worldpay

Compliance Risk Guide 2025

Compliance Department

2025

Compliance Risk Guide 2025

Getting Started

This guide gives Partners an overview of our higher risk processes and procedures, aiming to provide transparency and accountability, and guide business decisions to support your growth. Payrix uses various risk mitigation techniques through its fraud and transaction risk teams for onboarding and monitoring to protect merchants. Additional details can be found in the Merchant Risk Guide 2025 and the Merchant Onboarding Guide 2025.

What is this guide for?

As a payment-facilitator ("PF") that participates in the payment ecosystem, we rely on some of our relationships with other participants in the system that enables us to perform the unique business model and relationship we maintain with you, our Partners. We comply with all relevant laws and regulations to maintain high compliance and security standards, preventing financial crime and abuse. As a semi-regulated entity, we are obligated under laws like the Bank Secrecy Act and the Patriot Act to detect, prevent, and report money laundering and terrorist financing. We conduct continuous risk assessments to mitigate threats, similar to how you manage your business standards and strategies.

Contents

High Risk Areas

What is Money Laundering?

Money laundering is the activity described to disguise the proceeds of crime into appearing legitimate so that it can fund a criminal lifestyle – or criminal enterprise. There are three stages to money laundering. Placement, layering and integration.

Placement refers to moving criminal funds into the same place as legitimate funds.

Layering refers to disguising the funds ("washing") them with the legitimate funds that disguises their criminal origin

Integration refers to when the money 'exits' the layering stage and re-enters the economy to be used as though it had never been used for crime.

In the context of Payrix, our greatest risk is in the placement and layering stage as we enable payments to be accepted from a wide range of sources – into businesses (merchants), that by us facilitating those transactions could be performing the activity of 'layering' – disbursing to a merchant for them to use their 'revenue' to reintegrate those criminal funds for their own purposes.

It is done by concealing these proceeds to hide the nature, source, location, situation and movement of a crime – to make the ill-gotten gains look legitimate and manifest in a variety of different ways.

Money laundering usually has links to other predicate offences like fraud, but unlike fraud, the means of which the money has been obtained are criminal in nature and can be from drugs, human trafficking, modern slavery, or other types of crime.

What is Terrorism Financing?

Terrorism Financing is when money from legitimately sourced income – not usually criminal proceeds, is used as a method or means to fund terrorist activities. It can be performed by individuals or entities. It is particularly difficult to detect because it can and does use legitimate business fronts as well as potentially criminal operations.

What is an Unusual Activity Report?

An Unusual Activity Report (UAR) or Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) are all the same language that are used to define a regulatory mechanism for a company to protect itself and dispose of its own legal obligations that prevent it from breaking the law. In the US, a UAR/SAR/STR is a document that financial institutions must file whenever there is a suspected case of money laundering or terrorist financing and are used as active tools for law enforcement agencies to report suspected criminal activities.

How do we prevent it?

Unfortunately, that's where this conversation becomes difficult. We, as an entity under the law, cannot 'tip off' a suspect of an unusual activity report ("UAR") / suspicious activity report ("SAR") – it's against the law for us to do that, and the same goes for many of the other financial institutions in their day-to-day operations, to tell you about any suspicion(s).

If we alert the wrong people (and in doing so break the law), it could help criminals or terrorists hide their activities or change their tactics. They might move assets out of our system, make them look legitimate, or transfer them to another institution and continue with the activity. This would allow them to conceal their wrongdoing, which we aim to prevent.

Useful Terminology

Risk Based Approach

A risk based approach ("RBA") is where a business takes into consideration all of the elements that make up its business, including how it acquires its customers (whether by online, or physically in person), the types of products it offers (some products are regulated as higher risk: think forex, cryptocurrencies) while others are lower risk, but may hold diverse types of risk (think foreign exchange or sending money abroad) – and then how it performs its own risk mitigations.

Payrix has defined its own risk-based approach, based off the risk assessments it has performed and has more personalised controls against its risks of business. Because Payrix holds and uses customer data that is important to you – we must have certain Information technology standards

(as, for example, personal information and payment information is transferred from party to party) informed by the International Standards Organisation (like SOC II audits) and certifications that not only help protect you: these are internationally recognized standards that we have demonstrated steps that Payrix takes to defend you, and itself.

An effective RBA means that Payrix has been able to execute risk assessments that enable it to articulate its personal risks and apply proportionate measures in those areas – and you see the outcomes of those in where we add friction like if a bank account is changed too many times and we want to ensure that you and your merchants not being a victim of targeted fraud.

Ongoing Monitoring

Ongoing monitoring involves using technology and human review to spot suspicious transactions and trends, complementing due diligence and customer knowledge efforts to prevent fraud, phishing, and account takeovers. It ensures a comprehensive review of merchants, applying a risk-based approach, which may include more frequent human reviews for higher-risk businesses. Advanced algorithms and tools help minimize exposure to criminal activities like money laundering or terrorist financing.

Enhanced Due Diligence

Enhanced due diligence involves applying additional oversight during customer onboarding or ongoing monitoring when encountering higher-than-usual risks, which we have previously accepted based on our 'risk appetite.' This includes higher-risk businesses like online pharmaceutical sales, cannabis, or firearms merchants. We have an internal process to manage these high-risk businesses that include applying appropriate mitigations to ensure we gather only necessary information based on the risk they pose to Payrix.

Sanctions Screening

Sanctions screening is a process that enables organizations to identify, assess, and manage potential risks associated with individuals or entities that are on international sanction lists. Sanctions aim to prevent funds from supporting inappropriate causes. In the US, the Office of

Foreign Assets Control (OFAC) manages the Specially Designated Nationals and Blocked Persons List (SDN List). As Payrix operates in multiple countries, there are other lists which allow Payrix to maintain a compiled list of sanctions lists like Australia's United Nations Security Council ("UNSC"), the UK's Office of Financial Sanctions Implementation ("OFSI") and Canada's Special Economic Measures Act ("SEMA") – as well as global regimes like the United Nations consolidation lists. As a global leader in sanctions, the US sets standards that many countries follow. Payrix uses tools during onboarding and monitoring to ensure no one on this list is onboarded.

Sanctions can be comprehensive, affecting all transactions, or selective, targeting specific industries. Payrix has policies to prevent blocked individuals from accessing their services and identifies them if they appear on the list later, maintaining compliance with jurisdictional laws.

Impacts

Partner Outreach

Customer outreach is sometimes needed by the Compliance team and is not done frequently as it tries to operate 'behind the scenes.' There may be occasions we must obtain more information about a transaction or set of transactions to identify and understand the narrative behind behaviours – there are so many use cases around the world of why certain behaviours may be normal – asking questions is our method of understanding and comprehension because the better we understand your business, the better we can protect you.

To help us ensure that we keep you safe, we may then reach out – we ask for your compliance in this matter. During this outreach, we will always outline our scope in full and try to be as least intrusive as possible.

Voluntary Disclosures

The power of voluntary disclosures allows us to better understand the specific risks that you encounter in your business – as we serve a variety of different sectors and solutions, we are always seeking to improve our risk engine and where we have base mitigations in place as well as more specialised solutions for higher risk areas, voluntary disclosures allow us to drill down

into the specifics of your business strategy and enable you to 'level up' your protections with us.

By making voluntary disclosures, you can provide us with valuable data and information that we can then use to improve our own services and tailor them to the specific needs of your business, thereby benefitting you even further to prevent bad actors and other types of activity that you don't want to see. By doing that, we help generate activity that you do want to see – growth for your business.

How can I make voluntary disclosures?

1. You can raise disclosures through our partner-servicing portal **here**.
2. Alternatively, you can send an email to **px_compliance@worldpay.com.**
3. Alternatively, you can raise an issue to your **relationship manager** who can forward it to us.