payXpert

Beyond the forms

Understanding KYC & onboarding with Financial Institutions for merchants

Radar Ready: Why KYC is your compliance radar in a high-velocity world

A white paper by PayXpert
June 2025

Disclaimer

This white paper is mainly built based on information that is publicly available.

In no circumstances does it reflect details of PayXpert's processes and policies.
It is not meant to represent any advice to merchants.

It primarily focuses on the Know Your Customer (KYC) process for financial institutions providing payment services to merchants.

Context and general explanations

In an increasingly digital and interconnected world, **trust is currency, and Know Your Customer (KYC) is its verification process.** Whether you're a merchant launching your e-commerce business or a retailer, navigating the regulatory requirements for onboarding with a payment company like PayXpert is not optional. It's a foundational step—akin to getting a passport before crossing borders.

What often feels like a bureaucratic nuisance is, in truth, a critical safeguard for merchants and their PSPs (Payment Service Providers). **KYC protects everyone in the financial ecosystem** —from institutions to individuals—by identities, mitigating the risks of financial crimes, including money laundering, terrorist financing, tax evasion, and other illicit activities.

KYC is often generating frustration as well as doubts for merchants and their PSP, and **it can rapidly transform what should be the beginning of a nice collaboration into a tense relationship and in the worst scenario,** it prevents the collaboration from starting—sometimes for good reasons and sometimes for the wrong ones.

Beyond obligation, KYC represents an opportunity. When properly implemented, it unlocks faster onboarding, trusted relationships, and access to global markets.

It's not just about knowing your customer; it's about building the infrastructure for confidence and compliance in digital commerce. This white paper outlines the regulatory framework for KYC and onboarding processes, focusing on how merchants and payment providers can collaborate to fulfil these obligations, and the severe consequences of non-compliance, especially when shortcuts are taken to onboard clients more quickly.

Moreover, **this white paper aims to reduce the misunderstandings that often arise** between merchants or individuals and Financial Institutions **during the Know Your Customer (KYC) onboarding process.**

The purpose of writing such a document is to educate merchants and individuals about the importance of mandatory steps that all financial institutions must follow in a virtually identical manner.

Therefore, a financial institution that does not apply them, while distorting market competition, is also possibly creating a risk for the ecosystem, as well as for its clients.

KYC is also an opportunity to appreciate the vital work and responsibilities performed by the various departments of a Financial Institution to make our financial world more secure.

Table of contents

Financial institutions and their environment

Introduction

A financial institution is a type of financial service provider that facilitates the transfer of funds between parties. Financial institutions in the EU are regulated under the Payment Services Directive (PSD), as well as other laws and regulations, and must therefore adhere to various regulatory requirements, including capital adequacy and anti-money laundering measures. **PayXpert is a regulated Financial Institution ('FI').**

It is supervised by regulatory authorities, which are governmental bodies, regulatory agencies, or supervisory authorities that are legally empowered to oversee, regulate, and enforce laws and regulations within specific areas of the financial sector. **Their primary role is to ensure the stability, integrity, and fairness of financial markets, protect consumers, and prevent financial crime.**

As part of the submission for authorisation and a 'Payment Licence', the FI (Financial Institution) must adhere to strict rules related to its background, financial stability and staff competency, specifically in terms of its leadership and ownership.
It must also engage specific routines in terms of Know Your Customer ('KYC') and Client Due Diligence ('CDD').

Responsibilities of a regulated entity

The rules and regulations that a Financial Institution must adhere to can vary from jurisdiction to jurisdiction. However, the primary responsibilities of a payment entity are to ensure:

- The financial system used only operates with legitimate monies from legitimate entities who are engaged in legitimate operational activities
- That any monies held are retained securely and will not be affected by its financial situation

The responsibility of the FI commences as soon as a business relationship is created with a client, meaning even before any monies or transactional activity occurs.

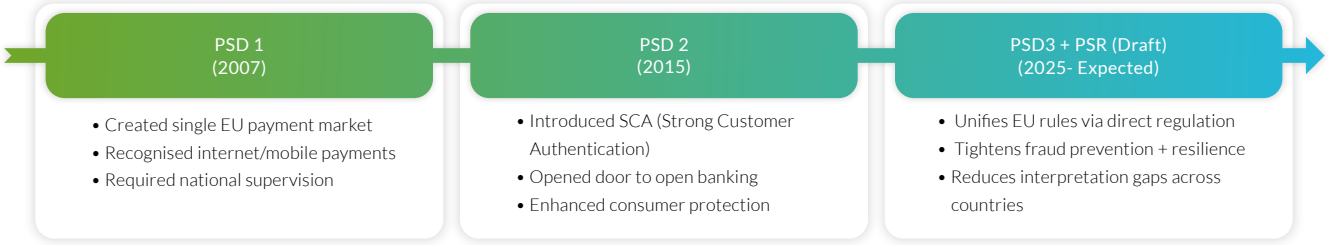
However, it is a key responsibility of the FI to ensure that it completes a full suite of Anti Money Laundering (AML) and Combatting the Financing of Terrorism (CFT) laws and regulations **by detecting any potential or actual suspicion of money laundering (ML) and Financing of Terrorism (FT)** before entering a commercial relationship and thereafter by constant review of any transactional activity or other operational activity of the client relative to the business relationship.

PSD2 and forthcoming PSD3 Directives

The PSD Directives and forthcoming updates require that all payment services providers be authorised (licensed) and regulated. They authorise the relevant regulators to monitor and supervise their activities.

The first European ('EU') Payment Service Directive ('PSD') came into effect on December 25, 2007 December 2007. It considered emerging and innovative payment services, such as internet and mobile payments. EU Member States had until November 2009 to incorporate it into national law and create a competent authority for prudential supervision.

Building on PSD1, the EU adopted "PSD2" in 2015, requiring national implementation by 13 January 2018. Most provisions have applied since then, while the strong customer authentication (SCA) and secure communication measures were phased in later, the key SCA obligation taking effect on 14 September 2019. **PSD2 sharpened consumer protection, opened the door to innovative internet and mobile payments, and tightened security for cross border services.**



To keep pace with digitalisation and rising fraud threats, EU co-legislators are now finalising a third package: the draft Payment Services Directive 3 (PSD3) and the directly applicable Payment Services Regulation (PSR).

Council, Parliament and Commission negotiations are scheduled to conclude in the second half of 2025, with market watchers expecting formal adoption by year end and an 18 month transposition window that would push national go live dates into 2027.

PSD3 largely carries forward PSD2 standards on liability, transparency, open banking and SCA, but — because much of the detail will sit in a regulation — interpretation gaps between Member States should narrow, giving payment service providers a more uniform rule set across the EU.

Each successive directive raises the compliance bar for payment service providers: **PSD1 created a single market, PSD2 mandated open banking and stronger authentication, and PSD3/PSR will deepen fraud prevention duties,** level the playing field between banks and non banks, and embed tougher safeguarding and operational resilience requirements.

That greater burden serves a single purpose—protecting customers. **We don't just move money; we put our clients' security, rights and trust at the heart of every payment we process.**

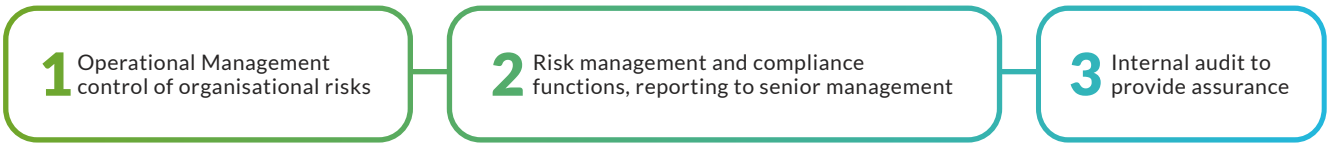
Important people of a Financial Institution

Governance and oversight

The FI shall aim to ensure that the previously mentioned obligations are fully adhered to. In line with this, a culture of risk and compliance should be maintained, led by the governance body.

This ensures that all departments and individuals understand the **importance of protecting the company and its operational activities from involvement in or association with illegal activities.** To facilitate such governance and oversight, the business has a series of well-defined defences:

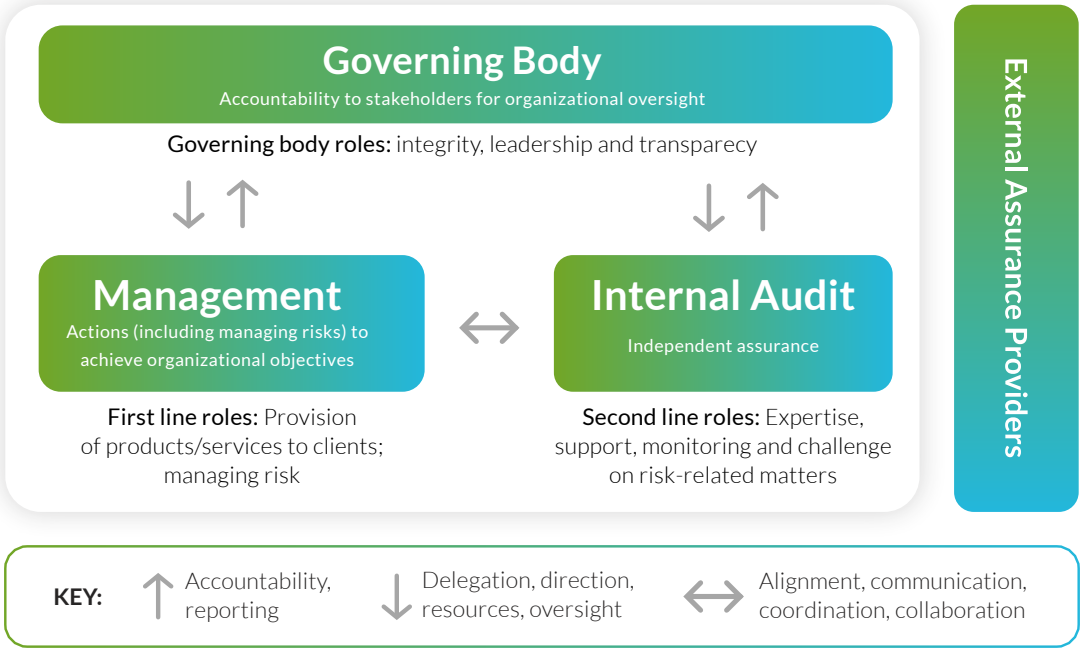
The Three lines of defence



The First line of defence: is the front-line staff who are responsible for managing risks as part of their day-to-day activities. In the context of AML/CFT, this includes Sales, Operational Risk, accounting and finance, and KYC. **Implementing due diligence processes to verify the identity of customers and assess their risk profiles.**

The Second line of defence: is the Compliance and Risk Officers of the entity. In our focus on AML/CFT, the Compliance Officer works to implement and streamline measures that mitigate AML/CFT risks. **The AML Compliance Officer is responsible for developing the entity's comprehensive AML/CFT program,** aligned with its risk exposure.

The Third Line of defence: is the Internal Audit. **The main difference** between this third line of defence and the first two lines **is its high level of organisational independence and objectivity.** Internal Audit may not direct or implement processes, but they can provide advice and recommendations regarding processes.

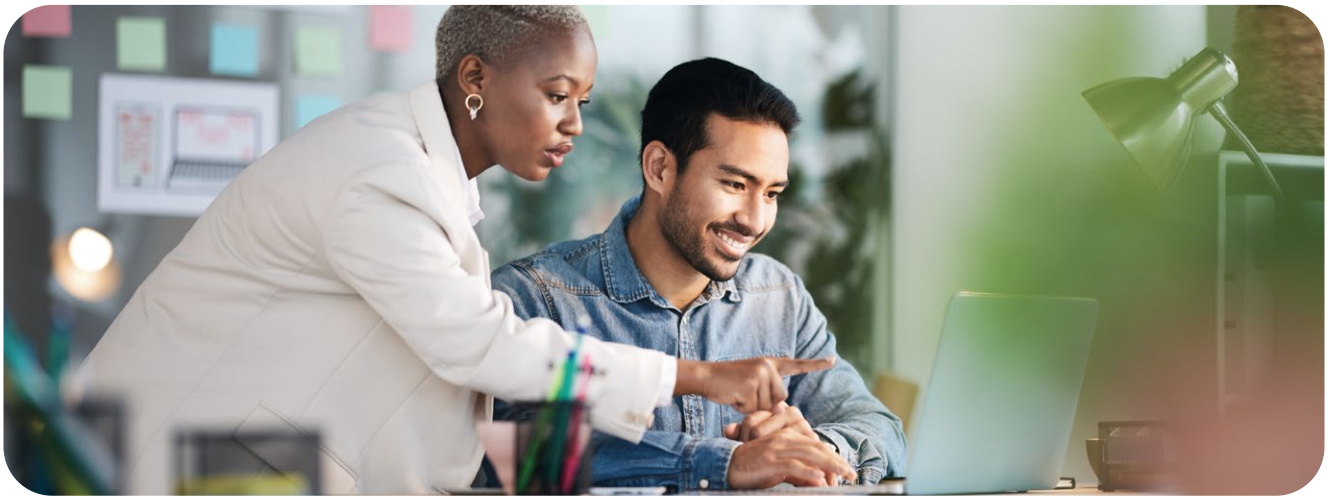


The Sales Representative

The Sales Representative is usually the first contact you have with the company. He will, of course, present a PSP such as PayXpert and its services, its Unique Selling Points and will prepare the nurturing of the relationship by asking lots of questions so he can:

- First, verify the adequacy of your needs with the services we have ready or in our roadmap;
- Then, understand your business and its adequacy with our acceptance policy and risk appetite.
  We want to see if we can provide our services to you or not;
- Then, to be able to explain to the colleagues who are further from the business and who will proceed with the checks and verifications, things that may be difficult to understand and that would trigger further investigation if not previously disclosed.

The Sales Representative or the CSM (Customer Service Manager) will support you with the collection of documents and overall relationship with the other departments of the company. Ensuring a good understanding of your activity and requirements.



The KYC Officer

The KYC Officer is the person who collects all documents, verifies their authenticity, and requests additional documents if needed, typically when required by the acquirers.

This may result in some delay and friction, as the quality of the documents provided and the complexity of your file may raise more questions.

The Money Laundering Reporting Officer ('MLRO')

The Money Laundering Reporting Officer ('MLRO') forms part of the Governance routine of the FI and is an **individual responsible for ensuring that the company remains compliant with the rules and regulations relating to the prevention of Money Laundering.**

They are responsible for **establishing a framework that ensures the protection of the company** and its staff from the risks associated with Money Laundering and Financing of Terrorism.

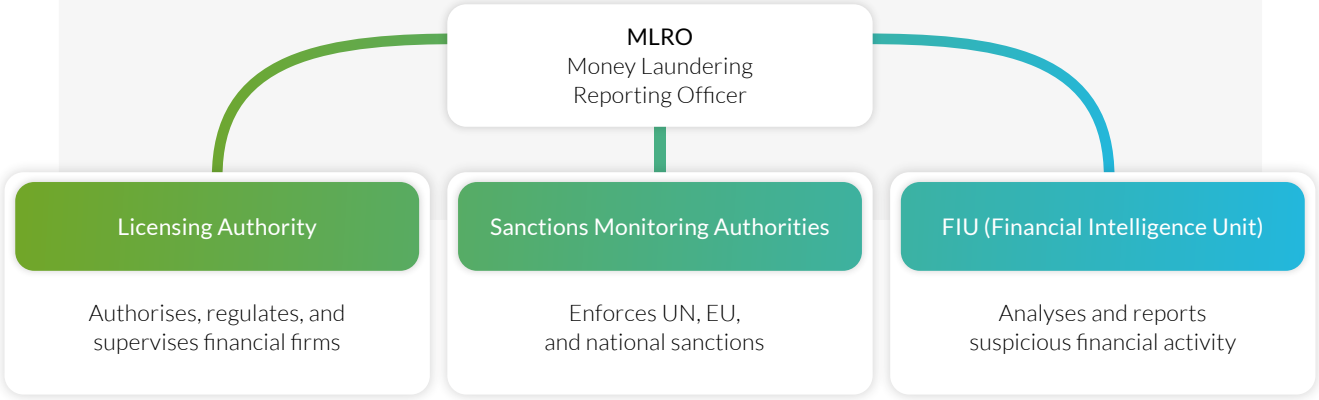
Whilst there are many obligations embedded into the MLRO's role, there are key aspects that must be enacted:

- As part of their responsibilities, the MLRO is required to train all relevant staff every year, confirming their duties and obligations as part of a regulated financial institution. This includes detecting and reporting any doubts they may have regarding a client or merchant, its funding, beneficial owners, and activities. This is known as the KYC process.
- The MLRO reports any relevant matter directly to the board or, if required, to any external regulator or FIU
- It should be noted that the extent of the MLRO's duties can attract significant financial and personal liability
- The MLRO acts as the main point of contact for agencies such as:

A licensing authority - Authorises, regulates, and supervises financial firms and individuals to ensure market integrity, consumer protection, and financial stability

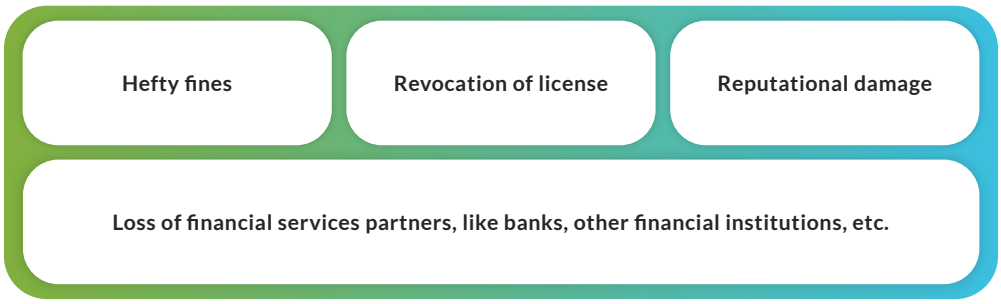
Sanctions Monitoring Authorities - ensures the effective implementation and enforcement of UN, EU, and national sanctions within the country

FIUs - *Financial Intelligence Unit* – A central national agency that receives, analyses, and disseminates information on suspicious financial activities, primarily related to money laundering and terrorist financing, to law enforcement and other competent authorities



Why employees of regulated entities must prioritise KYC

When a payment company like PayXpert is regulated, every employee is effectively part of a compliance mechanism. Whether in tech, sales, operations, or customer service, staff are custodians of regulatory responsibility. Failing to meet KYC obligations can result in:



More critically, it exposes the financial system to abuse by criminals and terrorist networks. Therefore, it's not why employees of regulated entities must prioritise KYC only about safeguarding the regulated company itself but all its customers and partners, and by extension, the financial system. **Employees must view KYC not as a formality, but as a frontline defence.**

Details about KYC and regulation in the Payments Industry

What is KYC, in simple terms?

At its core, KYC – *Know Your Customer* - is a process through which financial institutions verify the identities of their clients.

This process ensures that the business understands its customers and can serve them better while managing its risks. It's mandated under international AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) obligations and is implemented through national and regional laws and frameworks such as:

- **The FATF** (Financial Action Task Force) 40 Recommendations
- **The European AML** (Anti Money Laundering) Directives (4AMLD, 5AMLD and 6AMLD)
- **The Schemes** (Visa, Mastercard, etc.) **rules**
- **PCI** - Payment Card Industry rules
- **CESOP** – Central Electronic System of Payment Information (CESOP is an EU-wide system to report detailed data on cross-border payments to combat VAT fraud, especially in e-commerce)
- **Consumer Protection** – requiring financial institutions to treat customers fairly, and actively ensuring products and services offer fair value, are clearly understood, and are supported effectively throughout the customer journey, while avoiding foreseeable harm by additionally protecting vulnerable people (put another radar illustration)

For all institutions , such as PayXpert, which operate under strict regulatory oversight, **KYC isn't just good practice—it's a legal obligation.** Regulators require payment companies to understand with whom they are doing business, monitor transactions, and ensure that services are not used for criminal purposes. The data gathered during the KYC process must be accurate, current, and retained for a specified number of years, as required by law.

Who requires KYC?

Individuals or companies interacting with a regulated financial services provider must undergo KYC procedures.

This includes:

- Merchants onboarding to payment gateways
- Corporates and startups expanding to new markets
- Medium to high-risk businesses requiring tailored risk assessment
- Sole traders or freelancers offering digital services

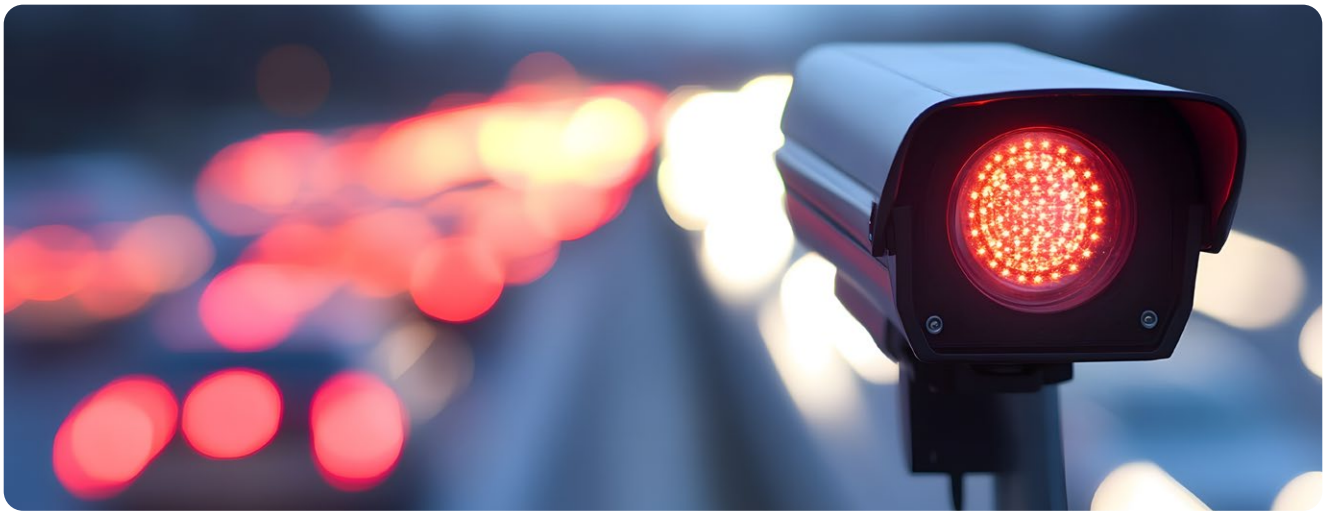
The key elements requested in KYC (and why)

Identifying the people

Element	Purpose
Government-issued ID	To verify individual identity (passport, national ID, etc.). By being independent (government-issued) and valid (unexpired), the financial institution gets comfort that the document proves the identification details of the customer are truthful
Proof of address	To confirm residency and assess jurisdictional risk (can be the Government-issued ID if the address is shown on the document). It can be a utility bill for services that are physically provided, such as electricity, water, or gas. Mobile phone utility bills are not acceptable, but cable television is adequate, given that the service is provided physically
Company registration certificates	To validate legal existence, the incorporation country, date of incorporation and company type
Beneficial ownership documentation	To comply with AML laws by identifying ultimate owners. We need to ensure that the individual who ultimately controls or benefits from the legal entity, even if they are not formally listed as the owner. Any physical person with 25% or more direct or indirect share ownership, with 25% or more direct or indirect voting rights or who has control over the entity is deemed to be a Beneficial Owner (BO). Hiding the UBO would impair the PSP's ability to perform its checks, and as such, it is a situation that will be reported
Business activity description	To assess legitimacy and match with the customer's business. It shall correspond to the business that the Financial Institution will have to process. If it's not clear and straightforward, questions will be raised. Therefore, it's better to anticipate and explain to the sales representative the complexities of your business model so they can better identify any difficulties and help prepare your customer profile and explanations to make the process easier and straightforward for the KYC and Onboarding officers

Element	Purpose
Financial statements	To understand scale, stability, and match to transaction volume expectations. This also provides insights into the company's resilience, its share capital, profit or loss levels, and assets. This will impact the level of risk for the customer
Financial statements PEP, Sanctions and Adverse Media Screening	To assess exposure to Politically Exposed Persons, sanctioned entities and/or jurisdictions or adverse media. Again, this will affect the risk level of the merchant. The more layers of holdings and eventually, in different countries, the greater the risk the company setup represents in hiding UBOs and creating opacity. This does not apply only to small risk companies; huge brands have a complex setup with shareholders and investors from many parts of the world. Adverse media is another indicator of the risk that a company will pose to its users as well as to the PSP. In the event of adverse media, it's better to anticipate and explain the why and how; do not hide, as the PSP will discover it

These elements are essential for verifying identity and assigning a **risk profile**, which determines the depth and frequency of ongoing monitoring.



Identifying the business

Any Business

- Memorandum of articles
- Minutes naming, he governance
- Certificate of good standing stating all elements are still in force at the company
- POA and other delegations exist, giving authority to the person dealing with the FI
- Definition of the UBOs with name and date of birth, and above a certain level with proper ID documents
- Source of Funds: explaining where the funds to create the business and finance its growth are coming from
- Source of Wealth: explaining the origin of the accumulated wealth is of an individual or a company
- Documents proving the address of the individuals, as well as the company
- Documents proving the ownership of the bank account on which funds will be settled
- Is advertising according to activity?
- Complaints on the net about the merchants and their activities?
- Are the General Terms and Conditions coherent?
- Pricing is coherent
- The business model is coherent
- The merchant has the licences for the said activity
- Photo of stock of goods or contracts with providers

E-commerce

- Owner of the domain name?
- The domain name has visitors concerning the turnover
- Is the website working properly and designed accordingly?
- Is advertising according to activity?
- Complaints on the internet about the merchants and their activities?
- Are the General Terms and Conditions coherent?
- Pricing is coherent
- The business model is coherent
- The merchant has the licences for the said activity
- Photo of stock of goods or contracts with providers

Shop

- Picture of the shop(s)
- Verification of the address given
- Is advertising according to activity?
- Complaints on the net about the merchants and their activities?
- Are the General Terms and Conditions coherent?
- Pricing is coherent.
- The business model is coherent.
- The merchant has the licences for the said activity
- Photo of stock of goods or contracts with providers

PLEASE NOTE

The act of hiding information, or not giving clear details when requested will raise doubts that will require further Investigation, documents and will delay the onboarding. Obfuscating the Ultimate Beneficial Owners, having a director that is not the real director, are potentially criminal offenses that can be declared to the authorities. Not being able to justify the origin of funds used to setup the company and fund its activity will also be dedarable.

Periodic KYC refresh and Client Due Diligence (CDD)

KYC must always be conducted at the time of opening a new account or entering into a business relationship.

As the FI is obligated to ensure that it maintains adequate and up to date KYC documentation it may, from time to time, be necessary to obtain additional information from existing clients based on the operational conduct of the account, external changes to key personnel, trading addresses, or based on any regulatory or risk level change.

This is often referred to as CDD. There is often some confusion about the ways that Know Your Customer and CDD relate to each other.

The differentiation is quite simple. **KYC checks are conducted at the start of the business relationship through background checks.** As the business relationship continues, the ongoing process of CDD is also necessary, especially in identifying transactional anomalies or behaviours that may be in breach of Money Laundering Rules.

The Financial Institution must have a defined routine for CDD review for all clients. During the review, any identified issues will be brought to the attention of the board and the Money Laundering Reporting Officer.

EDD (Enhanced Due Diligence)

Enhanced Due Diligence (EDD) measures are heightened verification processes applied to customers and business relationships that present a higher risk of money laundering or terrorist financing.

These measures extend beyond standard customer due diligence (CDD) and **involve a more thorough examination of a customer's background, transactions, and the legitimacy of their funds.**

Evaluation of the business relationship

Once KYC is completed, the Financial Institution will evaluate the potential business using a Customer Risk Analysis (CRA) **to determine if it falls within its risk appetite.** If it is, the IP will then fully engage with that business and allocate it a Risk Rating. This rating will be reassessed periodically throughout the relationship. **The following Risk Factors are considered in assessing the potential business relationship.**

Geographic risk

The risk linked to the countries where the business is based, or the domicile of the individuals, is a significant factor that must be evaluated. If there are differences in language, translated documents may be required. Geographical Risks identified by States and Governments can restrict any engagement or business relationship.

IT security Credit risk

Credit Risk is an assessment, often independently defined, of the financial risk to which the Financial Institution will be exposed in working with a merchant. This would examine the business's creditworthiness, its liabilities, and its Profit and Loss statement.

Reputational risk

This risk exposes the FI to sustaining damage to its reputation by engaging with the business. This can occur when a merchant is publicly involved in a scandal, whether due to its activities or not. Assessment is made on an equitable basis, considering multiple factors related to the nature and extent of the identified issues.

Customer risk

The risk is associated with the customer. **The Financial Institution will check if there are any international sanctions or adverse media on the customer or connected parties.** It will also verify whether the customers (in the case of individuals) or the connected parties (in the case of legal entities) are Politically Exposed Persons (PEPs) or have a connection to PEPs.

Other customer risks relate to complex shareholding structures, opaque beneficial ownership through the use of trusts or bearer shares, or inconsistent or tampered documentation.

Operational risk

Operational risk is associated with risks arising from the merchant's activities.

The risk of chargebacks typically occurs after a few months of activity, either suddenly or gradually, when consumers claim that the merchant has engaged in fraudulent activity.

The level of fraud is also a crucial factor. Both fraud and chargebacks are limited by the Schemes as well as by the acquirers. Even if tools like Ethoca or Verify allow for shortcuts to the chargeback process before it occurs, enabling the merchant to proceed with a refund or discuss the issue with the customer, the fraud alert will remain.

The difficulty to distinguish from the files sent by the acquirers of the first party fraud (real fraud done with stolen cards) **or the Third-party fraud** (friendly fraud where the customer has done the payment but is denying it or not remembering it) **makes that the Financial Institution will have to report all frauds in its regular reporting to authorities.**

The Financial Institution can be challenged on its overall level of fraud as well as on a merchant-by-merchant basis. **For this reason, PayXpert has developed advanced data tools, as well as anti-fraud and velocity checks, that enable merchants to manage their level of chargebacks and fraud better.**

Turning a potential hassle into a benefit

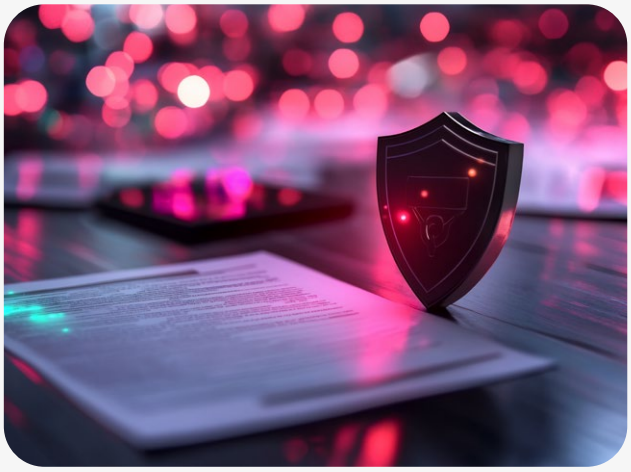
Why merchants should see KYC as a strategic advantage

Merchants often view KYC as a barrier — another checklist, another delay. But it's a gateway to long-term business benefits.

Reputational strength: Compliant businesses signal trustworthiness to partners, investors, and customers.

Lower fraud exposure: A robust KYC framework protects both the merchant and the provider. **Indeed, if the FI did not perform the KYCs adequately, it might be exposed to excessive risks, controls from schemes or regulators, and ultimately expose all its merchant portfolio.**

Trusted relationship: Once KYC has been verified, this ensures a smooth relationship between the merchant and their PSP, and a faster onboarding.



Package readiness: Once your KYC "package" has been completed, you can easily replicate it with other banks or PSPs you're partnering with (if kept up to date).

Future-proofing your business

Global regulations are tightening. What seems optional today becomes mandatory tomorrow. **Merchants who integrate KYC readiness into their operations early on reduce future friction and open doors to domestic and cross-border expansion.**

Partnering with the right PSP can help you navigate these requirements and future-proof your business transactions, and

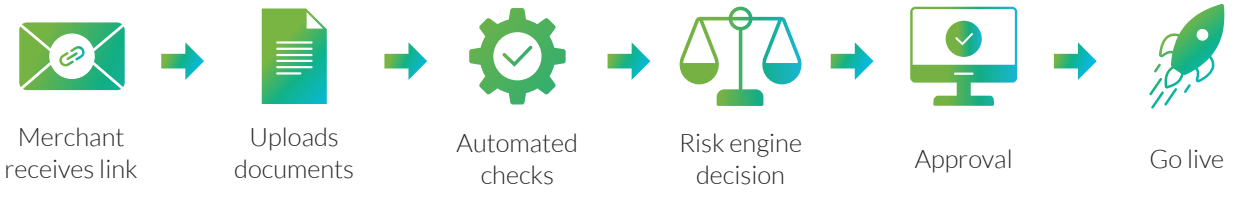
PayXpert's new automated onboarding flow: Compliance at the speed of commerce

Understanding that speed and compliance are often at odds, PayXpert has partnered with Ondorse, a next-generation compliance automation platform, to redefine the onboarding experience.

How it works:

1. **Smart link sent to the merchant**
   Merchants receive a personalised, secure link to upload required documents.
2. **Real-time API checks**
   API connects to official registries to validate corporate and identity data.
3. **Automated screening**
   Integrated checks against sanctions, PEPs, and watchlists reduce manual review time.
4. **Case management in one interface**
   All data is reviewed, stored, and updated in a unified interface accessible across PayXpert teams.
5. **Facial recognition through Liveness test**
   When a face-to-face meeting with the merchant is not possible, the risk level increases. To mitigate this risk, we are using advanced facial recognition tools that enable us to verify the ID documents with their owners.

Advantage	Impact
Seamless experience	Merchants can complete their KYC verification in minutes, not days. We are collecting as many documents as possible from the registries ourselves. We only ask what we cannot get for ourselves.
Standardised compliance	Reduces errors and ensures consistency across jurisdictions
Faster time to market	Enables quicker activation of merchant accounts
Scalability	Onboards more clients without adding manual overhead thanks to the automation of processes.
Real-time risk alerts	Triggers proactive actions if a file becomes outdated or a risk change



Conclusion: From compliance to confidence

The financial ecosystem is only as strong as its weakest link. KYC ensures that the link is fortified. For regulated entities like PayXpert, it's a regulatory requirement. For merchants, it's a smart business move.

By investing in compliance, we're not just ticking boxes. **We're building a safer, more connected world of payments,** especially in a world where technology (notably AI) makes it easier to bypass the systems.

At PayXpert, our mission is to make that future frictionless.

We believe in the importance of educating both our employees and clients and being as transparent as possible. We explain concepts that are obvious in the financial world but complex, and even understandable, to a non-financially educated person.

Want to experience seamless, fast, and secure onboarding for a resilient and durable relationship?

Get in touch with our experts

Here!

Best Practices

Have all your business registration documents, licenses, permits, and tax identification numbers readily available.

Understand your ownership structure, including all Beneficial Owners (BOs), and be prepared to provide personal identification for key stakeholders. The more precise your business information, the smoother the verification process is;

Be completely honest and transparent about your business model, the products/services you sell, your target markets, and expected transaction volumes and values.

Any discrepancies or hidden information will inevitably raise red flags and delay the process;

Provide accurate financial statements and be prepared to discuss your payment processing history, including any past chargeback rates.

This helps the financial institution assess your risk profile accurately;

Maintain meticulous records of all business activities, sales, and customer interactions

to ensure accurate and comprehensive documentation. This demonstrates a professional approach and aids in any future inquiries;

Protect sensitive customer and payment data with robust security measures.

This not only builds customer trust but also helps prevent data breaches that criminals could exploit;

Beyond legal compliance, strive for ethical business practices in every interaction.

This includes transparent pricing, clear terms and conditions, fair customer service, and honest marketing. A strong moral foundation builds enduring trust with customers, partners, and financial institutions alike.

If you encounter any transactions or customer behaviours that seem unusual, inconsistent with typical patterns, or have no apparent economic or lawful purpose, report them to your financial institution without delay.

This is a critical legal obligation and a shared responsibility in fighting financial crime;

When your financial institution requests additional information, respond promptly and thoroughly.

Proactively anticipate their needs and have supporting documentation ready. Remember, they are protecting both themselves and you from illicit activities;

Understand that AML is not a one-time check. Your financial institution will continuously monitor transactions and business activities.

Be prepared for ongoing inquiries and provide updates on any changes to your business, ownership, or operational model;

payxpert

Let's talk payments!

Contact us today to accept seamless payments

France: +33 1 23 45 67 89
Spain: +34 912 345 678

sales@payxpert.com
www.payxpert.com