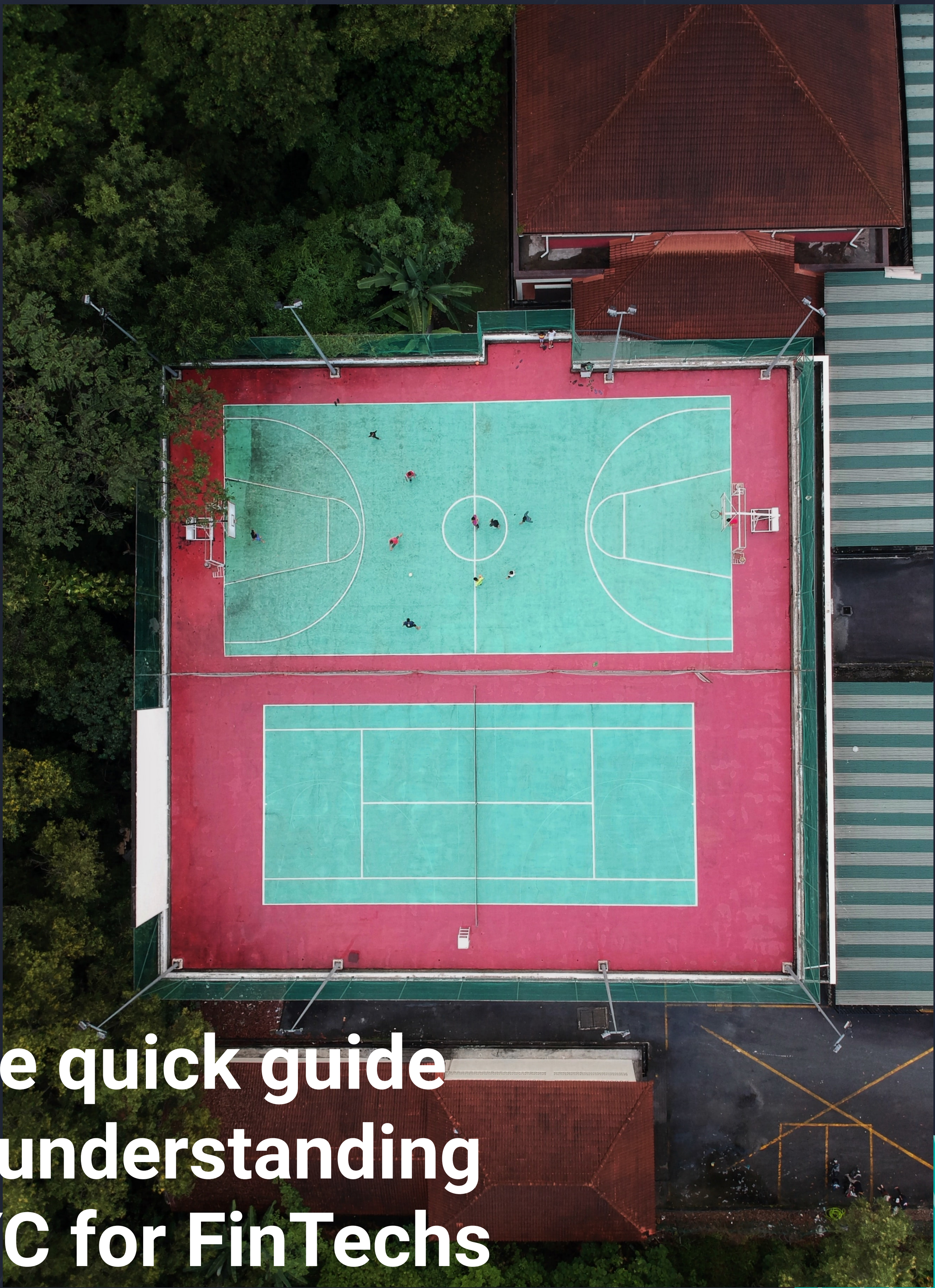
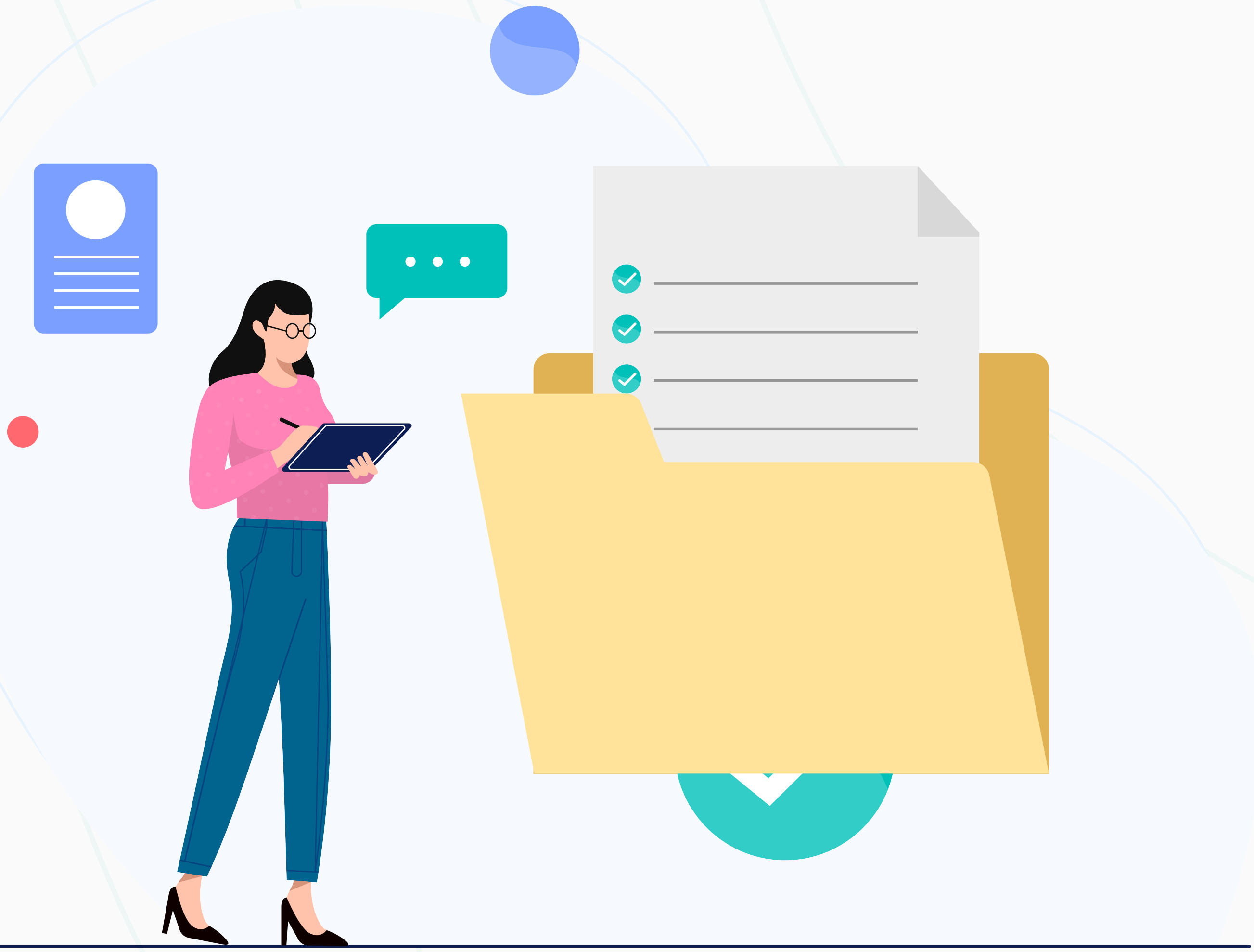


The quick guide to understanding KYC for FinTechs around the world

How to comply and scale quickly to other countries by understanding local regulations.

mati

Table of Content



Introduction

Do you remember the movie "Catch me if you can"? And yes, I'm referring to the one where Leonardo Dicaprio keeps switching identities and tricks everyone into thinking he is a pilot, a detective, a doctor, and a lawyer, all the while he's cashing forged checks for thousands of dollars around different financial institutions throughout the U.S. And do you know what's even crazier than this plot?

Well, this movie is actually based on a true-life story. Frank Abagnale is not only the name of Leo's character but also a real person who got away with all of this in the 1960s. This obviously would be very difficult even to attempt today, and one of the most important reasons for that is KYC.

If you've downloaded this white paper, you're probably aware that KYC stands for **Know Your Customer**, and actually refers to a set of procedures and processes that a company employs to confirm the identity of its customers.

To put it simply: verify a customer is who he says he is. These procedures are, most of the time, the first step of a larger framework - AML regulations - for **Anti Money Laundering** policies, which generally include 3 types of obligations:

- Verifying customers identity
- Monitoring their accounts
- Managing their risk factors

KYC is probably the most important step in an institution's AML policy, not only because it helps to keep customers protected and satisfied and reduces risk on a given platform, but also because, well, it's the law in most countries - at least if you're operating in financial services.

KYC and AML policies were indeed initially built for the financial industry, which is very logical if you consider that their first goals as regulation is to fight money laundering as well as financing of terrorism. If you want to discover what the link between Pablo Escobar, 9/11 and the obligation you have today of asking for your customer's ID at onboarding is, then you should head straight into **chapter 1.**

The purpose of this white paper is not to give you a history lesson on KYC and AML though; it's to solve the issues and questions you may have today. How do we know that? Well, basically, we've spent the last 3 years working with FinTech customers in different countries, to help them comply with local and international KYC / AML regulations.

And the funny thing about it is that no matter the country, the type of business, or the job title of our interlocutor, the same question always comes back: **what the heck am I supposed to do to comply?** KYC and AML regulations can appear quite mysterious, especially when you don't have a strong background in legal or compliance.

And frankly, this is often the case - even in our clients' portfolio. To be fair, a Head of Compliance is not usually the first person you're thinking about hiring when you're launching your neobank or scaling your lending company to other countries.

If that's your case, then this white paper is made for you! Our goal here is to give you a good understanding of general KYC and AML policies and to go a bit deeper into different countries to help you understand **what you're supposed to do to become or remain compliant** in the countries where you operate today. Our second goal today is also to give you **some tips** on how other companies are doing it, and where to start if you don't have a dedicated process to ensure KYC compliance internally yet.

Ready to dig in? We hope you'll enjoy the ride!

CHAPTER 1

Understanding KYC and AML - a quick historical focus

Okay, for this chapter, I'm going to suggest you put on your favorite jazz music, pour yourself a glass of your favorite red wine, and if you have a fireplace, light it up and get ready to be seduced by the sexy world of compliance. Just kidding, compliance might not be that sexy, but it's definitely important, and now that I have your full attention, I'm going to teach you once and for all what AML and KYC are.

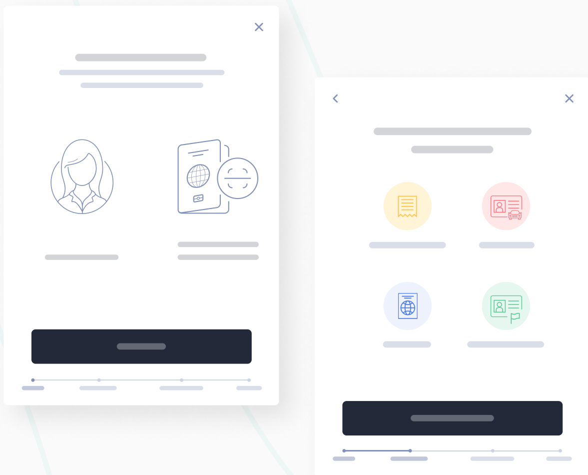
Let's begin with **AML:** AML stands for Anti-Money-Laundering. Money laundering is the process (crime) of making "dirty money" look "clean," and it occurs when funds from illegal activities such as drug dealing, terrorist funding, prostitution, human trafficking, among others are integrated into the financial system to make it appear as though they belong to legitimate sources.

Anti money laundering refers to the entire set of rules, laws, and regulations that are designed to prevent money laundering crimes. Most developed countries have laws or a set of regulations in place against money laundering and terrorist financing - however, **the enforcement of these laws really happened in the US only after 9/11.**

Okay, but how is AML related to KYC?

Well, complete AML compliance includes KYC, and as we described it in our introduction, it is probably the most important step. Not only because it helps keep customers protected and satisfied and reduces risks on a given platform, but also because, well, it's the law in most countries.

KYC (for Know Your Customer), on the other hand, refers to a set of procedures and processes that a company employs to confirm the identity of its user or customer. The robustness of KYC procedures varies across companies and jurisdictions. However, KYC fundamentally involves the collection and verification of a customer's means of identification — including government-issued identity cards, phone numbers, a physical address, an email address and a utility bill, to name a few.



From historical money laundering scheme to modern KYC regulations

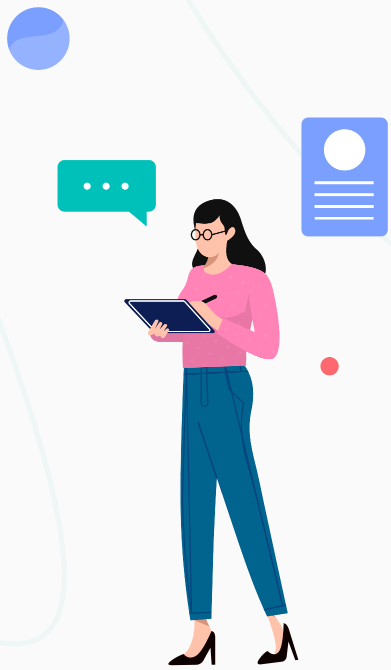
Now, these regulations didn't just happen out of the blue: they are the product of many years of money laundering, identity theft, and terrorist funding. So before we go in-depth as to how KYC works globally, it'd be wise to look at how it began.

We won't go back 2000 years ago in Ancient China, where according to some historians, the first money-laundering schemes ever registered in the history of humanity occurred [1] - neither will we go back to the 1920s in the US, where Al Capone invented quite successfully, modern money-laundering practices. Nope, we'll go straight to the 1950's, because this is **when modern KYC was invented**. And of course, it was in the USA, notoriously famous for fighting corruption and gangsters like Mickey Cohen, aka The King of Los Angeles. Familiar with the name? Well, that's expected - both L.A Confidential and Gangster Squad movies, (the second starring Sean Penn in the role) are based on this extraordinary character.

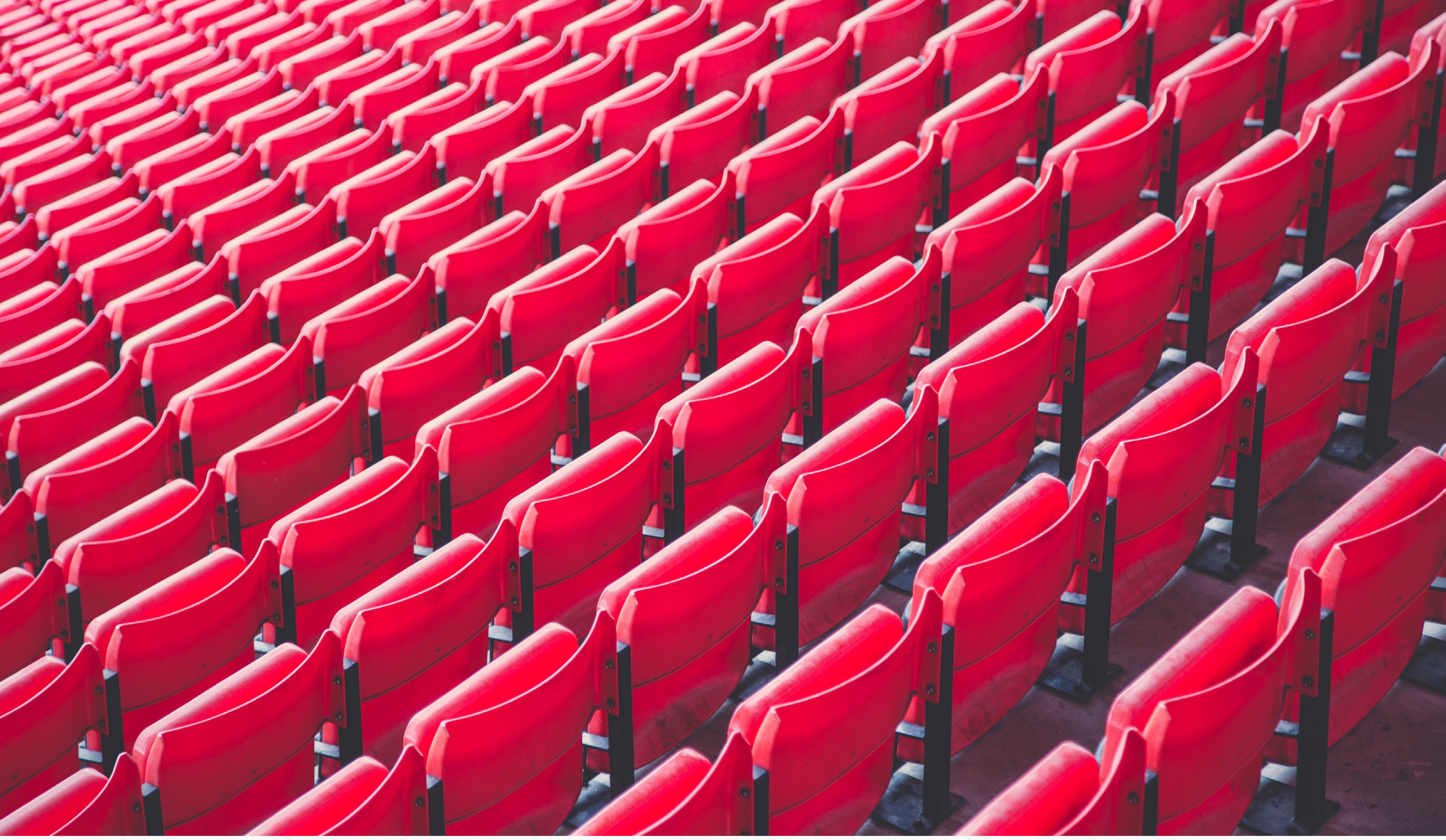
Now that I've successfully brought up the name "Sean Pean" in a white paper on KYC, let's go back to the history: those first regulations included a list of rules that financial institutions must comply with to remain insured by the Federal Deposit Insurance Corporation (FDIC) which is a type of insurance all banks that store customer's money must have to avoid tax evasion.

This formed the very foundation of modern KYC laws. In the 1960s, **AML regulations arrived on the scene** and were tied with KYC regulations from the 1950s. In the 1980s and 1990s, Pablo Escobar was being all too successful smuggling cocaine into the U.S., fuelling the 'crack epidemic' and draining a chunk of the country's wealth into Colombia. The Money Laundering Control Act, The Anti-Drug Abuse Act, and the Financial Crimes Enforcement Network (FinCEN) came into effect in the U.S. as part of the effort to fight these Escobar-like, increasingly sophisticated money laundering schemes and structures.

Throughout this time, KYC regulations were really just aimed at preventing money laundering and tax evasion stemming from drug trafficking and smuggling, but all that changed in 2001. Following the events of 9/11, the U.S. federal government passed the U.S Patriot Act, in which combating **terrorism financing** was added to the scope of the regulations as one of its primary missions, making KYC a global concept.



[1] Historian Sterling Seagrave has written that more than 2000 years ago, the wealthy Chinese merchants laundered their profits because the regional governments banned many forms of commercial trading. [Source.]



Making KYC global

Following 9/11, most countries in the world decided to impose similar regulations to control the money transiting via financial institutions. In Europe, the third EU Directive was released with a strong focus on KYC. Regulated entities were obliged **to increase due diligence checks** on their customers and the accounts they may hold.

South Africa followed in 2001, India in 2002, Japan in 2003, New Zealand in 2009, etc. Currently, almost every country in the world is applying some sort of AML regulation. And what they have in common is that they all enforce the necessity to conduct KYC procedures.

In terms of KYC, the common approach, worldwide, is to start your process by simply **collecting basic data** about their customers, through manual or digital identity verification. Information such as full names, social security numbers, birthdays, and addresses can be very useful when determining whether or not an individual is involved in financial crime.

Once this information is collected, financial institutions traditionally compare it to blacklists, watchlists, and lists of Politically Exposed Persons, aka PEPs. From there, the institution defines how much of a risk-factor their client appears to be, and how likely they are to engage in illegal activities. The company will then plan what the account of that customer will look like in the near future. Once the planned account course has been identified, the institution can monitor the client's account activity regularly to ensure that nothing looks suspicious.

As you can see, KYC was first used exclusively by banks and financial institutions for AML purposes. But over the years, it has become more and more popular since it turned out to be super effective in 2 other areas: **reducing fraud and reducing incidents.** It has also proven to be useful for sharing economy platforms: you're more likely to be a model Uber passenger if they have access to the ID you submitted when registering, right?

The rise of FinTechs and its impact on regulations

The extension of KYC procedures to other industries is interesting, for sure - it's the best demonstration that a tool initially designed for regulatory purposes can become **a tool for business**. But the panorama here wouldn't be complete without mentioning the biggest revolution in financial services since the democratization of the internet - and by that, I mean obviously the explosion of the FinTech industry, starting in 2008.[2]

What happens when hordes of startups are created by people that don't belong to the traditional industry, and are using disruptive technologies and models governments don't understand yet? Well, governments start to freak out - and they need to pass some processes pretty quickly to ensure this new type of activity is not in a **legal loophole.**

Majority of countries solved this by making sure FinTechs are regulated as regular financial services, meaning these companies need to verify that their clients:

- Are who they claim to be;
- Are accepted as customers of the product or platform in the first place;
- Fulfill the requirements to use the service;
- Do not misuse the product or platform to commit a crime.

As financial institutions, FinTechs face risks of fines or an abrupt stop to their services if these procedures are not respected.

[2] "How did the FinTech Industry come about?" by Jay Tikam. Vedanvi Blog. November 2015. Source.

FOCUS ON
SANDBOXES

Some countries have taken matters a step further by implementing regulatory sandboxes, which are platforms issued by local regulatory agencies in order to provide a space for companies that want to experiment with new business models and do not have a legal framework in place at the time. Their main goal is to facilitate viable projects with their arrival at the market.

The United Kingdom was the first country to introduce and put one into operations in 2014, but other countries soon followed, like Australia, Canada-Ontario, Malaysia. Hong Kong, Switzerland, Dubai, Russia, Indonesia, Singapore, Taiwan, Thailand, Uk, Norway and Spain. Be on the lookout for more countries joining the list though, such as the US: Arizona launched a sandbox earlier in 2019 and now there's talk of a federal sandbox on the way.

When it comes to regulations though, there's one country that is clearly ahead of the curve: Mexico. It is indeed one of the only countries in the world that has an actual FinTech law, passed in 2018.

This law and its implication on the local FinTech ecosystem are as such under scrutiny: for a lot of countries, this is a good occasion to examine the pro and cons of specific FinTech regulations (read more in chapter 4).

Conclusion

As you've seen, KYC regulations are a complex subject. Depending on your country or your industry, it won't have the same impact on your business. Now is time to dive deep: next chapters explore how these regulations apply specifically in different countries, from the US, to Europe, to Latam & Asia.

We'll break them down for you, so you get a better sense of what you're up against when trying to comply globally.

CHAPTER 2

Focus on the USA

As you read above in our brief history lesson, the US was the founder of modern KYC regulations. Now, it is true that they began in an effort to fight money derived from drugs from being laundered and placed back into the economy- but completely evolved into what they are today after the terrorist acts of 9/11. As founding fathers as the United States are, they have lagged in terms of FinTech regulations and watched while other countries take the lead in this area. However, the USA remains as the first ecosystem for FinTechs in the world: understanding the regulations that apply is a necessity if you're planning to start or expand your business here.

A regulatory framework ruled by the U.S. Patriot Act

The **U.S. Patriot Act of 2001** introduced KYC regulations after 9/11 and made KYC mandatory for all banks in the United States. The Patriot Act first defined KYC requirements and led to the development of a version that most countries apply today. It also requires financial institutions to comply **with tougher AML and KYC,** including the Customer Identification Program (CIP) Customer Due Diligence (CDD), as well as Enhanced Due Diligence (EDD), for the collection of additional CDD information about a customer. Typically, you'd conduct EDD for higher-risk customers to get a better understanding of their business activity.

FOCUS ON CIP

The Customer Identification Program (CIP) was introduced to combat money laundering, terrorism funding, corruption, and other illegal activities. Its main goal is to verify that your customers are who they say they are. It requires that any person handling financial transactions verifies themself. Financial institutions such as FinTechs use CIP to identify individuals that want to conduct transactions with them.

FOCUS ON CDD

The Patriot Act requires banks or businesses to file reports of suspicious activity when they notice unusual or illegal behaviors. But without knowing its customers, companies are not able to meet these criteria. To achieve KYC compliance in the U.S., you may need CDD. It is a component of risk management and the protection of your company. When you implement CDD, you must monitor and understand your customers' activities. Then, you can use the information you find to evaluate how risky they are for your business.

That's a lot to digest, right? Well, bad news... there's more!
Let's not forget, the Bank Secrecy Act (BSA) which requires banks and financial institutions to file 5 types of reports with the Financial Crimes Enforcement Network (FinCEN) and the Treasury Department, the American authorities regulating AML policies for all financial institutions:

1. **Suspicious Activity Reports (SAR)** for suspicious cash transactions.

2. **Foreign Bank Account Report (FBAR)** for any U.S. citizen or resident that owns at least $10,000 in a foreign bank account.

3. **Currency and Monetary Instrument Report (CMIR)** to report a person or institution that physically transports monetary instruments (cashier's checks, traveler's checks, and money orders) of $10,000 or more into or outside of the U.S.

4. **Currency Transaction Report (CTR)** for cash transactions that exceed $10,000 in one business day.

5. **Monetary Instrument Log (MIL)** for banks to keep a record of all cash purchases (e.g., money orders, cashier's checks, traveler's checks) for $3,000 and $10,000.

Remember we talked about FinCEN before? Here's some more: as of 2016, the new FinCEN rule requires all banks and financial institutions to collect basic data such as name, date of birth, address, and Social Security number of people who own 25% or more of an equity interest in a legal entity. Phew, that's definitely a lot of entities and regulations 😨

However, take comfort in the fact that regulations can be made pretty easy to follow with the right solutions in place, given KYC processes are very similar for any business:

- **First,** you need to make sure you can verify a customer's identity (preferably through an electronic Identity Verification Service);

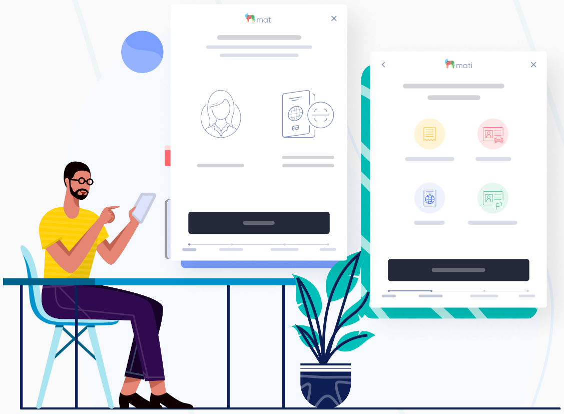
- **Second,** prove that you're managing the risk factors;

- **And third,** that you're able to monitor their accounts in order to create risk profiles and report activity that falls outside of "regular" use.

KYC Obligations for Fintech

In the USA, the minimum requirements to open an individual financial account are to provide:

- **Name**
- **Date of birth**
- **Address**
- **Identification number**



$259,955

According to a study by cloudtask, this is what an in house a team of 4 in the US dedicated to manual verifications could cost you. Digital ID verification processes can reduce that cost by more than 50%: as you can see, verifying people faster is not the only quality of digital or electronic ID verification!

While recollection of this data at onboarding is enough to legally comply, American authorities also recommend that, for extra security, the institution should also verify the **identity of the customer** through documentation, public databases, etc... Typically, financial institutions tend to examine official government issued IDs which include a picture and nationality, and cross reference it to public records. When done manually, with an internal or external team, you're looking at a 3-business-day process. However, there are other methods that are much more convenient and reliable such as **electronic Identity verification**, which crosschecks ID documents electronically with the identity information, to further reduce the risk of fraud.

Conclusion

As you can see, KYC compliance for Fintechs is no different than for other financial institutions in the U.S. And even if the number of stakeholders or regulators here can be a bit scary, let's not forget that KYC is not only a way to comply but also to protect your business.

CRYPTO USA

Complying with US regulations when operating a crypto trading service: Beaxy's case study

About

Beaxy is a cryptocurrency exchange platform created in 2017 in the USA, that quickly expanded to other countries. Beaxy's mission is to revolutionize crypto exchanges by bringing all of the tools and technologies that traders in traditional markets use on a regular basis to the cryptocurrency space for the first time.

The issue

According to its founders, Beaxy differentiates itself with two core values: being the first exchange to offer top tier trading tools applied to the crypto industry, and **being strong on KYC/AML checks**. On that matter, the issue for them was to find the right identity partner and to turn it into a **competitive advantage**, while being able to open the exchange to new countries super quickly.

What does Beaxy verify?

In terms of KYC/AML, after signing up, users have access to Beaxy's mock exchange, where they can discover all features. But as soon as they want to exit the sandbox and trade for real, they need **to get verified**. It's a simple 20 seconds process where they upload their ID and a selfie.

> "Thanks to Mati, we could become completely KYC / AML compliant within a few weeks. I remember before Mati, we had these endless discussions about how to comply with SEC, Fincen, or even CFTC regulations as they arise. Mati helped us solve that for good."

Nick Murphy
Executive VP Operations @ Beaxy

Read Case Study

CHAPTER 3

Focus on Europe

European FinTech companies have created over 2x more value since 2013, than any tech sector in Europe. Fintech is Europe's largest venture capital investment category: over the last years, the sector has received 20% of all venture capital in Europe[3]- which is a higher percentage than in Asia & USA. With great power however comes great responsibility, and fighting schemes has also become part of the daily agenda. Money laundering & tax evasion are one of the biggest threats to the financial system in Europe. In order to avoid such impacts, the EU has been promoting targeted regulations in the last 10 years to reduce this risk. Let's take a deeper look into how these targeted regulations can impact your business.

Meet your new best friends, AMLD & PSD2

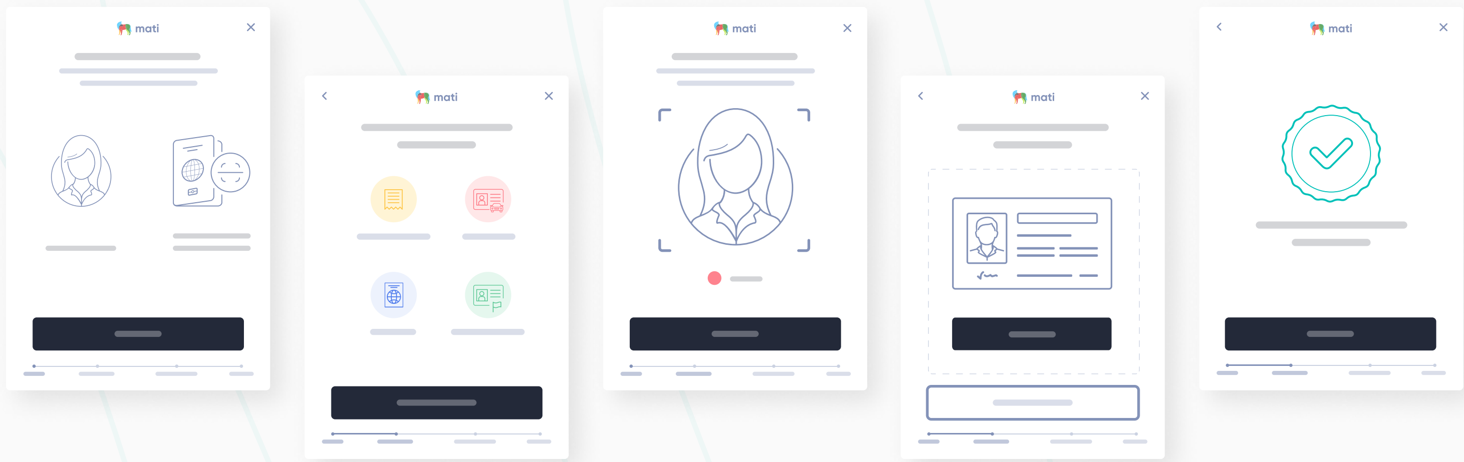
AMLD & PSD2 are two clunky acronyms representing two critical directives that impact everyone running a FinTech. They stand for Anti Money Laundering Directives (AMLD) and Second Payment Service Directive (PSD2).

The AMLD is a set of regulatory requirements issued by the EU containing rules **to fight money laundering and terrorist financing** by EU member states. Its main goal is to protect the financial system by enforcing procedures for prevention, detection, and investigation of money laundering and terrorist financing. AMLD is suitable for credit and financial institutions, certain legal professionals such as auditors, notaries, trust or company service providers, people trading in goods for payments made or received in cash totaling the amount of €10,000 or more, and gambling service providers.

PSD2 is the second Payment Services Directive, designed by the EU to revolutionize the payments industry, influencing the way we pay online as well as the information we see when completing a payment. PSD2 will also require stronger identity checks such as KYC, especially when dealing with higher transactions.

So how exactly is KYC carried out for Fintechs in Europe?

[3] "The State of European FinTech" by Finch Capital & Dealroom October 2009. Source.



KYC Obligations for FinTechs

There are several simple methods that can be implemented in which the user submits identity documents, which must be authenticated, and a picture or a video of their face (in some cases their fingertips), in addition to other biometric tests and security checks.

Not all KYC verifications comply with legal qualifications in Europe. For example, selfie-based identification solutions (meaning that you ask your user to submit a picture of their face to make sure it matches the photo on the ID) are not KYC/AML compliant in the EU. The latest version of AMLD, going under the name AMLD5 (yep, because it's the fifth edition) establishes that they have weak reliability and do not fit requirements demanded by legislation.

Good news is that AMLD5 introduced a new regulation last year called eIDAS (electronic Identification Authentication and trust services), that allows other recognized identification methods that provide security equal to physical presence, such as Liveness Recognition a.k.a proof of life.

Neobanks, lending companies, eCommerce, to name a few, are some of the industries that will now have to comply with KYC; as well as the uprising Cryptocurrencies exchanges which had a big impact on AMLD5 by stating that all EU member states must implement AML regulations when it comes to crypto. These exchanges will now be required to not only **follow KYC rules** but also to monitor customer transactions and file suspicious activity reports. That way, it will be ensured that they're legitimate and are not attempting to abuse the platform for malicious purposes.

Fintechs operating in the EU need to comply with basic KYC/AML regulations, which can be summed up in 3 steps:

- **Making sure your user provides an authentic document to verify their identity;**
- **Ensure it's the same person as the one on the document provided running a liveness check;**
- **Confirm users aren't listed on international anti-money laundering watchlists or blacklists.**

Focus on GDPR

GDPR stands for General Data Protection Regulation. It's a set of rules designed to give EU citizens more control over their personal data. Under the terms of GDPR, organisations have to ensure that personal data is gathered legally (not through a data breach for example) and it should also be protected from misuse and exploitation. Failure to do so can result in expensive penalty fees. Under GDPR regulations, financial institutions will have to follow a number of practices for storing and accessing data. But if KYC data is compromised due to improper handling, the penalties under GDPR can be very harsh.

This means that, among other steps, any institution with KYC data must:

- **Avoid storing data in the public cloud;**
- **Have BYOD (Bring Your Own Device) policies in place to protect against unauthorized storage of KYC data;**
- **Update IT security protocols in every area of the business to protect against liability;**
- **Ensure that third-party vendors and organizations meet GDPR requirements.**

Good news though is that automation is definitely a way to help GDPR compliance by reducing the risk of an employee compromising critical data :)

Conclusion

Although KYC regulations in Europe do vary a little from other places in the world, their main goal remains to prevent abuse by money laundering or other financial crime activities. Therefore, the regulatory requisites are rigorous, challenging, and compulsory for financial institutions. The good news for FinTechs though, is that unified European regulations make it easier for any company to scale across the region and open up in new countries - provided that you have a good KYC process.

CRYPTO EUROPE

Complying with European regulations when operating a crypto exchange platform: Bitclude's case study

About

BitClude is a cryptocurrency exchange platform created in 2017 in Poland by a team of blockchains developers. The mission of the company is to provide a worldwide service of exchanging currencies for all, equally and transparently. The company has been quickly expanding in the last two years, helping its users to buy or sell crypto in less than 5 minutes, through an integration with banking system platforms.

The issue

Immediately after they launched Bitclude in Europe, the biggest question for the founding team was about **how to become compliant**. According to them, any issue with regulators or fraud can kill your business in crypto, and **having a serious and legit identity provider is the smartest thing** to do when you deal with regulators in Europe. Bitclude was then looking for a solution that could make them compliant in the eyes of regulators in Europe, as well as making sure they didn't have fraud on their platform.

What does Bitclude verify?

After a new user signs up, he is prompted to start the verification flow. It consists of an official ID upload and a 5 seconds **liveness video.** Last time the team measured, on average users spent 19 seconds to finish the entire flow. Their backend receives then within seconds the user verification data, that consists of 9 KYC/AML checks. If all of them are green, the user is accepted. Otherwise, it is flagged as "manual review" on the Mati dashboard, and Bitclude's support team contacts the user.

> “In terms of guidance, Mati helped us understand and comply with all the regulators in Europe for KYC and AML in no time. We were so relieved once we got the approval, we were finally in business!”

Jakub Wierzcholski

CEO & Co-Founder @ Bitclude

Read Case Study

CHAPTER 4

Focus on Latam

When you hear Latin America, you probably think of warm people, good weather and beautiful beaches, and you're right: honestly, who wouldn't want some downtime here. But what if we told you, Latam is actually as exciting for work as it is for play. Latam is indeed the fastest-growing region in the world for the FinTech industry: In the last six years, FinTech funding has grown from less than $50M to over $2.1B, and even local governments are finally catching on, competing to attract more domestic and foreign investors through preferential regulatory treatments.

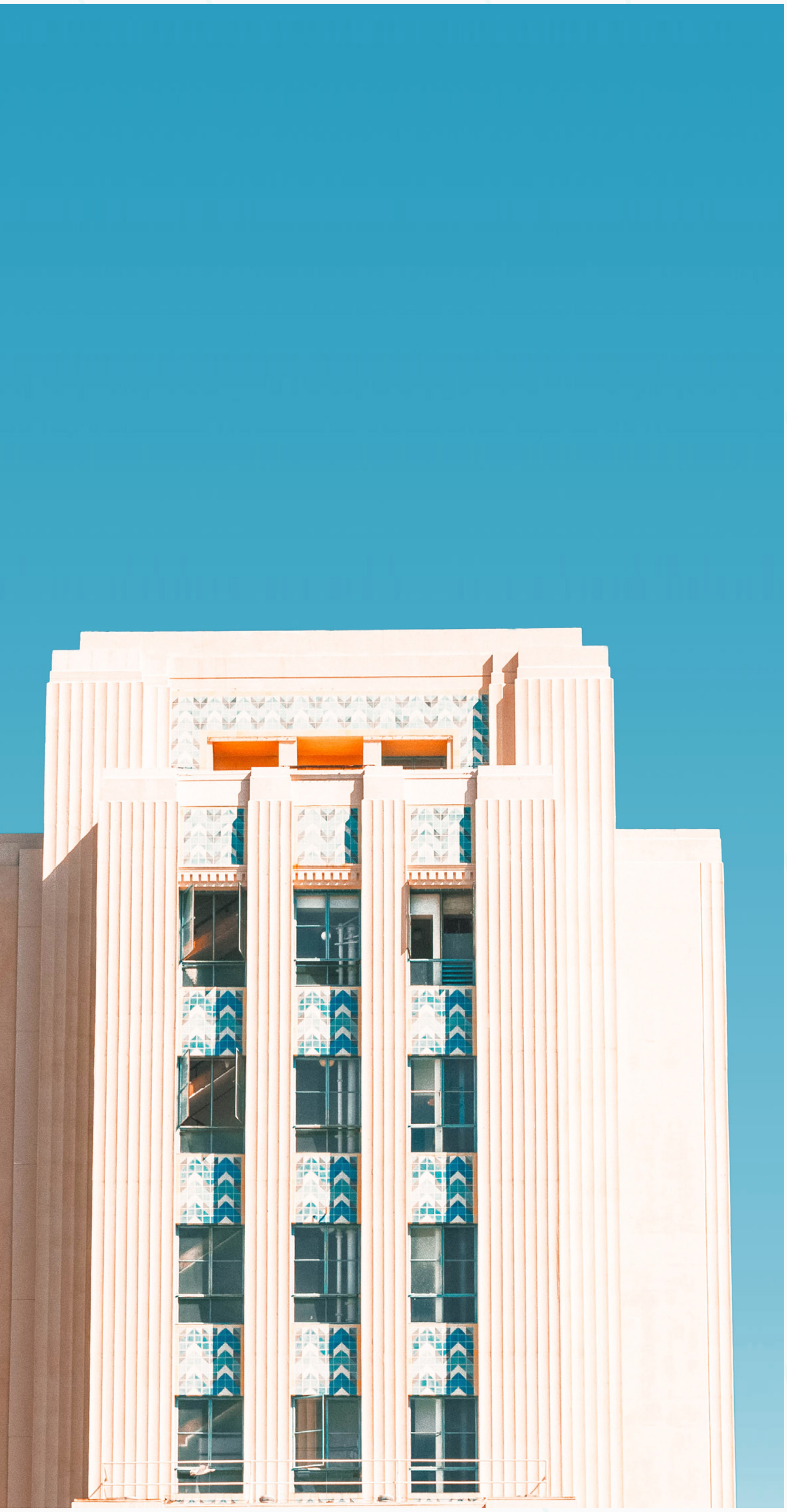
So what explains the FinTech boom? The reasons are numerous, from the penetration of mobile devices to the difficulty of opening traditional bank accounts for certain thin-file populations. Given these constraints and opportunities, it's a no brainer that the preferred companies of the Latam ecosystem are Neobanks and new lending businesses. **Together, they hold the promise to bring those neglected by traditional banking and lending services into mainstream finance.**

However, when you think of Latam, you also undeniably think of corruption and drug money (especially if you've devoured Narcos in confinement). This explains why local governments are being proactive in building regulatory frameworks to monitor and supervise this upcoming market. Because practice makes perfect, Latam has ironically become a beacon in the world in terms of FinTech regulations. Mexico is the definition of progress as a **true pioneer** in the field, being one of the only countries in the world and the first in Latam to implement sector-specific FinTech laws since March 2018.

Mexican FinTech laws regulate 3 main verticals: crowdfunding, crypto, and payment methods (which include Wallets and Neobanks). The laws are based on a few key principles, like financial inclusion and innovation, as well as the promotion of competition. The big boys here are the CNBV, which supervises and regulates Mexican financial entities, and Banco de Mexico (Banxico), which facilitates credit flows and injects liquidity into the Mexican financial system.

A complex patchwork of authorities and regulations

As for the other regions in Latam, let's look at how regulations are being handled at the moment:



Brazil: FinTechs are not regulated as an industry in Brazil. The highest regulation authority for FinTech is the Brazilian National Monetary Council. Financial services & activities fall under the regulatory scope of the Brazilian Central Bank. In recent months the Brazilian Central Bank has issued new money laundering regulations aimed at Fintechs, bringing them closer to their regulatory scope.

Argentina: As of today, there hasn't been any FinTech regulation approved in Argentina. Only certain specific aspects of the industry are regulated, such as equity crowdfunding and ICO's (Initial Coin Offering) but to a limited extent. However, FinTech companies do fall under the supervision of the Comisión Nacional de Valores (CNV).

Chile: Lawmakers in Chile are starting to look into regulations covering FinTech – including cryptocurrency firms, but as of now none of these are regulated. They are, however, required to set up a special corporation with one exclusive purpose and to register in the Financial Market Commission's Card Issuers Registry, in the case of wallets and other debit based solutions.

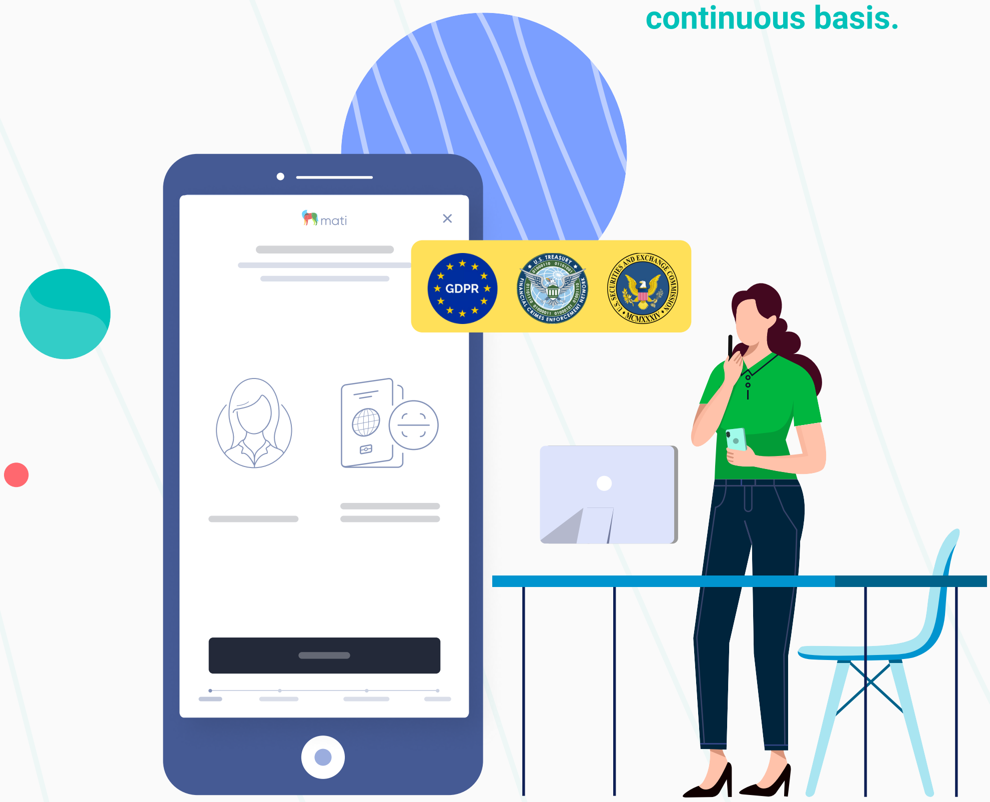
Colombia: There is no specific legislation or regulation addressing FinTech as a whole industry. However, the Colombian financial regulator addresses FinTech from an Anti-Money-Laundering (AML) perspective. Some drafts of a prospective Fintech regulation have started making the rounds in the Colombian parliament.

Alright, that's definitely a lot of moving parts- and this is also one of the issues for Latin American companies, or international players willing to set foot in this market: scaling a product from one country to another in Latam can be quite complex because of it.

KYC obligations for Fintechs

If you're building or scaling your operations in the region, a good rule of thumb to apply is using international standards (FATF guidelines) since they regularly exceed Latin American standards.

Nevertheless, based on experience and engagement with local authorities in Latam, we recommend that you cover your bases by ensuring that you **verify your customers' identity, manage their risk factors consistently and monitor their accounts on a continuous basis.**



Conclusion

In Mexico, these 3 steps are already foundational to operating as a FinTech. Chances are that Colombia, Brazil, Chile, and other Latam countries will adopt similar regulatory structures soon. You can't say we didn't warn you!

NEO BANK MEXICO

CUENCA

Complying with mexican regulations when operating a neobank: Cuenca’s case study

About

Cuenca is a Mexican neobank created in 2018. The ambition of its founder? Turning Cuenca into the only account people need in Mexico. The FinTech have since raised around 10M$ USD, is expanding its services and offers in Mexico and LatAm, and is one of our historical clients in Mexico.

The issue

Cuenca opens bank accounts for users from Mexico, as well as internationally, and is regulated by CNBV in Mexico. For them, **having the highest KYC/AML standard was a priority**: with the new screening regulations in Mexico, the risk of not being compliant is now so high that it could shut any company down in no time. Cuenca was also looking for an international partner, as the company was planning to **expand globally**. The CEO wanted to avoid at all costs to have country-based plans: for him, these plans are a pain to manage and cost a lot.

What does Cuenca verify?

To comply with Mexican regulations on neobanks, Cuenca asks its users during account creation to upload several things during the ID verification process: an **INE** (the Mexican national ID) and a few sec video of the user to perform a **Liveness check.** Cuenca also uses Mati to verify that the user is officially existing in **Mexican governmental database**, and is not registered on **Mexican watchlists** like PEP.

“I remember before Mati, we had these endless discussions about how to comply with user onboarding / account opening regulations in Latin America as we were starting operations in Mexico.”

Matin Tamizi

CEO and Co-founder @ Cuenca

Read Case Study

CHAPTER 5

Focus on the rest of the world

Mexico is not the only country that has taken firm steps in its commitment to promote and regulate the FinTech sector. An increasing number of regions are joining the trend to create regulatory sandboxes, in order to accelerate innovation in their business sectors, and turn themselves into international hubs. Among some of the most exciting areas are countries like Nigeria,Singapore, Hong Kong and Australia. Understanding what's happening in these places is key, not only if you operate there, but also to get a glimpse of big regulations trends for FinTechs.

Current FinTech regulations in Africa

Right now, Nigeria is currently Africa's Fintech capital and major place for digital start-ups. It's also one of the most exciting countries in the world in terms of FinTech ecosystem: in 2019, the country attracted Fintech investments worth US$400million.

Regulators haven't yet started to do what they do best, though: regulate. As of today there are no regulations applied specially for FinTechs in Africa, and most countries abide by existing local regimes. Some of them are experimenting with **regulatory Sandboxes** which allows them to observe and learn more about the Fintech space in a controlled environment, like South Africa.

As a matter of fact, an interesting phenomenon in Africa is that ID verification is mostly used to reduce fraud on financial services, not compliance. This is once again a good demonstration of how verifying your users is probably **the best way of protecting your business!**

Current FinTech regulations in Asia

Another place where FinTech has had an enormous impact is Asia. Given the ongoing fight for market shares in relation to start-ups and tech businesses in the area, jurisdictions are **increasingly focusing on regulatory requirements and initiatives** in an attempt to demonstrate how suitable they are to serve as a hub of innovation, but at the same time not allowing the climate to be too relaxed in terms of regulation and investor security. Let's discuss some regulatory entities by countries that FinTechs currently abide by in this region.

INDONESIA

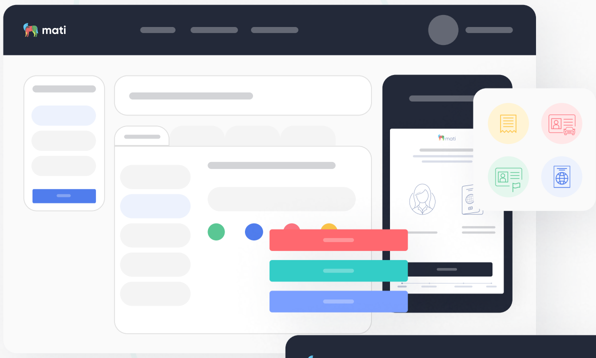
As of today the most established law for FinTechs would be The Bank of Indonesia (BI) introducing The National Payment Gateway (NPG) in 2017, in order to promote cashless transactions. Indonesia requires all of the cashless transactions made on the territory to be processed through NPG. This means that FinTechs wishing to operate in Indonesia have to connect to the NPG network.

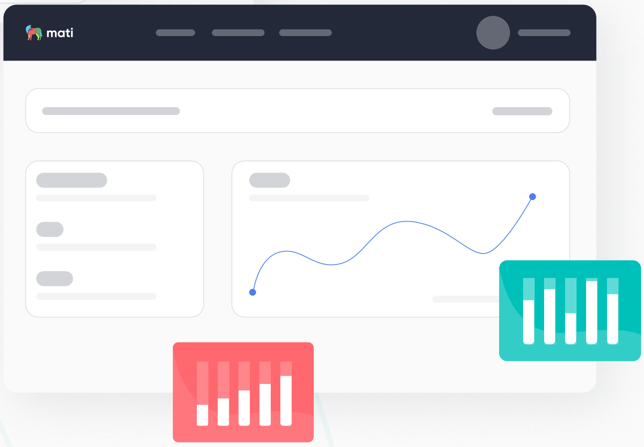
CHINA

China is a country that has definitely seen a lot of FinTech growth and therefore has created the People's Bank of China (PBoC) payment license that foreign-invested enterprises (FIEs) can qualify for. This license allows companies to issue and accept prepaid cards, offer online payments and collect funds.

The 5 requirements to qualify for the Payment License from the PBoC are:

- **First,** establish a Foreign-Funded Enterprise within the territory of the People's Republic of China.
- **Second,** having at least RMB100 million paid-in capital for nation-wide license or RMB30 million for operating within a particular province.
- **Third,** having an Anti Money Laundering (AML) procedure in place.
- **Fourth,** storing and processing all of the personal data acquired in China inside the territory of China.
- **Fifth,** complying with the supervision requirements of the People's Bank of China.





THAILAND
Thailand has also taken steps to ensure compliance in the FinTech sector. The Bank of Thailand (BoT) along with the Ministry of Finance (MoF) released the Payment Systems Act (PSA) which is aimed to ensure efficiency, and security of payment services as well as make the regulations in line with the international standards. All of the banks, neobanks, credit card, debit card or ATM card services, trading platforms, cryptocurrency wallets and other payment services must obtain this license.

SINGAPORE
Singapore is definitely one of the most advanced areas for FinTech in Asia. FinTechs here are required to sign up to the Singapore Fintech Association (SFA) as well as:

- **Notify users of all their e-payments.** This will allow users to monitor their transactions and promptly report unauthorized payments.
- **Inform users about possible liabilities** in case users decide to change their preferences and see less notifications.
- **Provide a reporting channel,** through which users should be able to report unauthorized transactions.
- **Assess and investigate the claim** while providing all reasonable effort to recover the money.

HONG KONG
The Hong Kong Monetary Authority (HKMA) created a Fintech Supervisory Sandbox (FSS) in September 2016. Fintech technologies covered by the FSS include mobile payment services, biometric authentication, blockchain, robotics and augmented reality. The FSS is available to FinTechs as well as other technology initiatives intended to be launched in Hong Kong by authorized institutions.

ABU DHABI
Abu Dhabi Global Market (ADGM) has created the FinTech RegLab, a specially-tailored regulatory framework which provides a controlled environment for FinTech participants to develop and test innovative FinTech solutions. It's the first RegLab in the region and **the world's second most active FinTech sandbox**. By signing up to RegLab, FinTechs automatically comply with the Financial Services Regulatory Authority (FSRA) of ADGM

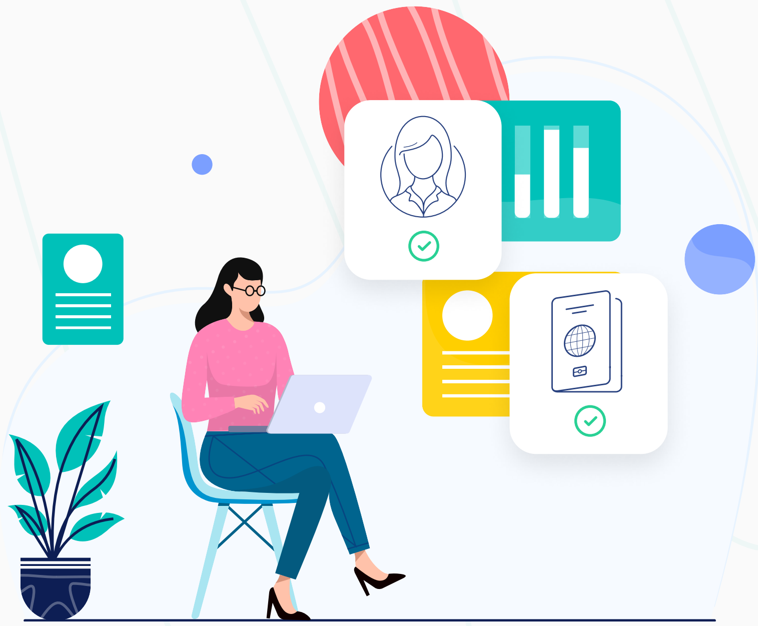
Current FinTech regulations in Australia

If you engage in credit activities in Australia you will generally need to have an Australian financial services (AFS) licence (Unless you are exempt or authorized by law to operate without one and instead abide by a regulatory sandbox) Credit activity includes:

- **Providing credit under a credit contract or consumer lease**
- **Benefiting from mortgages or guarantees relating to a credit contract**
- **Exercising rights or performing obligations of a credit provider or lessor (either as the credit provider or lessor or on behalf of another person who is the credit provider or lessor)**
- **Suggesting or assisting with a particular credit contract or consumer lease**
- **Acting as an intermediary between a credit provider and a consumer (for a credit contract) or between a lessor and a consumer (for a consumer lease).**

You will need to have your credit licence or authorisation from the day you start your business. Strict penalties may apply to persons who unlawfully engage in credit activities.

Good news though: the Australian regulatory sandbox allows eligible fintech companies to test certain products or services for up to 12 months without an Australian financial services (AFS) licence or credit licence.



Conclusion

As you can see, the majority of these countries have regulations in place, whether specifically for FinTech or financial institutions in general. Some regulations may be more advanced than others, but make no mistake, every country is working towards a more controlled economic environment. Failure to do so wherever you are will lead to expensive fines and a potential end to your business. Compliance with authorities is essential for companies to operate, grow, and ultimately succeed.

Conclusion

In today's complex economy, making sure that all the money in circulation is regulated can be an extremely challenging task. Despite the many advancements in banking processes and technology, money-laundering is an issue that still exists. There are many banks and financial institutions, still facing money from illegal sources coming in to be laundered. KYC is the first defense against this, and therefore, it has also become a regulatory requirement in the majority of countries. Doing business with individuals and organizations with questionable backgrounds can lead financial institutions such as FinTechs to face possible fines, sanctions, and even reputation damages.

As simple as verifying someone's identity may sound, it can be a very painful process to carry out without the proper tools. The global pandemic we are now facing has introduced **tremendous challenges** for organizations that are required to comply with KYC regulations – at least, for the ones that were unprepared to digitize operations. While many companies have adapted to digital processes and compliance, many others have not, and therefore have seen a substantial loss of customers during this time.

Major financial institutions such as banks are struggling to keep these processes running throughout this crisis, which should be an eye-opener for **how unprepared the whole world was for COVID-19**. Truth is, the onboarding of customers shouldn't come to a complete stop when a pandemic occurs. However, this should be taken as a lesson that being able to digitally onboard new customers is key, as is following regulations aimed at preventing crimes such as tax evasion and money laundering no matter the situation, whether its a pandemic or any other world-crisis.

Final thoughts: KYC/AML regulations can be challenging to understand, but it's a great way to **protect your business from malicious activity**. Especially during these times where fraud keeps skyrocketing everywhere in the world. This is why accelerating processes such as fully digitalized, seamless compliance should be a must on your agenda. If you're wondering where you should start, our KYC consultants are here to help!

Book a Demo

Discover our other publications

CUENCA

NEOBANK MEXICO

How the Mexican **neo bank** Cuenca became **KYC compliant** in a few days

Read More →

bien para bien

LENDING AUTOMATION

How Bien Para Bien automated its user verification flow in 2 days

Read More →

mati

MATI WHITE PAPER

User Verification 101

Learn how to create a powerful user verification process to cut down fraud and stay compliant

Read More →

mati

MATI GUIDE

Product Guide

Read More →

mati

Book a Demo