LegitScript

PaymentCloud

Compliance Tips for Healthcare and Telehealth Payment Processing

Contents

I. Introduction

Of the hundreds of thousands of internet pharmacies that LegitScript tracks in its database, the vast majority — more than 85% — are rogue or unapproved. This means that these businesses are operating in a noncompliant manner and, in most cases, with flagrant disregard for the law.

Sales from illicit pharmacies and telehealth operations have been responsible for deaths, overdoses, and other adverse health effects from substandard or counterfeit drugs, or prescription drugs sold without a valid prescription.

Because of the risks to consumer safety, Visa and Mastercard require merchants who facilitate card-not-present sales of pharmaceuticals, such as pharmacies and telemedicine providers, to register as high-risk merchants under **MCC 5122** and **MCC 5912**. The expectation is that these merchants will be continuously verified and monitored for compliance.

In this FAQ-style white paper, created by LegitScript and PaymentCloud, we help telehealth companies learn about the payment processing industry and understand the special approach card networks take to healthcare providers who want to accept payments.

You'll learn:

- What payment processing is and why you need it
- What high-risk businesses are and how this classification affects you
- Compliance considerations for your business
- How to more easily obtain a merchant account and open up advertising opportunities by getting LegitScript-certified

II. Payment Processing

What is payment processing?

Payment processing is a sequence of technological steps that transfers funds from a customer to a business or individual. This process traditionally involves different security measures, such as authorization, verification, and settlement of transactions through electronic payment systems. The simplest way to describe payment processing is how a merchant accepts payment — an essential part of any business.

Why do you need payment processing?

A payment processor is critical for accepting funds, whether physical or digital. Without payment processing, businesses could not receive payment from credit cards and checks or mobile, online, or contactless methods. Payment processing allows a merchant to facilitate transactions in various ways, highlighting its benefits and necessity.

How does it expand business opportunities? How are you limited without it?

Payment processors expand business opportunities for merchants in many ways. In addition to allowing businesses to accept both traditional and alternative payment methods, they offer enhanced security and fraud protection, advanced e-commerce, shopping cart, and POS systems, automated subscription and recurring billing options, reliable compliance support, and strong data analysis. Without a payment processor, merchants are forced to navigate the marketplace alone – severely limiting their ability to operate.

III. High-risk Businesses

What is a high-risk business, and why is healthcare/telehealth considered high-risk?

High-risk businesses have an elevated risk of financial exposure, which can depend on numerous factors. Businesses can be labeled as "high-risk" due to:

- Excessive chargebacks and/or refunds
- Fraud-prone industry
- High-risk transactions
- Lack of business history
- Reputational risk
- Poor credit score
- Process recurring payments

Specific industries, such as CBD, adult entertainment, gambling, and firearms, have a merchant category code (MCC) that flags them as part of the high-risk field.

Although it may seem surprising, healthcare/telehealth also falls into this category, due to:

- **Chargeback Risk:** Healthcare transactions can involve large sums of money. Often, this leads to disputes over services rendered, insurance coverage, or billing errors, which can result in excessive chargebacks.
- **Regulatory Compliance:** This industry is heavily regulated to protect patient privacy and safety.
- **Fraud Risk:** Healthcare transactions can be prone to cybersecurity attacks due to the high value of medical services, products, and patient data. Fraudulent claims, stolen identities, or unauthorized use of medical insurance can end in financial losses for payment processors, highlighting this industry's considerable risk.

- **Complex Payment Structures:** Healthcare transactions often involve complex billing structures, such as co-payments, deductibles, and insurance reimbursements. This complexity can lead to errors or disputes, resulting in chargebacks or delayed payments.
- **Reputational Risk:** Payment processors may want to avoid associating with merchants in the healthcare industry, mainly if they perceive a potential for negative publicity due to billing disputes, regulatory violations, or data breaches.

How do payments companies vet high-risk merchants and healthcare/telehealth companies in particular?

Due to the sensitive nature of the business, payment companies take extensive measures to vet high-risk merchants. They can determine if a high-risk merchant has a viable future through underwriting, risk assessment, compliance verification, processing history, background and credit checks, and evaluating a company's overall financial health.

For healthcare/telehealth companies, there are a few more credentials to consider. Medical licenses and agreements with pharmacy partners are required. Payment companies need evidence that the companies in question can legally dispense medications and healthcare products. Without these documents, the potential for financial and legal risk is too great for payment companies to move forward.

IV. Compliance Considerations

What are the compliance considerations for companies looking to get a merchant account?

There are multiple compliance measures that a company must follow to open a merchant account.

PCI Compliance: If you accept credit cards in any capacity, you've discovered the importance of PCI Compliance. PCI Compliance occurs when businesses certify that they adhere to the strict security standards required to operate a credit card machine. Due to the sensitivity of the consumer data stored during the transaction process, there is a high risk of data breaches. So, the five largest credit card providers created the Payment Card Industry Data Security Standards (PCI DSS) to counter potential threats. These standards consist of 12 PCI Compliance requirements, which provide merchants with the guidelines to keep their data secure from cyber attacks.

NACHA Compliance: If your business accepts or issues Automated Clearing House (ACH) payments, you must follow NACHA Compliance. ACH payments are used for payroll, vendor invoices, consumer direct deposits, and tax refunds. Under the jurisdiction of the Federal Reserve, NACHA guarantees the safety and security of electronic payments.

KYC Verification: Know Your Customer (KYC) is critical for preventing money laundering in the financial sector. To open a business, international, or investment account, you must become KYC-verified. To do so, you need to provide various legal documents, such as your business license, address confirmation, ownership structure, and government-issued identification. Each bank and financial institution has its own KYC compliance steps to follow; otherwise, they risk significant penalties and fines.

Obtaining **LegitScript Certification** is another critical component of compliance if you are a merchant in the healthcare/telehealth field. Once certified, approved merchants can demonstrate their legitimacy to the marketplace and accept payments for medication dispensing and other services. For more information on how the LegitScript Certification works, see the following section.

V. LegitScript Certification

What is LegitScript Certification?

LegitScript offers a highly recognized seal of approval provided to verified businesses in highly regulated industries including healthcare, CBD, and addiction treatment. LegitScript-certified entities are vetted to ensure they operate legally and in compliance with applicable laws and regulations. LegitScript Certification is recognized by major companies and platforms like Google, Bing, and Visa, and works to support these platforms in confidently onboarding the businesses we certify. Our seal of approval also supports consumers in identifying legitimate and compliant businesses within these high-risk industries.

What are the key aspects of LegitScript Certification?

Compliance With Laws: Certified entities must comply with all relevant laws and regulations, and possess all required licensure to operate in compliance with these laws.

Transparency: Certified providers must be transparent and compliant within their operations. This includes, but is not limited to, accurate domain name registration, public disclosure of business locations, and accessible contact information for patient inquiries and consultations.

For entities that dispense medications, LegitScript ensures that prescriptions are issued based on a legitimate patient-prescriber relationship as defined by applicable laws.

Background and History: LegitScript conducts thorough reviews on submitted businesses, its principals, and affiliates. This includes verifying the absence of significant disciplinary actions, criminal records, fraudulent activity, and ensuring that the business, and affiliates of the business, comply with all Certification Standards.

Privacy and Security: Businesses must adhere to stringent privacy and security standards to protect patient information. This includes using secure transmission technologies and complying with privacy laws like HIPAA.

Ongoing Monitoring: LegitScript continues to monitor certified entities to ensure ongoing compliance throughout the certification lifecycle.

Our Healthcare Certification Standards provide a comprehensive list of all criteria that must be met in order to be certified.

What is the value of having certification?

When LegitScript approves a business, it demonstrates to the marketplace that it operates securely and legally. Once certified, merchants can showcase their compliance, opening them up to online advertising opportunities and the ability to participate in e-commerce and payment processing programs. Therefore, businesses can reach a wide net of people, having every opportunity to build a strong consumer audience. Since LegitScript is considered a leader across highly regulated industries, its certification gives any business legitimacy in its field.

How are you limited without LegitScript Certification?

Many banks, advertising programs, social media platforms, and e-commerce websites require certification from a recognized organization like LegitScript to support your merchant account. Without certification, merchants risk being shut out of these platforms — and, most importantly, may be unable to open a merchant account or advertise their business. Without advertising visibility or support from banks, a business cannot properly function, drastically limiting its growth opportunities.

LegitScript's Healthcare Merchant Certification program in particular provides a recognized stamp of approval for businesses that facilitate transactions for pharmacies. Our healthcare certification is recognized by entities such as Visa, Mastercard, Google, Microsoft Bing, Facebook, LinkedIn, and TikTok.

Benefits of Certification

The below section details various benefits businesses stand to gain by possessing a LegitScript Healthcare Certification:

Enhanced Consumer Trust

- **Credibility:** LegitScript certification is a mark of legitimacy and compliance with industry standards. It reassures consumers that the certified provider is trustworthy and operates legally.
- **Reputation:** By displaying the LegitScript certification seal on their websites, providers can differentiate themselves from non-certified entities, which is particularly important in the healthcare industry where trust is paramount.

Access to Major Platforms

- **Advertising:** Certified providers can advertise on major platforms like Google, Bing, and Facebook, which often require LegitScript Certification for healthcare-related advertisements. This expands their reach and potential customer base.
- **Payment Processing:** Certification can also facilitate smoother transactions with payment processors like Visa and Mastercard, which look for certification from a third party as a sign of compliance with industry regulations.

Regulatory Compliance

- **Legal Adherence:** The certification process ensures that providers comply with relevant laws and regulations, reducing the risk of legal issues and penalties. This includes compliance with controlled substances laws, compounding practices, telemedicine regulations, and patient privacy laws like HIPAA.
- **Ongoing Monitoring:** LegitScript's continuous monitoring helps ensure that providers remain compliant over time, providing ongoing assurance to both regulators and consumers.

Competitive Advantage

- **Market Differentiation:** In a competitive healthcare market, LegitScript certification can serve as a key differentiator, helping providers stand out as reliable and compliant service providers.

- **Customer Confidence:** Enhanced trust and transparency can lead to increased customer confidence and loyalty, driving repeat business and positive word-of-mouth referrals.

In summary, LegitScript Certification provides businesses with numerous benefits that can enhance their credibility, compliance, and operational efficiency. These advantages not only help in building trust with consumers, but also provide access to important advertising and payment platforms, ensure regulatory compliance, and support compliant business practices.

What healthcare businesses qualify for certification? Which do not?

Many types of healthcare businesses qualify. Below is a list of potential LegitScript Certification recipients.

- **Pharmacies** (including internet pharmacies, mail-order pharmacies, brick-and-mortar pharmacies, local pharmacies with remote dispensing, internet veterinary pharmacies, and sterile compounding pharmacies)
- **Telemedicine and telehealth** (providers that facilitate prescribing)
- **Supply chain merchants** (including pharmaceutical manufacturers, wholesalers, and distributors)
- **Other healthcare merchants** (prescription eyeglasses and contact lens merchants, price comparison websites/apps, and discount pharmacy websites/apps)
- **Pharmacy aggregators and facilitators:** including any platform that processes or facilitates card-not-present transactions for pharmacies

In general, businesses that are not involved in facilitating the manufacture, sale, or prescription of prescription-only drugs are likely not in scope for our program. Inquiries regarding scope can be sent to LegitScript's Client Relations team at certification@legitscript.com.

What are some common compliance issues that we help healthcare/telehealth companies with?

LegitScript assists with compliance issues in the following ways:

- We identify and and correct inadvertent errors in compliance with pharmacy and telemedicine regulations.
- We offer access to a comprehensive supplements, drugs, and healthcare products database that allows companies to check the status and legitimacy of these product's ingredients and the websites that sell them.
- We protect affiliated companies against cybercriminals with actionable investigative analysis.
- No additional domain name expenses are required. Only pay a simple application and annual monitoring fee to maintain your LegitScript-certified status.

What are some common compliance issues that we identify and help rectify?

- **Compliance with licensing requirements across multiple jurisdictions.** When businesses expand outside of their home state or country, licensing regulations can become quite complicated. LegitScript ensures that merchants hold the proper and necessary licenses in order to operate compliantly in all jurisdictions the merchant serves.
- **Compliance with telehealth regulations.** Each US state has its own guidelines and regulations pertaining to telehealth that providers must abide by, but those requirements vary state to state and country to country. Common telehealth compliance issues that LegitScript has identified include:
    - Ensuring the merchant utilizes the necessary technology modalities to conduct consultations (i.e., are consultations conducted via video call, questionnaire, store-and-forward technologies)

- Ensuring that patients are provided with all required information about their medical provider(s) where required by law such as license numbers, specialties, and contact information

- **Marketing and website content.** LegitScript ensures that merchants advertise their products and services in compliance with applicable laws and regulations. This includes verifying that any claims or descriptions regarding a merchant's products or services are transparent, truthful, and do not mislead consumers about the safety or efficacy of the treatments.

Thank You

For more information on payment processing or obtaining a merchant account, contact the team at PaymentCloud.

To learn more about LegitScript or start the application process, visit our Healthcare Merchant Certification page.

VI. Resources

PaymentCloud

What Are High-Risk Businesses? How to Handle Being Labeled "High-Risk"

What Is Payment Processing & How Does It Work? The Ultimate Guide

What Is a Payment Gateway? A Comprehensive Guide

How to Get a Merchant Account in 5 Simple Steps

What is PCI Compliance: The Facts You Need to Know

What Is NACHA? Regulations, Compliance, and Benefits

LegitScript

LegitScript Healthcare Merchant Certification

LegitScript Healthcare Merchant Certification Fact Sheet

LegitScript Healthcare Certification Process

LegitScript Certification FAQs

Other

Healthcare Sector Cybersecurity (HHS)

How Do Payment Processors Determine a Merchant Is a High Risk? (eCheckPlan)