merchants who refer to the masseuses as young, attractive, or of a particular ethnicity
- Representation on third-party websites that primarily exist as online communities for sexual-massage seekers

Since illicit massage merchants who are more adept at obfuscating their true business may not display these obvious red flags, LegitScript also uses merchant phone numbers, email addresses, and other data points to perform a thorough risk assessment.

8.6 Hate/Harm

Extreme political discourse often plays out in the online space, with violent and hate-filled speech becoming increasingly prominent

and tolerated on social media. Extremist merchandise available for sale through websites and on e-commerce platforms often helps to support extremist groups.

Although the First Amendment of the US Constitution offers broad protections for speech, card brands, payment service providers, and internet platforms frequently reject "hate/harm" content in their terms and conditions.

Hate/Harm Defined

Hate/harm content encompasses merchants or users whose primary purpose is to advocate for, or to promote products or services that advocate for, hatred, hostility, or violence toward members of a race, ethnicity, nation, religion, gender, gender identity, sexual orientation, or any other designated sector of society.

The FBI compiles data on hate crimes in the US, and the Southern Poverty Law Center (SPLC) tracks hate groups. These can be useful reference tools for understanding both trends in hate/harm and being aware of specific groups to watch out for. Even so, many advocates of extremist views have no formal affiliation with a recognized hate group.

Legality of Hate/Harm Content

The First Amendment provides broad protections for the freedom of expression. As a result, much hate/harm content is not strictly illegal. Payment service providers and internet platforms, however, are free to enact their own policies based on company values and for brand protection purposes.

Even if extremist content does not violate laws, it poses an increasing risk of reputational damage. Some activist groups are increasingly diligent about seeking out this kind of content and publicly criticizing businesses that help to facilitate it, whether intentional

or not. Targeted companies can face financial losses from customer boycotts and/or devalued share prices.

Additionally, there has been an increase in crowdfunding on social media and fundraising platforms for extremist groups and their affiliates. Such merchants may violate payment facilitators' policies regarding aggregation, as well as present elevated risks for money laundering and transaction laundering. It is worth investigating fringe accounts and borderline blogs because they typically do not exist in isolation.

Policies Around Hate/Harm Content

Payment service providers, social media networks, and e-commerce platforms typically recognize the ambiguity surrounding hate/harm content and treat the issue with caution. To illustrate: a merchant offering assorted World War II collectibles containing pieces of Nazi memorabilia will not receive the same degree of scrutiny as a merchant making blatantly racist proclamations. While often difficult to pinpoint, a merchant's overall intent is the key distinction in such cases.

Payment service providers and some internet platforms typically prohibit merchants that are extremely inflammatory, affiliated with hate groups, or inciting violence. For example, the group Atomwaffen faced scrutiny for its connection to several murders, so any content affiliated with them would be highly problematic.

Red Flags of Hate/Harm Content

Hate speech often tries to fly under the radar. Many groups use coded language, memes, emojis, symbols, and insider references to promote their messages.

These "dog whistles" often make it difficult to uncover hate speech, but there are many common warning signs or red flags, such as:

- Runes and Viking iconography
- References to the "Jewish question" (frequently abbreviated as JQ)
- The number 14 (referring to the 14-word slogan, "We must secure the existence of our people and a future for white children")
- The number 88 (used among white supremacists as code for "Heil Hitler")
- Holocaust denial
- The term globalist (employed as a euphemism for Jews)

This is not meant to be an exhaustive list, but rather to illustrate the coded language and symbols common to many of these merchants. Themes of white persecution, a revival of white identity, and demonizing diversity are common motifs of these websites.

We note that racial supremacy is only one of many forms of hate/harm content, though it is one LegitScript commonly encounters in our monitoring and research. Other common themes of hate/harm content include gender bias, transphobia and homophobia, and hostility toward certain religions, typically Judaism and Islam.

8.7 Weapons

The sale of guns and other weapons typically surges in the midst of a crisis, and the pandemic has been no exception. According to National Public Radio, millions of Americans purchased guns in the first half of 2020, and about half of them were first-time gun owners. The FBI's National Instant Criminal Background Check System reports that background checks of handguns were up 80% in 2020. While in-store sales comprise the majority of gun purchases, first-time buyers who are used to shopping online may turn to the internet for their purchases. While many internet platforms decline advertising for firearms and many payment service providers refuse to process payments for them, it's important to watch out for sellers who offer a small selection of weapons embedded in a larger catalog of goods, or ones who sell gun kits made of parts that can be readily assembled into a functioning firearm, known as "ghost guns."

Ghost Guns

The notion of "ghost guns" — firearms that are assembled at home and untraceable with no associated serial number — has been around since at least the 1990s. Ghost gun kits originated as a way to circumvent gun laws in the US, as federal law regulates the manufacture and sale of firearms, but not firearm parts. These parts are available a la carte or as complete kits; in both cases, the final step usually involves using an included drill bit to create a hole in the receiver portion of the gun, which is the part the government regulates, to make it operational. Many of these merchants include

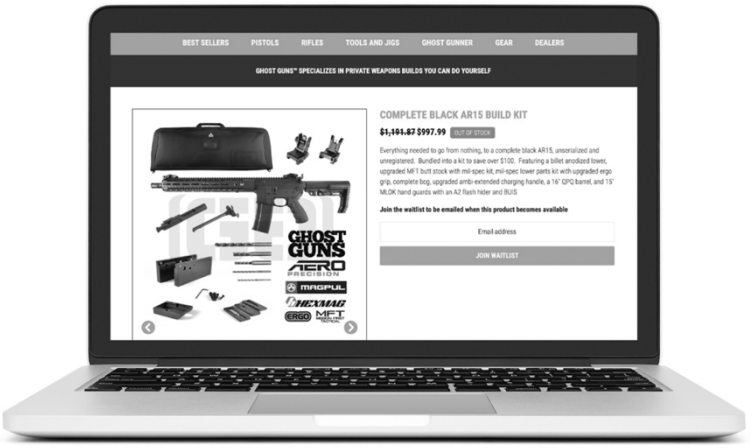
links to videos showing customers how to make their gun parts operational firearms.

Despite an increasing amount of legislation at the state level, the proliferation of both legal and illegal 80% lower receivers, continues to allow individuals to avoid background checks and registration. At the state level, New York, among other states, passed one of the most restrictive ghost gun laws in the US in 2022. Many of the newer state laws make it illegal to sell or transfer an unfinished receiver to anyone but a licensed gunsmith or dealer. Other states hoping to address the issue of 3D-printed firearms, such as Washington, have made it illegal to possess a firearm that is not detectable by a metal detector or magnetometer.

In April 2022, the White House announced the finalization of a rule that would require makers of gun kits to include serial numbers on the firearms and mandate sellers to follow the same standard as with other guns, such as requiring a background check for purchase.

Weapons Case Study

Some merchants selling gun kits may attempt to obfuscate their intended purpose as firearms by calling them replicas. Other merchants, such as the one featured below, brazenly market their ghost guns, including a build kit for an AR-15 assault rifle. For less than a thousand dollars, a customer can, according to the website, buy "everything needed to go from nothing, to a complete black AR15, unserialized and unregistered."



8.8 Online Gambling

Online casinos have reported record traffic in recent years as a result of people being homebound during the pandemic and more frequently working from home. According to Statista, the global online gambling market is expected to be about $93 billion USD in 2023, up from about $59 billion in 2019. This surge in online gambling may continue into future years as websites increase promotions and boost payouts to turn new visitors into permanent players.

Internet gambling in the US is regulated at both the federal and state level, and local jurisdictions that permit forms of it often have strict laws by which merchants must abide. To circumvent these laws, many illicit online gambling operations have set up an offshore model to stay out of the reach of regulators. Governments have been putting pressure on payment service providers to stop the flow of money and discourage offshore operations, which are often based in countries with looser laws or poor enforcement.

Underwriting gambling merchants requires a thorough review that typically includes:

- Requiring licensing requirements

- Legal opinion of the merchant's operations
- Check for controls
    - Age verification
    - Location verification
    - Measures reasonably designed to ensure legal compliance, including interstate transactions
- A website review
    - Statements regarding cardholder responsibility; that "internet gambling may be unlawful in the jurisdiction in which you are located; if so, you are not authorized to use your payment card to complete this transaction."
- Acquirer obligation not to submit unlawful or restricted transactions

Illicit Gambling Case Study

Wirecard AG, a German payment processor that filed for insolvency in June 2020, provided payment services to many high-risk industries, including adult websites and online gambling. According to the Financial Times, Wirecard processed payments for CenturionBet, a Malta-based gaming company used by organized crime for money laundering. A report in the British newspaper The Times also reported that Wirecard helped facilitate transaction laundering to mask payment processing for gambling in the US and other countries where it was illegal. As parts of Wirecard are sold off to other financial institutions, it's possible gambling merchants that once used Wirecard may be forced to look for new payment service providers.

Conclusion

Creating a handbook about online risk and compliance may seem like an impossible task. Everything about the space is fluid and dynamic — from the commercial internet itself to the complex laws and card brand rules that help to govern it. By the time you've read through this handbook, some of the rules may have changed. That's OK.

Our plan in writing this handbook was not to create the final, definitive guide to online risk management. Rather, we wanted to offer you and your team some fundamental, universal principles for assessing risk online in some key categories. Even as laws change and new products or services emerge, the foundational approach to evaluating risk remains the same.

We hope you've taken away some knowledge and practical tips that will help you make the internet and payment ecosystems safer. That's our goal at LegitScript. We proactively track dozens of categories of high-risk activity that put payments companies, internet platforms, and consumers at risk. Our monitoring services provide best-in-class solutions for identifying and assessing high-risk activity so that our clients can quickly remove problematic activity and grow their merchant portfolios with confidence. If you're not one of our partners already, schedule a chat with us to learn how we can help you mitigate your risk while growing your business.

Want to learn more about our services, or learn more about a particular topic covered in this handbook? We'd love to hear from you. Reach out to us at legitscript.com/contact.