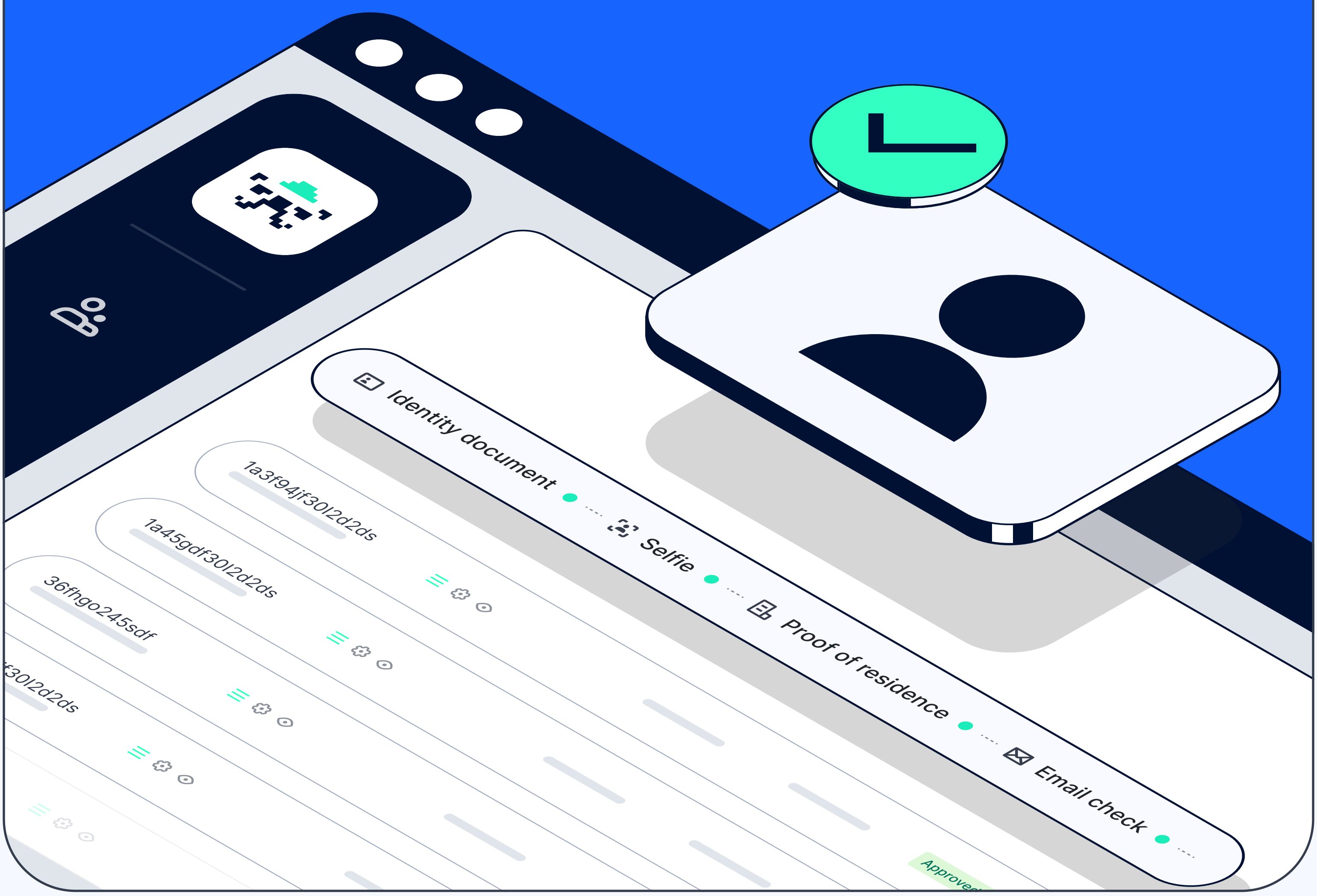
sumsub

The Ultimate KYC/AML and Fraud Prevention Guide For Fintechs

How to combat fraud at every step
of the customer lifecycle



Contents

Introduction 04

Key takeaways 05

Which Fintech companies are regulated and why compliance is essential 07

Fintech regulatory requirements across different regions 13

- Fintech regulations in the US 14
- Fintech regulations in the UK 21
- Fintech regulations in the EU 25
- Fintech regulations in APAC 29
- Fintech regulations in LATAM 33
- Fintech regulations in MENA 36

How to stay compliant without losing clients during verification 39

Building verification flows for Fintech with Sumsub: best practices 41

Success stories: compliance and fraud prevention results achieved with Sumsub 50

Summary 51

About Sumsub 52

Introduction

Anna Stylianou

Founder of AML Cube
and financial crime expert
in conversation with Tony Petrov,
Chief Legal Officer at Sumsub

The major issue with KYC is that people often try to use a tick-box approach.

The one-size-fits-all or "tick-box" approach to KYC/AML and transaction monitoring leads to weak regulatory compliance and fraud. In fact, many Fintech companies still fail to use innovation when identifying, verifying, and understanding clients.

The Sumsub team has created this guide to explain how, why, and where the most dynamic KYC/AML and transaction monitoring solutions should be applied. So, read on to discover how to keep your pass rates and fraud resistance at the highest possible levels.

Key takeaways

The tension between cutting-edge technology and consumer trust can be removed if Fintech businesses know how to implement the following steps:

Don't use the tick-box approach

Apply in-depth KYC/AML and Transaction Monitoring solutions so your company can go beyond generic compliance and offer advanced protection from fraudulent behavior.

Use regulations to innovate

Learn from proven regulatory success stories to help guide your compliance protocols so you can innovate with existing methods.

Tailor verification flows to different customer segments

Create onboarding processes that match your customer segments by using a no-code workflow builder.

Verify at the right time

Perform only the necessary checks at each user-journey touchpoint, so your clients can start using your service with basic verification and then complete more complex checks at later stages.

Consolidate your KYC/AML, KYB, and Transaction Monitoring platforms

Rely on one platform that covers the entire user journey, so you do not waste time and resources on multiple providers.

Check your pass rates

Compare your current client pass rates with world-leading levels to see where you can improve your onboarding metrics.

Lower legal and reputational risks

Speak with compliance experts in the KYC/AML space that can help you avoid risks, fines, and penalties before they happen.

Capitalize on regulatory sandboxes

Join Fintech sandboxes with your compliance and reporting processes at a high level so that you can benefit from new market opportunities.

Leverage AI advantages

Utilize the latest AI technology in your verification to automate workflows and detect even sophisticated types of fraud, such as deepfakes.

Focus on full-cycle client journeys

70% of fraudulent activity occurs after the KYC stage, so Fintech companies must check a client's activities throughout the entire user journey with a continuous Transaction Monitoring process.

Which Fintech companies are regulated and why compliance is essential

What exactly is Fintech?

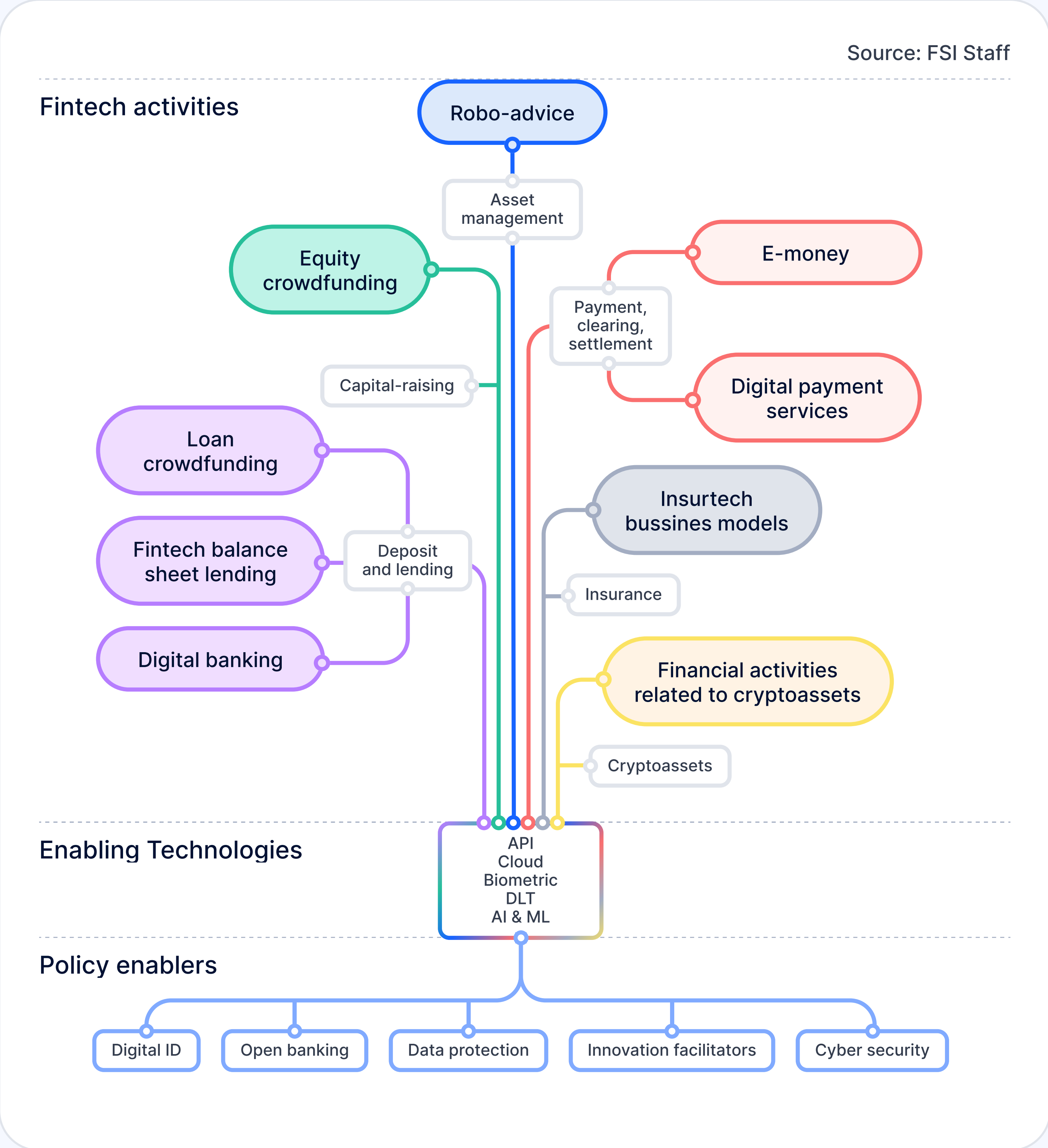
According to the Financial Action Task Force (FATF) Report on "Opportunities and Challenges of New Technologies for AML/CFT" (2021), Fintech is a broad definition that encompasses the use of new and emerging digital technologies in the financial industry for any of a wide range of objectives.

Initially, the term "Fintech" mainly referred to the use of technological innovations to offer fresh financial products and services geared towards consumers:

- Mobile payment solutions
- Online marketplace lending
- Algorithmic savings and investment tools
- Payments in virtual currencies
- Capital raising (crowdfunding)
- Deposit-taking (remote check capture, mobile banking)

In addition to providing automated mid- and back-office enterprise functions, Fintech now also includes the use of cutting-edge technologies for these purposes. Examples include the use of algorithms, big data, AI, machine learning, and link analytics for wholesale clearance, settlement, and other wholesale intermediation for things like securities, derivatives, wholesale finance, and payments, as well as regulatory compliance activities.

The "Fintech Tree" visualization:



From the above definitions, you can see that any financial services company that uses new technologies in designing or producing its products and services can be considered Fintech.

The specific list of regulated companies will depend on the jurisdiction, but in a general sense, the following Fintech companies can be considered regulated:

Credit institutions

Financial institutions, including:

- Acceptance of deposits and other repayable funds from the public
- Lending
- Financial leasing
- Money or value transfer services
- Issuing and managing means of payment (i.e., credit and debit cards, cheques, traveler's cheques, money orders, bankers' drafts, and electronic money)
- Financial guarantees and commitments
- Trading in:
    - money market instruments (cheques, bills, certificates of deposit, derivatives, etc.)
    - foreign exchange
    - exchange, interest rate, and index instruments
    - transferable securities
    - commodity futures trading
- Participation in securities issues and the provision of financial services related to such issues
- Individual and collective portfolio management
- Safekeeping and administration of cash or liquid securities on behalf of other persons
- Investing, administering, or managing funds or money on behalf of other persons
- Underwriting and placement of life insurance and other investment-related insurance (sometimes called InsurTech)

- Money and currency changing

Virtual Assets Service Providers

It should also be noted that not all Fintech companies can be regulated in some jurisdictions.

Fintech firms must abide by AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) laws, because they are comparable to traditional financial firms but use new technological processes.

Key takeaways

Fintech describes modern technology that enhances and automates the provision of financial services. With the aid of specialized tools, it enables business owners and consumers to manage their financial operations, procedures, and lives more effectively.

Lending, payments, international money transfers, personal finance, equity financing, consumer banking, and insurance are all areas where Fintech businesses might concentrate.

The Fintech regulatory landscape and main requirements

There are usually no specific regulations governing the Fintech sector. However, Fintech companies providing financial services must comply with the same laws as any other firms offering similar services.

A comprehensive list of global regulatory frameworks and licensing needs is provided in the next section, but here is a summary of the standard requirements:

- A license from the jurisdiction's financial authority specific to their services
- Compliance with AML/CFT regulations
- Compliance with other applicable acts and laws, i.e., data protection and consumer protection

AML/CFT compliance normally requires the following:

- Creating and implementing AML/CFT policies and procedures
- Appointing a compliance officer and or reporting officer (i.e., the Money Laundering Reporting Officer, or MLRO)
- Conducting personnel training and awareness
- Conducting risk assessment
- Conducting customer due diligence (CDD), including KYC, Transaction Monitoring, and ongoing monitoring of customer behavior and transactions

- Conducting simplified due diligence (SDD) and enhanced due diligence (EDD) (where applicable)
- Sanctions screening
- Reporting suspicious activity and transactions
- Record keeping and maintenance

Many countries also implement Fintech regulatory sandbox regimes, whereby companies can test their products and services in the market (in a live environment) under the guidance and supervision of the regulators.

For supervisors, Fintech sandboxes help to enhance supervisory understanding of new or changed risks brought by Fintech and facilitate an adequate policy response. For companies, it can reduce regulatory uncertainties and help lower the high barriers to entry in the sector.

Fintech regulatory requirements across different regions

Fintech requires simultaneous innovation and regulation.

Contrary to the belief that regulations can hinder progress, the world's leading companies use regulatory standards as a way to move their products and services forward. Indeed, regulation is driving success in the Fintech sector, where companies outside of the regulatory scope follow the example of groups that attain the highest levels of compliance.

Fintech-related regulations differ depending on the product or service being delivered. Plus, there is currently no singular piece of legislation that covers all areas of Fintech, which results in a complex regulatory framework.

The following sections will guide you through a non-exhaustive list of the licensing requirements within different global jurisdictions.

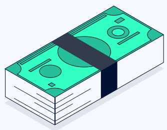
Fintech regulations in the US

Regulators in the US

Fintech businesses may be required to work with any or all of the following regulators:

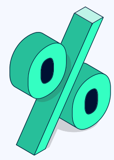
Office of the Comptroller of the Currency (OCC)

The Office of the Comptroller of the Currency (OCC) is an independent agency that charters and regulates all national banks in the United States. This regulator also has the power to grant a national bank charter to Fintech companies engaged in any of the following banking activities:



Receiving deposits

Paying checks



Lending money

Consumer Financial Protection Bureau (CFPB)

The CFPB helps provide consumer protection in the financial industry. It has conducted various enforcement actions against Fintech companies for misleading or abusive tactics, such as unlawful withdrawals from customer accounts and other fraudulent practices.

Securities and Exchange Commission (SEC)

The SEC helps govern the securities business (broker-dealers, investment advisers, and securities exchanges), where it serves three primary purposes: protecting investors, maintaining fair markets, and facilitating capital formation.

Commodity Futures Trading Commission (CFTC)

The CFTC has authority over companies, including trading and derivatives clearing organizations, and intermediaries, while overseeing the US commodities markets.

Financial Crimes Enforcement Network (FinCEN)

FinCEN writes, coordinates, and enforces anti-money laundering (AML) rules for more than 100,000 banks, credit unions, money services businesses (MSBs), insurance companies, securities brokers, casinos, mutual funds, precious metal dealers, and other financial institutions that could be used by criminals to support illegal activities. Plus, since crypto companies are generally considered MSBs, FinCEN is also involved with the AML regulation of crypto assets.

Licensing and registration in the US

The type of licensing and registration required for Fintechs depends on their specific types of activities.

Banking

Fintechs may seek partnerships with traditional and fully chartered banking institutions to avoid complicated licensing procedures.
If a Fintech creates such a partnership, they will be subject to the banking institution's obligations and must comply with their business partner's due diligence, monitoring, and oversight. In this case, it is also common for competitor-versus-collaborator dynamics to develop.

The correct charter or license* for a Fintech providing banking services will depend on its business model. However, for full banking chartership, here is a summary of possible requirements:

Consumer-related banking:
Full national bank chartership

Commercial banking:
Industrial Loan Company (ILC) chartership

Payment activities using blockchain technology:
Office of the Comptroller of the Currency (OCC) payments chartership

Money Services Business (MSB)

FinCEN defines a "money services business" (MSB) as any individual conducting business in one or more of the following capacities:

- Currency dealer or exchanger
- Check casher
- Issuer of traveler's checks, money orders or stored value
- Seller or redeemer of traveler's checks, money orders or stored value
- US Postal Service
- Money transmitter

A company providing money transfer services (including services with virtual assets) or payment instruments is classified as a type of MSB. Such businesses must register with FinCEN and obtain a state license. This licensing requirement applies to all states, with the exception of Montana. However, unless a business is 100% restricted to the state of Montana, it would require money transmitter licenses in all the other US states where customers use the service.

* A bank charter is effectively a business license that is required for depository institutions and certain financial institutions providing other bank-like services. A charter allows a financial institution to perform certain financial services, such as accepting deposits, making loans, and offering a wide range of fiduciary services to its customers.

Insurance (InsurTech)

Fintech insurance (or InsurTech) models refer to the technological innovations that are implemented to improve the processes within the traditional insurance industry. InsureTech does not yet have specific licensing requirements, so it is subject to the same regulations as conventional insurance.

The insurance licensing requirements in the US differ by state and vary depending on the insurer's role. Here is a summary of the most common licensing types:

Agency and individual resident license

Agencies and individual agents must first obtain a resident license from their native state in order to conduct business within state borders.

Surplus lines

A surplus line is a specialized type of license that is issued when an insurer refuses to accept the risk on a specific line of authority because it does not satisfy the state's established guidelines.

Third-party administrator (TPA) licenses

TPA licenses are required for companies, brokers, or individuals who manage different claims-related administrative tasks.

Securities

The Securities and Exchange Commission (SEC) regulates securities, and provides registration for any activities that include giving investment advice or acting as a broker or dealer of securities. This category also includes robo-advice services and cryptocurrency.

Additional financial products

To obtain a license, Fintech companies must be registered with various agencies. Here are two additional financial services and the agencies that regulate their provision:

Lending

Consumer Financial Protection Bureau

Derivatives markets and exchanges

Commodities Future Trading Commission

Regulatory sandboxes

Only state-level regulatory sandboxes exist in the United States at the moment. The most crucial thing for Fintechs to understand is that intrastate regulatory sandboxes may fall under federal control whenever financial activity crosses state lines and becomes interstate. This final step may subject financial transactions and services to federal restrictions that may differ from those of the original state.

The following US states have enacted regulatory sandbox programs:

- Arizona
- Florida
- Hawaii
- Nevada
- North Carolina
- Utah
- West Virginia
- Wyoming

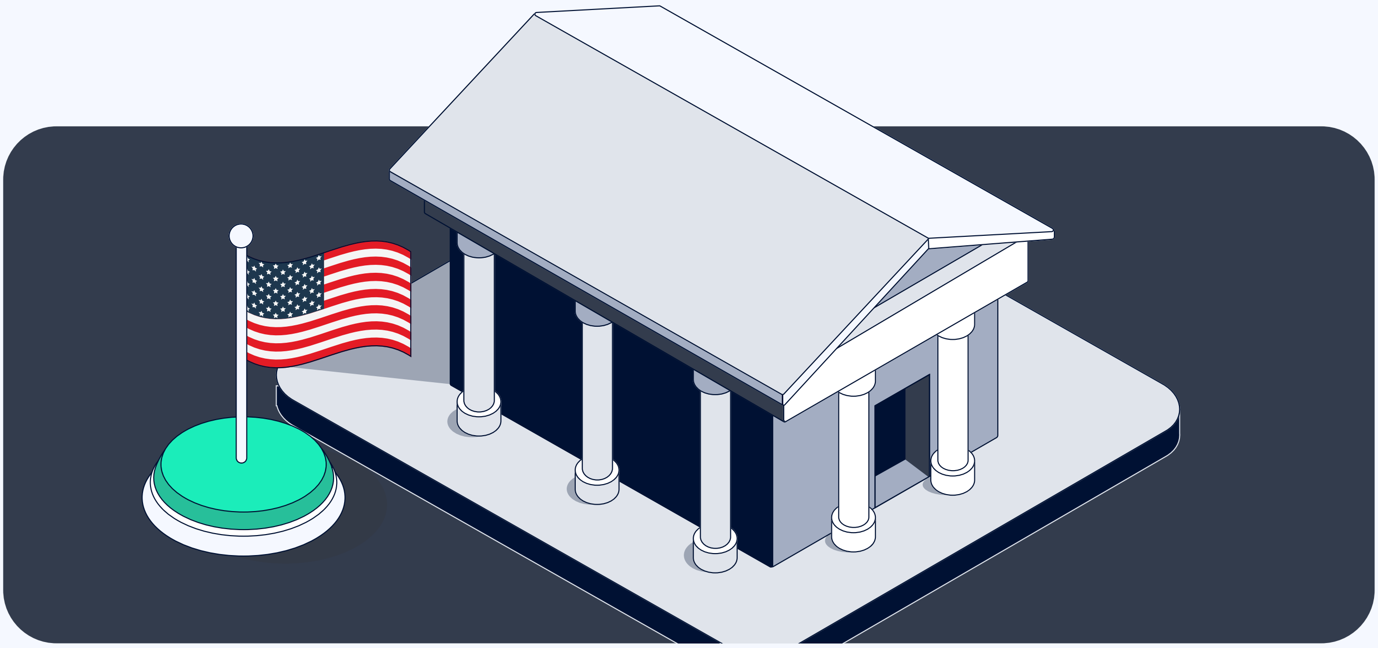
The above sandboxes differ in their scope. Differences include who administers the sandbox (some are administered by traditional state entities and others by newer regulators), and participation may be limited to a specific cohort or via applications from Fintechs who apply over a set period of time.

Conclusion

Due to the presence of both federal and state legislation in the United States, Fintech companies are required to follow both. Besides, it's not possible to obtain a license in one state and work in other states. As a rule, a Fintech company may only be able to operate in multiple states if it obtains a license from each of these states.

There is also a knowledge gap between US regulators and the businesses they are attempting to oversee, although the same is true worldwide. US regulators have been comparatively slow to adjust to the significant changes brought about by the rise of Fintechs.

As both federal and state-level lawmakers become more aware of the unique characteristics of the Fintech industry, efforts will be made to streamline the complex legal system to promote development.



Fintech regulations in the UK

Fintech businesses in the UK may be required to work with one or both of the following regulators:

Financial Conduct Authority (FCA)

The Financial Conduct Authority (FCA) is in charge of regulating the UK's financial markets. The FCA mostly focuses on the risks related to the conduct of supervised companies, and seeks to promote honest and equitable markets by protecting consumers, safeguarding financial markets, and fostering competition.

All types of financial services companies are supervised by the FCA for conduct purposes. Therefore, there are certain types of PRA-supervised companies which are also supervised by the FCA for conduct purposes and called "dual-regulated firms".

Prudential Regulation Authority (PRA)

Banks, building societies, credit unions, and insurers are all subject to prudential regulation and supervision by the Prudential Regulation Authority (PRA). As a regulator and the authority through which the Bank of England operates, the PRA aims to promote the financial soundness of the firms it regulates.

Licensing and registration in the UK

Fintech registration and authorization in the UK depends on the specific types of activities, such as:

Banking

There are no prohibitions or restrictions that are specific to Fintech businesses in the UK, but any Fintech business that offers financial services is subject to regulation by the FCA. Here is a non-exhaustive list of the types of registrations that the FCA provides, depending on the financial service being offered:

Electronic Money Institution (EMI) registration

An EMI Institution registration is required if a Fintech wishes to operate and disburse electronic money (or e-money).

Authorized Payment Institution (API) registration

To provide services such as remittance, payment processing, and managing payment accounts, an API registration may be required.

Small Payment Institution (SPI) registration

Fintechs that provide financial services and have less than €3 million per month in average turnover from payment transactions in the preceding 12 months may require SPI registration.

Money Services Business (MSB)

According to the FCA Handbook, a money service business (MSB) is a company that conducts business by operating a bureau de change (foreign exchange station), sending money or other monetary values via various channels, or cashing checks that are payable to clients. A Money Services Business registration is required to be registered as a MSB in the UK, which requires registration with HM Revenue and Customs (HMRC). If the company is already supervised by the Financial Conduct Authority, it does not also need to register with HMRC.

Insurance (InsurTech)

The FCA and PRA both have regulatory authority over UK insurers, regardless of whether they are traditional or technologically advanced. The insurer and its executives must abide by a set of rules that each of these regulators has established.

Securities and derivatives

The FCA regulates Fintech firms that offer services to customers dealing with "financial instruments," such as shares, bonds, securities, and derivatives, as well as the markets where these products are traded. To operate in this area, a UK FCA investment registration is required.

Cryptocurrency

Fintechs require a registration from the FCA to carry out certain crypto services within the UK. Such a registration is synonymous with FCA registration under the AML/CTF regime. This registration type is required for cryptoasset exchange providers and custodian wallet providers.

Lending

Most companies that provide customers with credit, lend them money, or give them additional time to pay for goods and services must be registered with the FCA.

Regulatory sandboxes in the UK

Here is the most prominent and current regulatory sandbox in the UK:

The FCA Regulatory Sandbox

Businesses can access regulatory knowledge and a set of tools to help with testing through the FCA Regulatory Sandbox. Depending on the nature of their business and the types of tests they are interested in, businesses will require different tools in order to participate in the sandbox environment. Fintechs can use the testing services whenever it is convenient for them throughout the year, and at the appropriate stage of their development lifecycle.

Conclusion

The UK is often highlighted as a leading benefactor of Fintech in the global market. In fact, the UK is only second to the US in the number of Fintech unicorns it has developed. The UK's regulatory landscape plays a key role in this growth, due to the provision of the necessary data required to develop new services while remaining compliant.

Fintech regulations in the EU

From a value-creation perspective, the total valuation of European Fintechs as of June 2022 is approximately €430 billion. Moreover, at least one Fintech in each of the seven largest European economies by GDP (France, Germany, Italy, the Netherlands, Spain, Switzerland, and the United Kingdom) now holds a position in the top five banking services institutions based on market value.

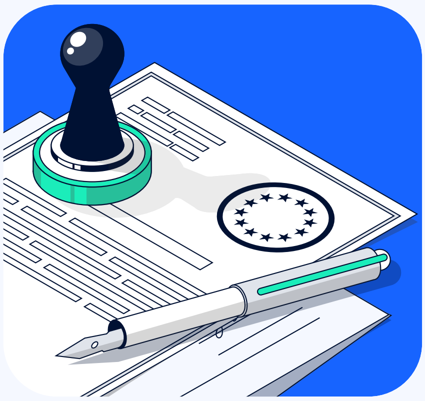
No single piece of legislation on the European level covers all aspects of Fintech. As a rule, Fintech companies must comply with the same laws as any other traditional financial firm offering the same services. Therefore, different laws apply depending on the financial activity that Fintech companies provide (i.e., payment services, crowdfunding, virtual asset services, etc.).

For example:

- The Payment Services Directive (2015/2366/EC)
- The E-Money Directive (2009/110/EC)
- The Credit Institution Directive (2013/36/EU)
- Insurance Distribution Directive (2016/97/EU)
- The Regulation (EU) 2020/1503 on European Crowdfunding Service Providers
- Markets in Financial Instruments Directive (MiFID II) (2014/65/EU)

In 2023, the European Parliament adopted the Markets in Crypto Assets Regulation ("MiCA") and the Regulation on Information accompanying transfers of funds and certain crypto-assets ("TFR"). This is part of the larger digital finance package published by the European Commission in 2020.

All these Acts imply corresponding requirements for Fintech businesses when they provide services falling under the definitions specified in the acts.



It should be noted that the "Regulation" is a binding legislative act. It must be applied in its entirety across the EU. While a "Directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals.

So, different EU members can have different approaches and rules for the regulation of Fintech businesses.

Regulatory requirements that Fintech companies may face include:

- Licensing/registration or other types of authorization from regulatory authorities for operating
- Compliance with AML/CFT and Sanctions Screening requirements
- Compliance with data protection regulation
- Compliance with consumer protection rules

The main regulators

On the European level, at least the following authorities work on common strategy and policy in relation to Fintech:

- European Commission (EC)
- European Banking Authority (EBA)
- European Securities and Markets Authorities (ESMA)

At the national level, Fintech companies are regulated by corresponding regulators, such as the FCA in the UK, AMF in France, CSSF in Luxembourg, and BaFin in Germany.

Sandboxes and innovation hubs

The EBA established a Fintech Knowledge Hub in 2018, bringing competent authorities together in a common setting and enhancing engagement with incumbent and new entrant institutions, other Fintech firms, technology providers, and other relevant parties. It aims to enhance the monitoring of financial innovation, knowledge sharing about Fintech, and technological neutrality in regulatory and supervisory approaches on an ongoing basis.

Many Member states already have regulatory sandboxes and innovation hubs for Fintech businesses in order to facilitate innovations, monitor developments, and mitigate risks that may arise; for example, Portugal, Lithuania, Italy, Ireland, Hungary, and Estonia.

The list of existing regulatory sandboxes and innovation hubs can be found here on the EIOPA Europa webpage.

Regulatory challenges

Despite existing regulations, there are still gaps that need to be filled. Such gaps are related to the unregulated nature of certain areas, the fight against fraud, and the provision of consumer protection, among other issues.

The EU has several projects to tackle the following challenges:

- Improving regulation for crypto-assets
- Revising the Payment Services Directive
- Legislative proposal for a framework for Financial Data Access
- Improving consumer rights
- Leveling the playing field between banks and non-banks
- Combating and mitigating payment fraud

Fintech regulations in APAC

As of May 2023, market research shows that the APAC region has the third highest number of total Fintech startups globally, with 5,061 Fintech companies (behind the Americas: 11,651 and the EMEA region: 9,681).

In the APAC region, there are different approaches to Fintech Regulation. So, the following one can be identified (where in one country, there may be a mixture of all approaches):

- Approaches mainly based on the existing regulation, i.e., based on the financial activity provided (e.g., Singapore, Australia)
- Existence of special laws regulating Fintech. For example, Indonesia introduced several acts regulating Fintech businesses:
    - Financial Services Authority Regulation No. 13/POJK.02/2018 regarding digital financial innovation in the financial services sector, dated 16 August 2018
    - Bank Indonesia Regulation No. 22/23/PBI/2020 regarding payment systems, dated 30 December 2020 (BI Reg 22)
    - Bank Indonesia Regulation No. 23/6/PBI/2021 regarding payment service providers, dated 1 July 2021 (BI Reg 23/6)
    - Bank Indonesia Regulation No. 23/7/PBI/2021 regarding payment system infrastructure providers, dated 1 July 2021 (BI Reg 23/7)

According to Fintech Regulation in Asia Pacific (APAC), Cambridge Centre for Alternative Finance (CCAF), 2022:

- 90% of sampled jurisdictions in APAC have established regulatory frameworks for digital payments
- 90% of sampled jurisdictions in APAC have established a regulatory framework for e-Money
- 85% of sampled APAC jurisdictions have a regulatory framework for international remittances in place, 5% have one under development, and 5% treat it as unregulated or self-regulated
- 50% of sampled jurisdictions in APAC have a bespoke framework that regulates P2P lending, and 6% plan to introduce one. 22% of jurisdictions have prohibited P2P lending, while 22% treat it as unregulated or self-regulated

In the APAC region, there is a tendency to increase the regulation of virtual assets and DLT. So, government and regulatory authorities work on special rules and regulations for such types of activities.

The main regulatory requirements that Fintech companies may face include (depending on the national legislation and activity of the business):

- Licensing/registration or other types of authorization from regulatory authorities for operating
- Compliance with AML/CFT and Sanctions Screening requirements, i.e., companies must have corresponding policies and procedures, conduct Customer Due Diligence (SDD and EDD where required), transaction monitoring, and report suspicious activities and transactions
- Compliance with data protection regulation
- Compliance with consumer protection rules
- Cybercrime rules

Main regulators

Fintech businesses are mainly regulated by national financial supervisory authorities.

Sandboxes and innovation hubs

Sandboxes and innovation hubs are very common in the APAC region. Fintech Regulation in Asia Pacific (APAC), Cambridge Centre for Alternative Finance (CCAF) shows that:

- 16 jurisdictions with at least one innovation office were identified across the region (e.g., Australia, Bangladesh, Bhutan, Cambodia, China, Hong Kong, India, Indonesia, Japan, Kazakhstan, Republic of Korea, Malaysia, Philippines, Singapore, Taiwan, and Thailand)
- 25 jurisdictions with at least one regulatory sandbox were identified (Australia, Bhutan, Brunei Darussalam, China, Fiji, Hong Kong SAR China, India, Indonesia, Japan, Kazakhstan, Republic of Korea, Malaysia, Pakistan, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Taiwan, Thailand, Timor-Leste, Tonga, Vanuatu and Vietnam)

Fintech Innovation Lab Asia-Pacific 2023

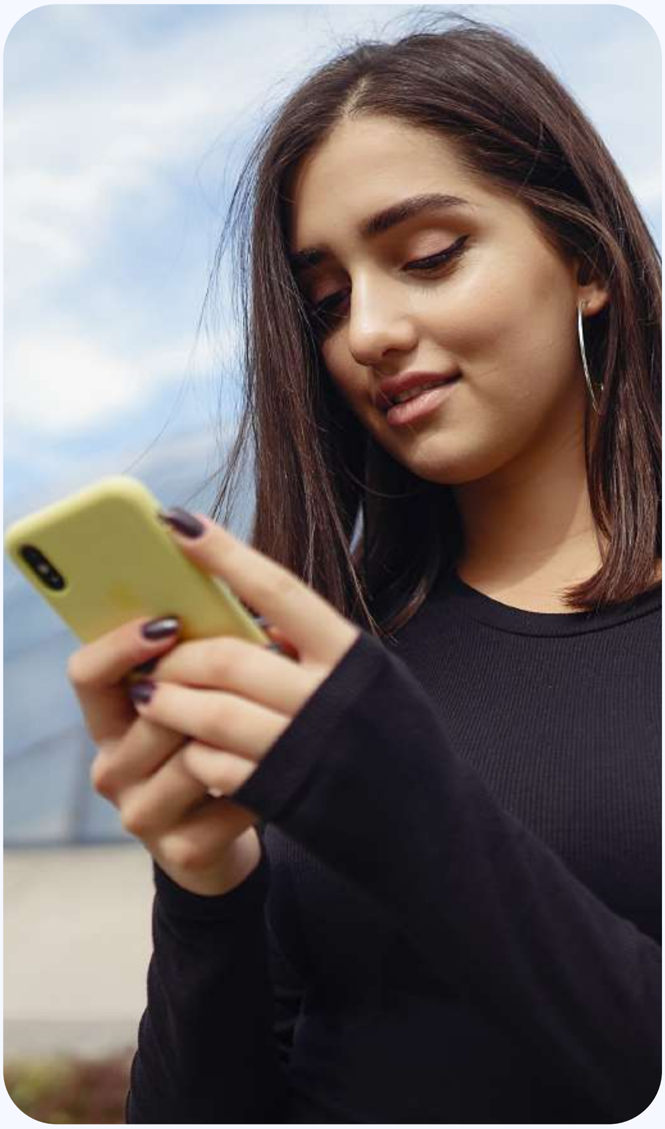
In October 2023, the world will be presented with the Fintech Innovation Lab Asia-Pacific program findings. This global accelerator program is helping ten Fintech startups from 19 different countries/regions address the industry's most important issues. The main focus is on areas such as generative artificial intelligence (GenAI), data analytics, and the use of Web3 technologies to improve the customer experience and drive business growth.

Regulatory challenges

Despite the rapid development of Fintech in the APAC region, various regulatory challenges remain:

- Not all countries have the possibility of conducting non-face-to-face verification
- There can be a lack of regulation for some types of activities
- Each country has its own rules and standards, so more harmonized rules are required

Fintech regulations in LATAM



In the past decade, Fintech has continued to grow in the LATAM financial sector, providing innovations in lending, payments, insurance, and other activities.

Between 2017 and 2021, Fintech companies increased dramatically in all the major Latin American nations. The country with the fastest growth was Argentina, where the number of Fintech companies increased by 383% throughout the period studied. However, despite the growth of Fintechs in Argentina, Brazil still had the most Fintech companies in 2021, with 771 businesses in operation.

Various approaches for Fintech regulation in the LATAM region are similar to those in the APAC region. In particular:

- The "wait and see" approach, i.e., country does not take any concrete actions
- The flexible "test and learn" approach
- The "innovation hubs and sandboxes" approach, which can help to understand new developments and make regulatory changes based on the outcomes. For more details, see the section below

- Adopting new legislation to regulate Fintech companies. An example of such an approach is Mexico, with the Ley para Regular las Instituciones de Tecnología Financiera
- Adaptation of existing norms. According to IMF Fintech Notes, the examples of such an approach can be Argentina, Brazil, and Colombia, which have published acts or amendments specific to existing credit, payments, and crowdfunding acts

The main regulatory requirements that Fintech companies may face include (depending on the national legislation and activity of the business):

- Licensing/registration or other types of authorization from regulatory authorities for operating
- Compliance with AML/CFT and Sanctions Screening requirements, i.e., companies must among other things, have corresponding policies and procedures, conduct Customer Due Diligence (SDD and EDD where required), transaction monitoring and report suspicious activities and transactions
- Compliance with data protection regulation
- Compliance with consumer protection rules

The main regulators

Fintech businesses are mainly regulated by national financial supervisory authorities.

Sandboxes and Innovation hubs

Regulatory sandboxes and innovation hubs are one of the regulatory approaches specified above. There are not a lot of sandboxes and hubs in the region, but the following countries also established innovation hubs (IH): Argentina, Brazilia, Colombia, Dominican Republic, and Costa Rica.
The sandbox programs (SP) are mainly located in: Barbados, Brazil, Mexico, and Peru, among other countries.

Challenges

One of the main regulatory challenges in LATAM is the rapid evolution of Fintech services that often outpaces the existing regulatory frameworks, resulting in regulatory gaps.

Additionally, some LATAM countries experience gaps and inconsistencies in laws, regulations, and enforcement mechanisms. These can leave room for potential risks and vulnerabilities to be exploited.

Fintech regulations in MENA

The MENA region has more than 800 Fintech startups worth over $15.5 billion, and the scale of its ongoing growth rate is partly due to its lack of established financial institutions as well as its population's embrace of new digital approaches.

According to Fintech Regulation in MENA, Cambridge Centre for Alternative Finance (CCAF):

- 92% of sampled jurisdictions in MENA have established regulatory frameworks for payments, with 8% of these frameworks specific to digital payments
- 92% of the sampled jurisdictions in MENA have established a regulatory framework for e-money. In 8% of sampled jurisdictions, they do not regulate e-money, while 50% regulate e-money through a general payments framework, and 42% have created a specific e-money framework
- 80% of the sampled MENA jurisdictions have a regulatory framework for international remittances in place, with a further 10% having one under development and only 10% treating it as unregulated or self-regulated
- 67% of sampled jurisdictions in MENA have a bespoke framework regulating P2P lending, and 17% of jurisdictions plan to introduce a framework. 17% of jurisdictions have prohibited P2P lending, while 17% treat it as unregulated or self-regulated
- 69% of the sampled MENA jurisdictions have a bespoke equity crowdfunding framework, with a further 8% planning to introduce a framework. 8% of sampled jurisdictions have prohibited this activity, and 15% treat it as unregulated or self-regulated

Regulators in the MENA region are also divided into several main approaches, such as:

- Adaptation of existing norms. Such an approach is partially used in UAE, Egypt, Israel, etc
- Adopting new legislation to regulate Fintech companies. The UAE, Egypt and Jordan, Lebanon, Bahrain, Israel, KSA, and Morocco have several specific acts regulating particular Fintech sectors
- Innovation hubs and sandboxes approach (see the section below for more details)
- The "wait and see" and "test and learn" approaches can also be partially applied in different countries

The main regulatory requirements that Fintech companies may face include (depending on the national legislation and activity of the business):

- Licensing/registration or other types of authorization from regulatory authorities for operating
- Compliance with AML/CFT and Sanctions Screening requirements
- Compliance with data protection regulation
- Compliance with consumer protection rules
- Cybersecurity rules

The main regulators

National financial supervisory authorities are mainly in charge of regulating Fintech businesses. There can be new regulators for particular types of activities, e.g., VARA in UAE.

Sandboxes and innovation hubs

In the past few years, the MENA region has seen an increase in the number of innovation hubs and sandboxes. In particular, the following jurisdictions established innovation hubs: Abu Dhabi Global Market, Bahrain, Cyprus, Dubai IFC, Egypt, Israel, Jordan, Palestine, Qatar, Saudi Arabia, Tunisia, United Arab Emirates.

The jurisdictions with at least one regulatory sandbox are: Abu Dhabi Global Market, Bahrain, Dubai IFC, Egypt, Israel, Jordan, Kuwait, Malta, Saudi Arabia, Tunisia, United Arab Emirates.

Regulatory challenges

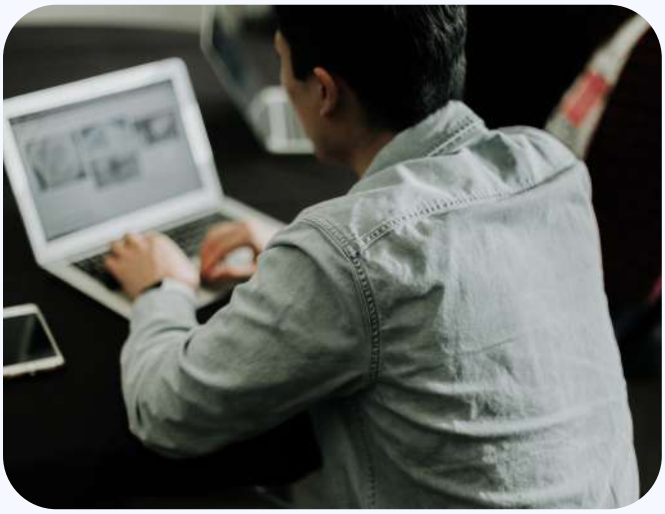
According to Fintech Regulation in MENA, Regulators in MENA have identified a range of internal challenges in regulating Fintech, such as:

- Limited technical expertise within the regulator(s)
- The need to coordinate the activities of multiple regulators
- Limited funding/resources for the regulator(s)
- The small size of firms or industries cannot justify intense supervision
- Regulators’ jurisdiction over this activity is unclear or limited
- Lack of usable/reliable data on firm activities
- Regulatory uncertainty in some jurisdictions
- Regulatory fragmentation

How to stay compliant without losing clients during verification

New technologies bring both benefits and risks. Your customers and the broader public enjoy faster services and efficiency, while fraudsters try to capitalize on compliance weaknesses.

Therefore, it is important to implement effective processes and practices regarding the detection and prevention of financial crimes in your company's activities, including anti-money laundering/counter-terrorist financing (CFT) controls and measures.



AML/CFT requirements can be resource-intensive for both Fintech startups and long-established companies. The following difficulties can arise during the onboarding process:

Data volume

Customer due diligence processes (CDD) (including KYC and KYB), sanctions screening, and transaction monitoring, involve processing and analyzing large amounts of data. This process requires the involvement of a significant number of employees in order to process the data quickly, and it also increases the likelihood of errors.

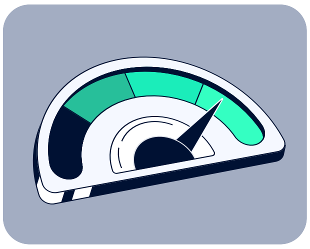
Data aggregation

If your company uses several providers for different types of checks, there can be a problem linking particular checks with the identified person in one profile.

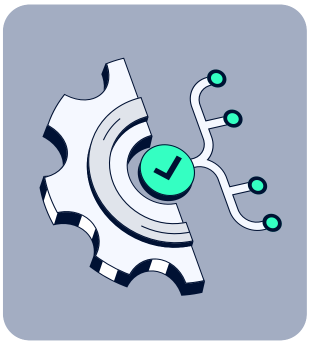
So, Fintech companies need to know the right balance of the above factors. By finding the correct balance, the customer onboarding process is easier, faster, and has better conversion rates while upholding regulatory requirements.

Enterprise-level KYC, KYB, and transaction monitoring processes

Your company needs to automate its verification flows as much as possible. This means finding a service provider which has many services in one platform, including identity verification, sanctions screening, transaction monitoring, and the full range of user journey checks. Plus, the service provider must be able to process different types of data and documents automatically.



You must tailor your verification flows for different customer segments based on their risk profiles and unique criteria. For example, you can make the onboarding process complex for high-risk clients and give lower-risk clients minimum mandatory checks.



You can also consider dividing verification into levels and place checks across the customer journey. So, your company can customize different numbers of checks for the first KYC process and for further steps such as withdrawal or transfer of particular funds. This helps to balance pass rates with the high level of protection.

Building verification flows for Fintech with Sumsub: best practices

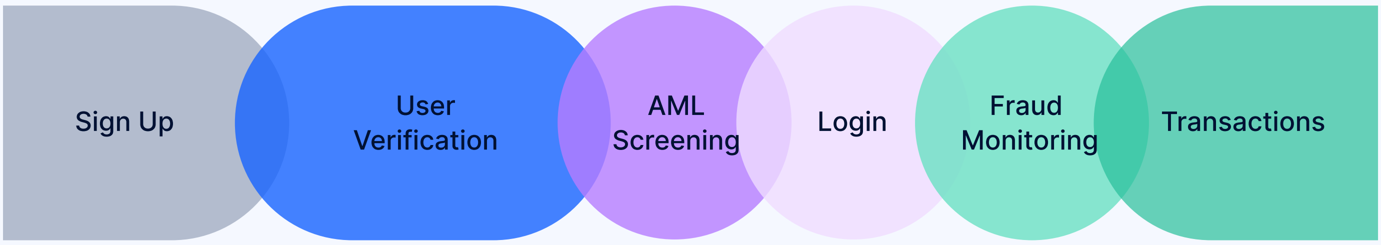
Sumsub helps you create unique verification flows that improve pass rates and reduce fraud

The problem with generic KYC/AML and Transaction Monitoring flows is that high compliance demands multiple scenarios for different customer segments. However, creating these workflows can be tedious and time-consuming to implement. To solve this problem, Sumsub combined automation and orchestration capabilities that allow you to manage user verifications and monitoring through the whole customer lifecycle, code-free.

Secure the whole user journey with one platform

Onboarding Orchestration

Ongoing Monitoring



Sign Up
- Email Risk Assessment
- Phone Risk Assessment
- Device Intelligence

User Verification
- ID Verification
- Liveness and Face match
- Address Verification
- Live Agent Video Call
- Doc-free Verification
- Public Digital Identity Systems
- QES/eIDAS (coming soon)
- NFC
- Known Face Search
- Blocklist Check
- Duplicate Check

AML Screening
- PEP+ Sanctions
- Adverse Media

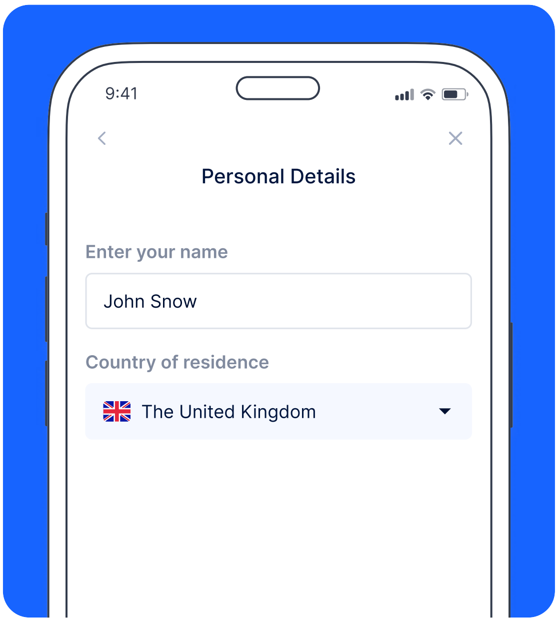
Login
- Device Intelligence
- Behavioral Fraud Detection
- Face Authentication
- MFA

Fraud Monitoring
- Device Intelligence
- Behavioral Fraud Detection
- Face Authentication
- Ongoing AML Monitoring

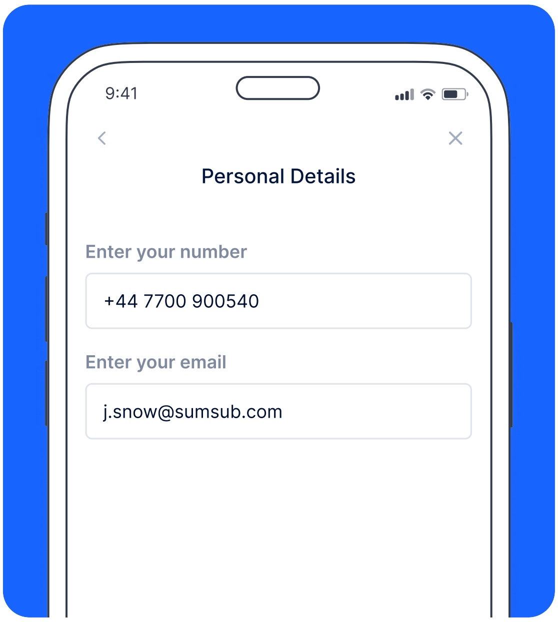
Transactions
- Ongoing AML Transaction Monitoring
- Bank Account Verification
- Fraud Transaction Monitoring
- Behavioral Fraud Detection

Sign up

Sign up and pre-screening with Email and Phone Risk Assessment



The user can identify themselves at registration by providing their name and country of residence (or nationality) without submitting any documents. This is a simple setting that allows fast registration.



You can also leverage pre-screening checks like Email and Phone Risk Assessment that can extract comprehensive information on the email's data deliverability, disposability, and suspiciousness, as well as a phone number, to identify potential fraud patterns.

Verification

ID verification

After the applicant uploads a photo of their ID, it's verified in three general steps:

Authenticity check

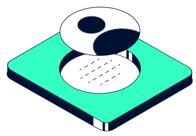
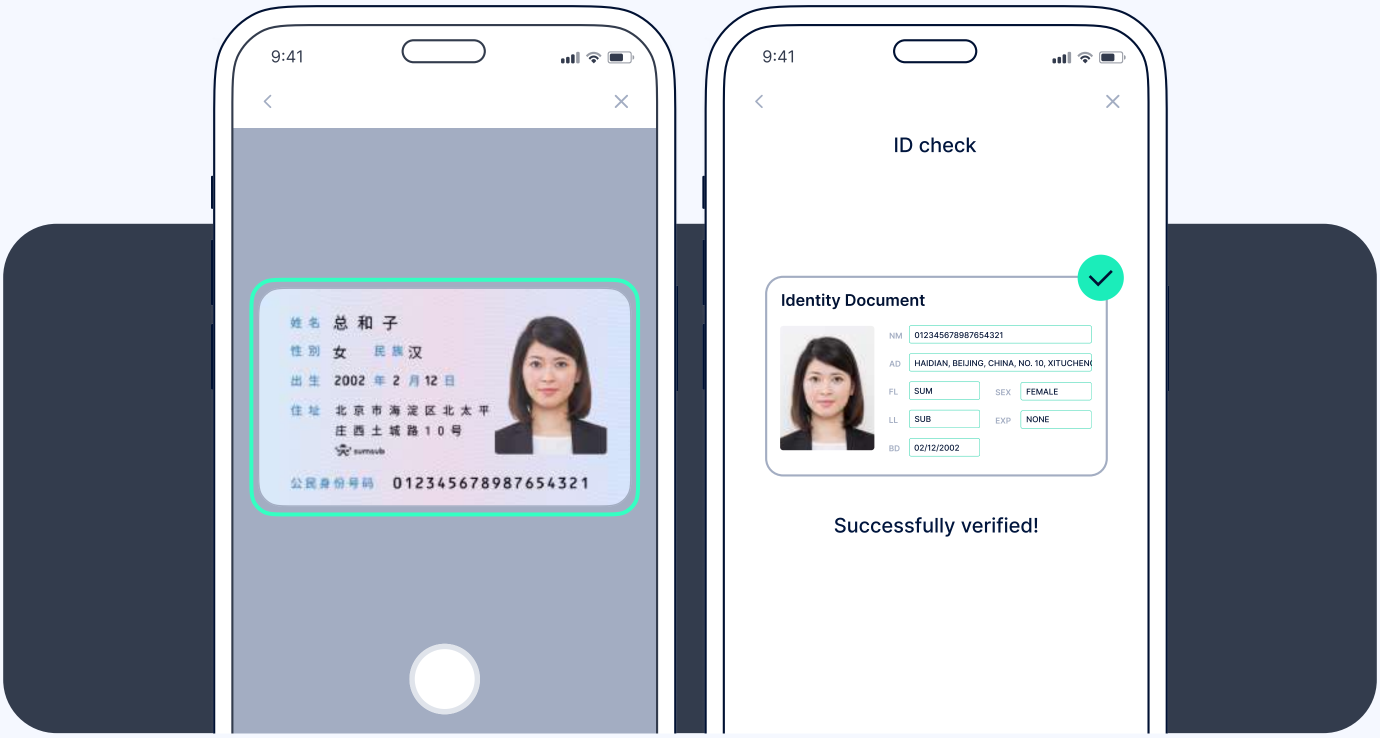


Image integrity check

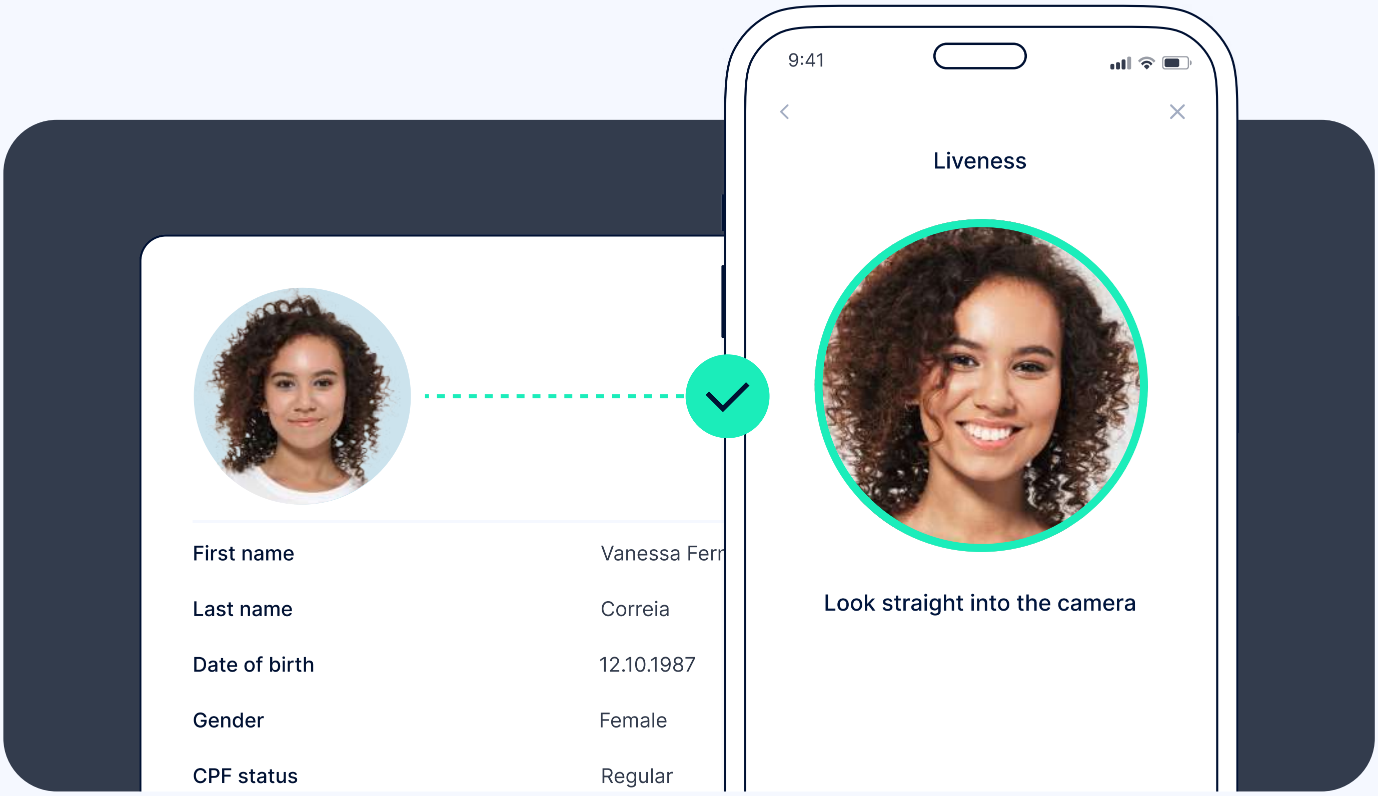
Document data validation

Sumsub also validates ID documents through reliable sources. This means that we use external databases to double-check that the document is authentic. This option is not available everywhere, but many countries are covered, and the list keeps growing.



Liveness and Face Match

Sumsub's Liveness and Deepfake Detection technology provides robust verification measures. Our technology ensures that applicants are real individuals, preventing the use of deepfakes, paper masks, photos, dolls, or similar fraudulent methods. Moreover, it verifies the authenticity of the provided documents by matching the applicant's face with the image on the document. This comprehensive process helps detect and prevent the creation of duplicate accounts.

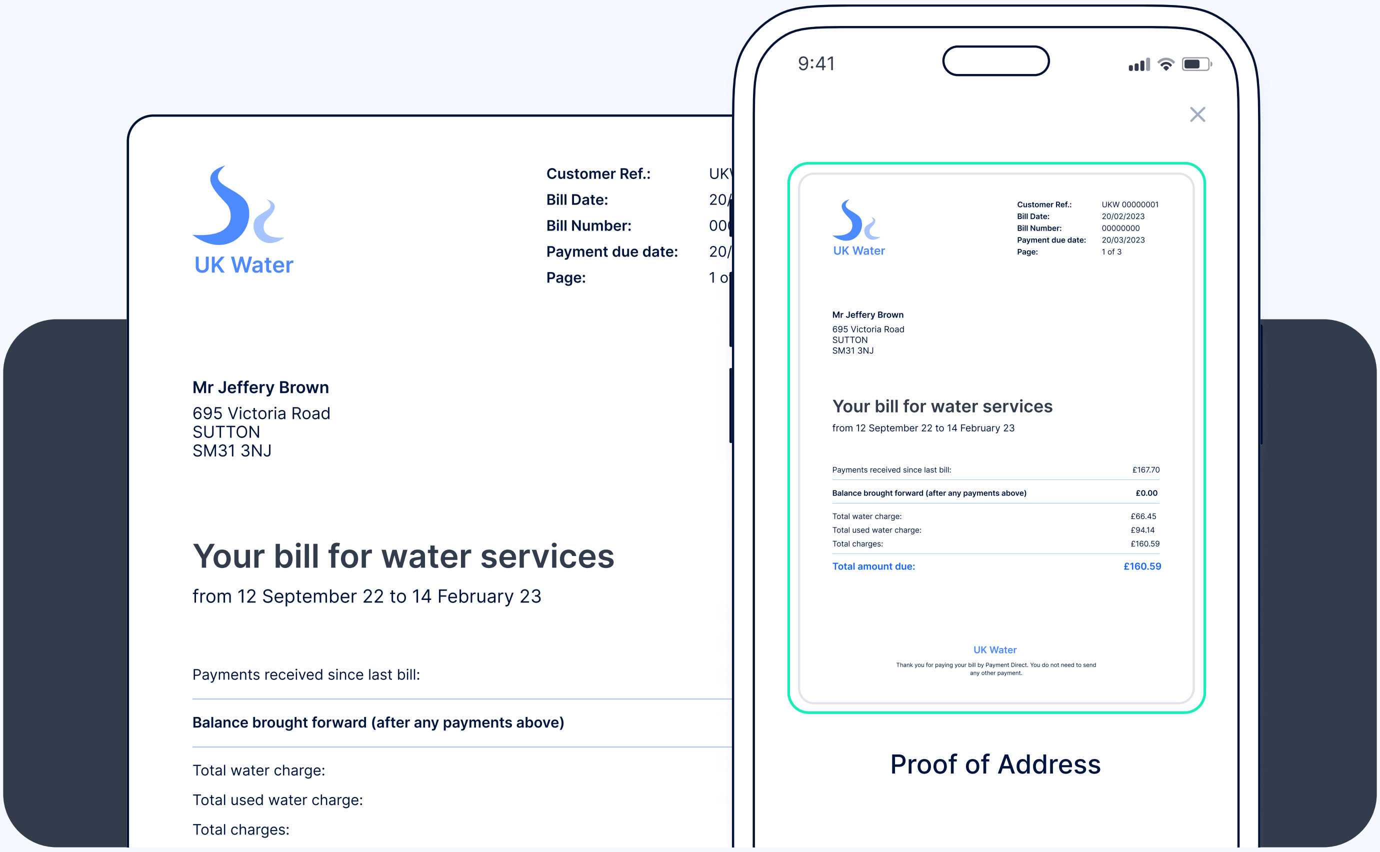


We can also help you with additional methods of verification if the AML regime of a certain country requires more than our standard Liveness process. For example, alternative methods like verification via videoconferencing with a trained operator can be applied when necessary.

Address verification

By default, Sumsub accepts PoA documents issued within the last three months and the acceptable issue dates can be further customized based on your verification needs. These are cross-validated against the provided proof of identity.

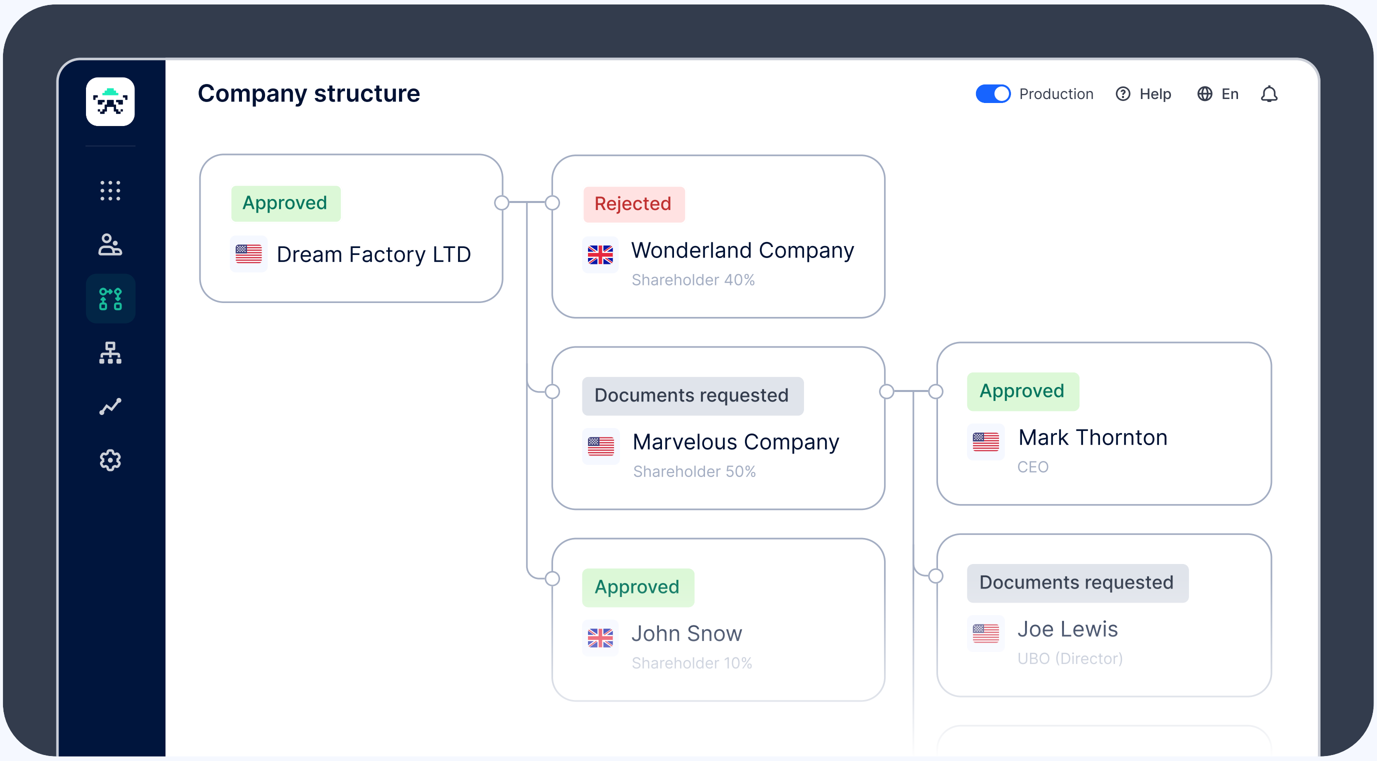
Sumsub's average PoA verification time is 59 seconds



As an alternative, the address can also be verified via the user's geolocation or using a government database. Supporting documents can be provided just as easily in the same flow if needed.

Business verification: Know Your Business (KYB)

Business verification is a due diligence process aimed at determining a company's structure, ownership, purpose, and activity. It allows companies to verify the legitimacy of the entities they are interacting with to prevent any illegal concealment of ownership.



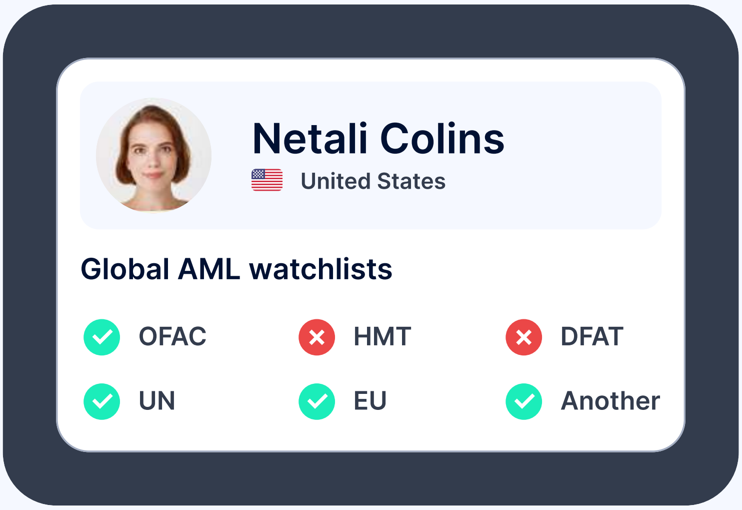
KYB verification is crucial throughout the entire company hierarchy. It can directly affect the Ultimate Beneficial Owner (UBO) because they are the ones who are legally responsible for owning and controlling customer and business transactions.

Sumsub integrates both automated and semi-manual KYB and KYC processes into a single workflow, streamlining company verification and AML screening. The full business verification flow involves human oversight from Sumsub’s compliance experts, who thoroughly review all submitted documents and perform necessary registry checks.

AML and Sanctions Screening

AML and sanction screening checks customers using multiple types of sources (sanctions, watchlists, and PEPs lists, etc.) to ensure they're absent from sanctions lists, not involved in money laundering/financial crime, and generally trustworthy. To optimize the screening process, companies use automated AML screening and scoring solutions to decrease manual workload and speed up user checks.

High-risk clients are easily detected with AML screening, while they are continually checked against global watchlists, sanctions, PEPs, and adverse media.



You can use AML Screening and ongoing monitoring for the following:

- Detect and restrict persons on sanctions and watchlists
- Pay attention to politically exposed persons (PEPs)
- Analyze adverse media

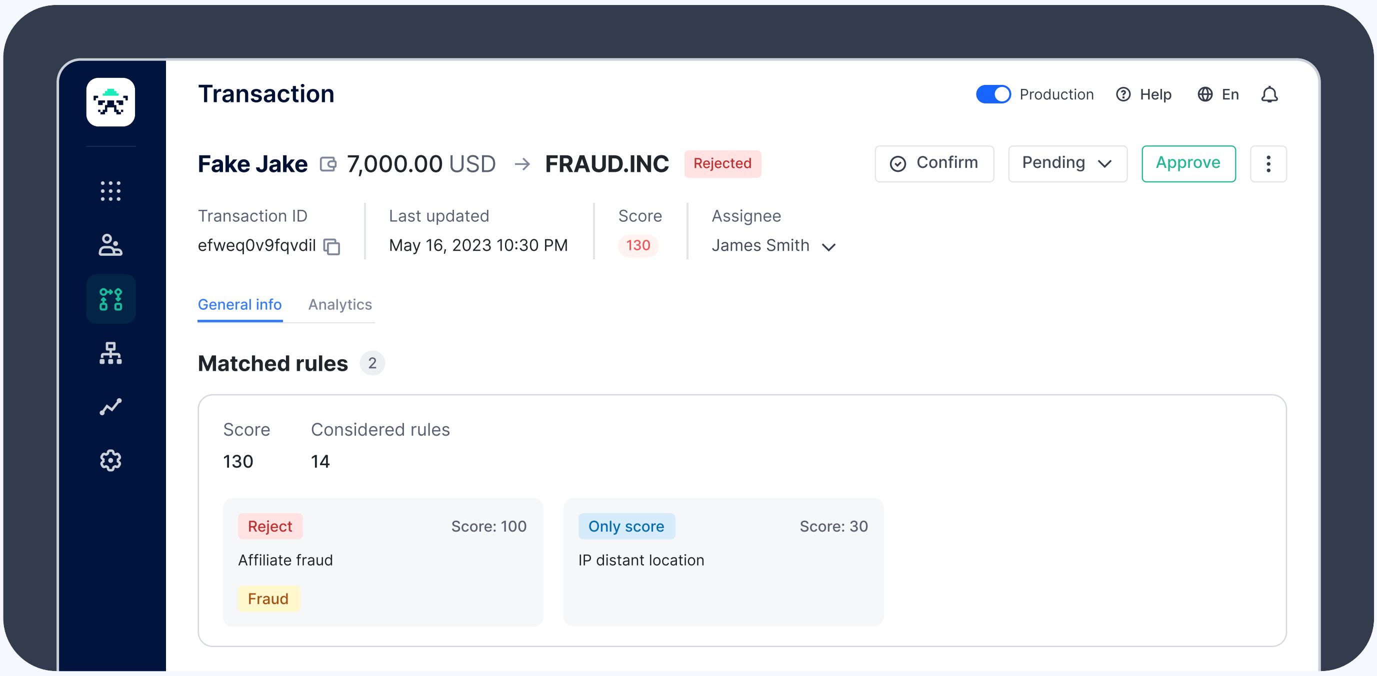
Monitoring

Transaction Monitoring

Under the applicable AML/CFT legislation, obligated entities must conduct transaction monitoring to determine whether the transactions are complex or unusually large. Other flags can be raised if there is an unusual pattern of transactions, or when transactions have no apparent economic or legal purpose, or in any case that may present a risk of money laundering or terrorist financing. Obligated entities must report all suspicious transactions and activity to competent authorities.

Businesses that do not adhere to the requirements risk regulatory penalties and fines.

The Sumsub Transaction Monitoring solution allows you to see detailed information for each transaction, report the transaction if necessary, and prevent fraud-related losses by detecting suspicious activities.



Transaction Monitoring for Fintechs

Fintech, Banking, or Payments

- Reduced false positive cases
- Improved team efficiency
- Risky users and transactions flagged
- Controlled transaction limits
- AML compliance
- Payment/chargeback fraud prevention
- Balanced onboarding speed and fraud protection

By utilizing customer onboarding data and taking a risk-based approach, banks can automatically detect signs of suspicious activity, such as income drastically higher than in the source of funds statement.

For more information, please refer to our "Complete Guide to Transaction Monitoring", where Sumsub and Pismo's experts cover industry-leading examples of Transaction Monitoring in action.

Ongoing Monitoring: AML and Sanctions Monitoring

Ongoing monitoring is crucial to AML (Anti-Money Laundering) and sanctions compliance in the Fintech industry. It is pivotal in identifying and mitigating potential risks associated with Politically Exposed Persons (PEPs) and High-Risk Individuals or Organizations (HIOs) within the system. Plus, it is essential to continuously evaluate the user's PEP status, as changes may occur after the onboarding process. By implementing effective ongoing AML screening measures, Fintech companies can proactively identify hidden risks and take the necessary actions to maintain a secure and compliant environment.

Case studies: verification results achieved with Sumsub

Flexibility, in-house technology, and a strong compliance background allow Sumsub to reach the highest verification results worldwide.

Jeton

50% increase in pass rates with Sumsub

- 71% pass rates
- 50% increase in pass rates in Asia
- 1 min 15 sec medium processing time

Learn more →

ANNA

95% reduction in manual work after switching to Sumsub

- 88% average pass rates
- 95% manual work reduced
- 1 min onboarding time

Learn more →

bitwallet

92% pass rates achieved with Sumsub's Optical Character Recognition

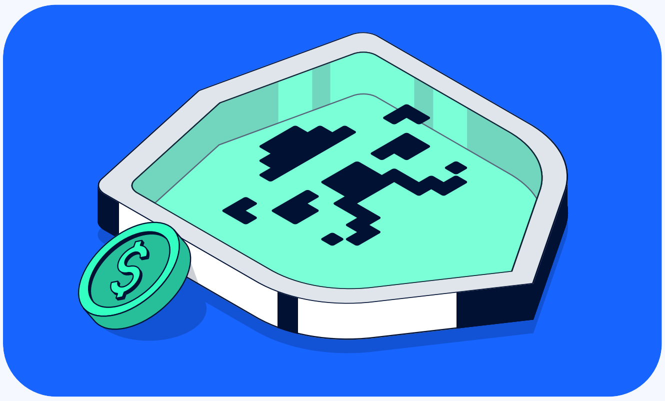
- 84.5% average industry pass rates
- 92% pass rates
- 2 min 50 sec median processing time

Learn more →

Summary

As you can see, Fintechs and regulations have a complicated relationship.

On one side, Fintechs working in regulated industries may face regulatory constraints that create challenges. In contrast, regulatory organizations are adept at gaining the public's trust, which is crucial for providing financial services.



The main point is that regulatory frameworks encourage Fintech firms to innovate in rapidly changing environments. Regulatory laws themselves can fortify business models, and the scrutiny gained from Fintech sandboxes can incentivize firms to meet and exceed expected global standards.

To reach these high standards, it is essential that Fintechs partner with a full-cycle verification platform.

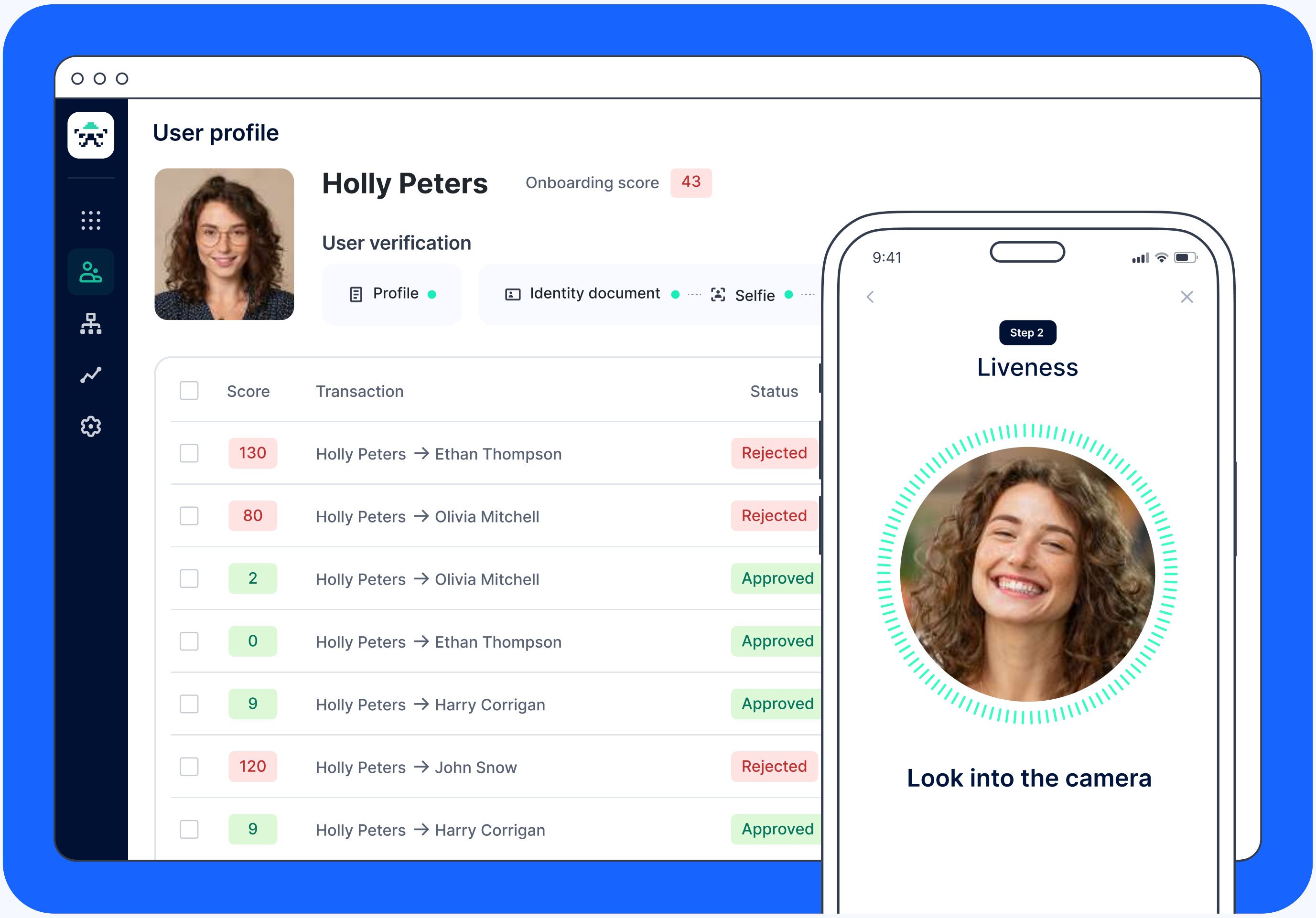
Over 70%

of fraudulent behavior occurs after onboarding, requiring an equally sophisticated KYC/ AML and Transaction Monitoring solution.

About Sumsub

All Fintech companies must discover how to avoid the flawed processes that allow fraudsters to capitalize on generic KYC/AML and transaction monitoring.

Sumsub offers you the solution to preventing fraud while optimizing your pass rates, with one platform to secure the entire user journey.



We have vast experience working with Fintech companies and certified compliance experts who can help you ensure regulatory compliance.