



Digital Onboarding: How It Works, Tools & Solutions



Contents

What Is Digital Onboarding?	3
How Does the Digital Onboarding Process Work?	3
The Benefits of Digital Onboarding	4
The 3 Key Types of Onboarding	4
The Challenges of Digital Onboarding	5
KYC Software Is Typically Expensive	6
Identities Are Easy to Falsify	6
Biometrics Are Easy to Beat	6
How to Set Up a Digital Onboarding Process for Fraud Detection	8
Digital Onboarding Solutions	10
1. KYC	10
2. Verification	10
How?	12
3. Dynamic Friction	13
Which Tools Should You Use to Complete a User Profile?	13
Conclusion: Creating a Frictionless Digital Onboarding Process	14
Digital Onboarding FAQ	15



On paper, a fully online business model has enormous advantages. You can target a global market, operate 24/7, and have more control over the data.

But there's an area where traditional brick-and-mortar setups win: verifying people's identities. This is precisely the challenge of the modern digital customer onboarding process. Let's see what works, why it's risky, and how to make digital onboarding as smooth as possible without attracting fraudsters.

What Is Digital Onboarding?

Digital onboarding, also known as remote onboarding, is the process that describes the journey as companies incorporate or acquire new customers online. It can take place on websites or in-app but, crucially, not in-branch or on-premise, since it is a fully digital experience.

Note that the term digital onboarding also applies to building new business partnerships. In both cases, a certain level of due diligence is required, whether it's to ensure you know your customer (KYC), or know your business (KYB). Since staff members or business partners do not get to interact in person during the user-customer journey, it is vital to establish security procedures to ensure people are who they say they are. This may be done via identity verification, digital footprint analysis, or other forms of due diligence.

Depending on your business vertical, the term onboarding may also be synonymous with signup, acquiring, new account creation, or self-boarding, among others.

How Does the Digital Onboarding Process Work?

Digital onboarding is a form of acquiring customers that fully takes place online. The user simply signs up through your service using their device, providing the necessary details step by step. Not only is the onboarding flow designed with usability in mind, but it also serves to meet know your customer (KYC) and [customer due diligence \(CDD\)](#) compliance standards.



In its simplest form, digital onboarding allows you to turn visitors into service users or customers in exchange for providing their personal details on signup, allowing you to verify their identity.

The Benefits of Digital Onboarding

As online browsing, be it on the web or in apps, is a solitary process, digital onboarding gives you the benefit of engaging your potential customers more directly.

This includes:

- learning more about them (via steps like KYC checks as well as [digital footprinting](#))
- a chance to market directly to them through emails and other messaging
- enabling easier purchases and inquiries
- allowing merchants to keep track of customer trends
- making customers feel attended to
- meeting KYC, CDD and AML obligations, where applicable

Digital onboarding can be used by any business that wishes to serve customers online, but it's absolutely crucial for e-tailers, online merchants, and online-only financial institutions, who have no other means of signing up users. It's also used in employee onboarding to manage remote workers, to save time on paperwork and/or to handle employee data digitally.

The 3 Key Types of Onboarding

While you may have heard of traditional vs. digital onboarding, these aren't the only options. Let's look at a few different user journeys you can offer to grow your customer base.

- **On-site client onboarding:** this is the conventional, or traditional method, whereby someone attends an office, branch, or store in person in order to verify their identity. The application process may be slower but more secure.
- **Hybrid onboarding:** companies can allow customers to fill out their initial application online, but they must still present themselves in person to confirm the new account creation. This creates a nice balance, allowing customers to be flexible about their initial input while still letting you accept or decline the application in person.
- **Digital onboarding:** finally, a fully digital onboarding model, also called online onboarding or remote onboarding, is crucial for companies that operate without physical locations, such as neobanks and fintech institutions. What you gain in flexibility (24/7 onboarding, access to a global market), you must make up for in terms of security checks, notably KYC verification.

Different business models require different approaches, of course, but the key is to always consider the balance between friction, security, and a user-centric approach.

The Challenges of Digital Onboarding

It is accurate to say that businesses that want to stay on the right side of the law aren't rewarded for their efforts. More often than not, customers who find too many obstacles during the signup process will abandon it.

This is known as **customer churn** and it's increasingly a battleground for the new wave of modern online businesses.

As the always-on economy shows no signs of slowing down, customers expect to be able to sign up for new services as easily as possible. Adding too many verification steps becomes an obstacle that sends them towards more lenient competitors. Yet, legislation and best security practices call for caution.

KYC Software Is Typically Expensive

To make matters worse, companies that rely on traditional KYC services find that their money is quickly going down the drain, as each customer identity verification can cost between **\$10 and \$100**.

Even alternative digital onboarding solutions that focus on identification, such as Stripe Identity, only reduce the cost to **\$1.5 per KYC check**, which is still pricey if you have a high volume of applications. Especially if most of them are fraudulent. You are essentially wasting checks on invalid users that bring nothing to your business.

Identities Are Easy to Falsify

Fraudsters do their best not to tie their real-life identities to online accounts. This is why they steal other people's identities or create synthetic identities by combining real and fake data.

Traditionally, the only companies that needed to verify people's identities were financial institutions because failing to identify that someone incurred risk meant they could end up lending money to criminals using fake or stolen data and ready to disappear without repaying.

But as more companies offering payouts have moved online, fraudsters have established novel methods for beating ID checks. They will use throwaway or freshly minted emails and phone numbers when signing up to different services, which allows them to use these as springboards for other schemes.

Biometrics Are Easy to Beat

To meet digital onboarding checks, fraudsters will:

- use stolen user information, acquired via phishing or bought on darknet marketplaces in the form of "fullz" – packages that include someone's name, address, and credit card number
- forge ID documents (using Photoshop or other editing software)
- combine real and fake data for [synthetic identity fraud](#) attacks.

A rise in rent-an-ID service is also occurring. This is when someone willingly sells their identity documents to criminals who need them to commit their crimes. By allowing fraudsters to use their identity online, the person becomes complicit and receives a small commission.

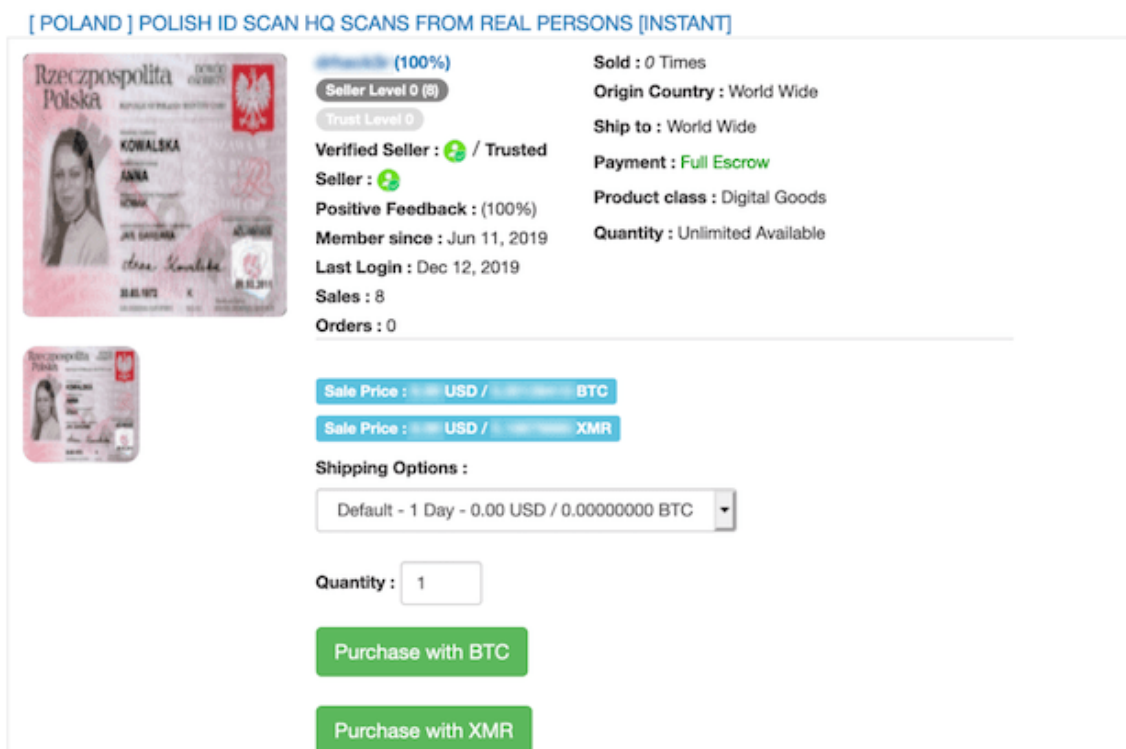
Everyone's ID details are valuable. Fraudsters often make use of identity details from deceased people and even children because the latter have positive credit scores by default.

What's more, the growing popularity of AI-based technology – such as deepfakes, which allow criminals to create a falsified video or audio recording of people without permission – raises new questions about the relevance of ID-based authentication. While this may sound like science fiction, biometrics technology has worryingly been shown to be relatively easy to beat, even with more low-tech methods.



For instance, Kraken Security Labs has demonstrated that anybody's fingerprints can be faked for under \$5, by simply using a close-up photo of their fingers. Automated facial recognition can be beaten by printing a photo of the individual, per Naked Security.

The takeaway? Biometrics are good for identification but have their own risks from a security standpoint.

[POLAND] POLISH ID SCAN HQ SCANS FROM REAL PERSONS [INSTANT]



Rzeczpospolita Polska
KOWALSKA ANNA
JAN SPOWAS
JAN SPOWAS
ANNA KOWALSKA
12.12.1991

100%
Seller Level 0 (8)
Trust Level 0
Verified Seller :  / Trusted
Seller : 
Positive Feedback : (100%)
Member since : Jun 11, 2019
Last Login : Dec 12, 2019
Sales : 8
Orders : 0

Sold : 0 Times
Origin Country : World Wide
Ship to : World Wide
Payment : Full Escrow
Product class : Digital Goods
Quantity : Unlimited Available

Sale Price : USD / BTC
Sale Price : USD / XMR

Shipping Options :
Default - 1 Day - 0.00 USD / 0.00000000 BTC

Quantity : 1

Purchase with BTC
Purchase with XMR

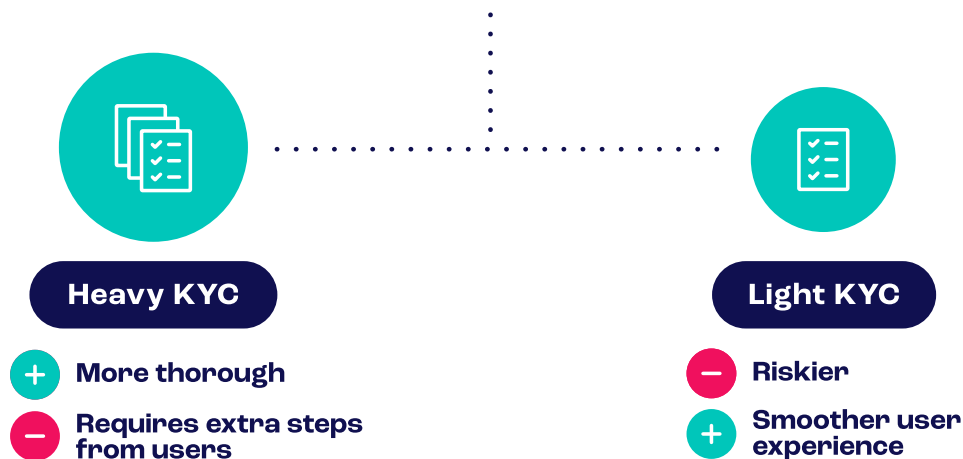
How to Set Up a Digital Onboarding Process for Fraud Detection

The digital onboarding process is quickly becoming an important battleground for online companies. Maximizing traction with high acceptance rates is key. If people cannot register fast and easily enough, they will go and do this with a competitor.

So what does a frictionless onboarding experience look like? It has to be all of the following.

- **Easy:** Nobody wants to have to fill long forms and answer in-depth questionnaires to access a new service these days, whether it's an online store or to apply for a new debit card.
- **Fast:** No long delays in accepting an application. That means having a clear understanding of the steps required and giving expectations of how long the whole thing should take.
- **Seamless:** Lengthy safety measures can put off new customers by creating churn. Asking customers to provide additional documents or a selfie, or even to have a video chat conversation in order to complete onboarding can be a barrier for those who want to quickly sign into a banking account.

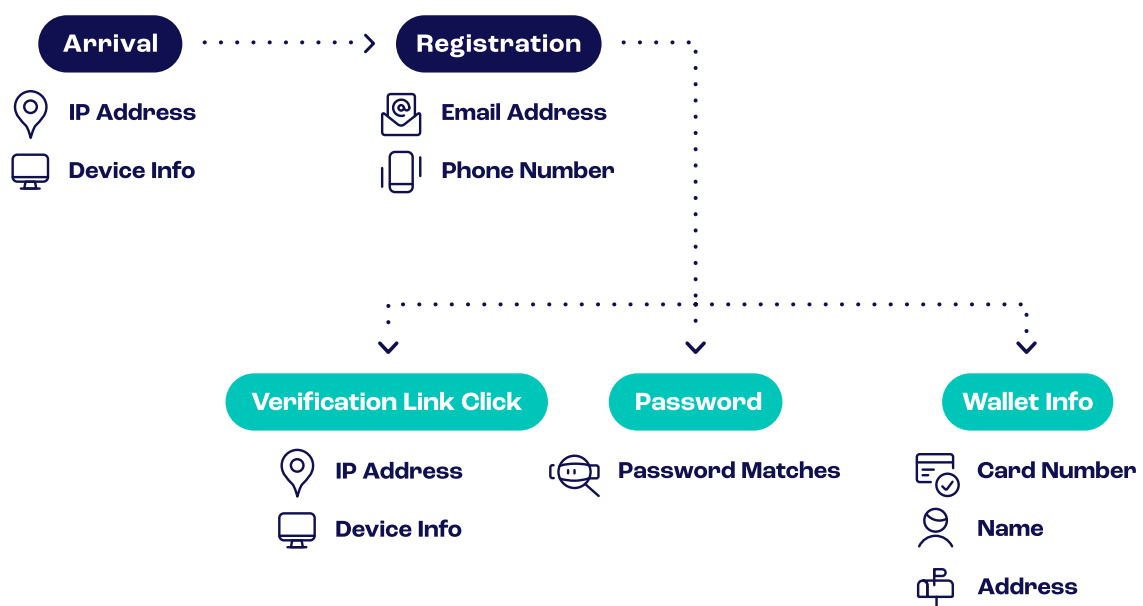
Heavy KYC vs Light KYC



Whatever your user onboarding flow is, you will be capturing a wealth of information about your user at each step. Instead of forcing through all of your users at a mandatory hard KYC chokepoint and relying on an expensive third-party verification service, **you can use the data they provide to build user profiles.** What's more, you can apply [risk scoring](#) at every step of the process to assess whether or not to allow the user to continue. If they are determined to be risky, you can trigger a stricter security check or manual review. If they are determined to be too much of a threat, you can block them completely – or any combination of these. This approach is called **dynamic friction**, and it's the bread and butter for many of our clients.

Think of your typical user journey on registration. Ideally, they should gradually reveal more and more about themselves in a game of establishing mutual trust.

- 1** When they arrive on your website or app, you will see their **IP** and **device information**.
- 2** When they sign up or register, they will provide you with a point of contact – **an email address or a phone number**.
- 3** You will send them an activation link, which they might use from a **different device** you will also find out about.
- 4** You can ask them to provide a **password**.
- 5** And finally, you ask them to provide their **card number, name, and/or address**.



This checklist will be more or less the same across verticals, with some details omitted in certain industries. But the point is that **risk checking each of those details** at the step you receive them should give you a clear view of who you're dealing with, which allows you to satisfy customer due diligence requirements even before you've asked for a selfie and an ID!

Digital Onboarding Solutions

So, how can businesses get a better idea of who they're onboarding without sacrificing user experience, cost, and security? At SEON, we believe you need a three-pronged approach to digital onboarding.

1. KYC

Electronic know your customer (eKYC) tools have improved in sophistication and ease of use in recent years. You can now integrate them directly into your platform and submit and receive data via API calls. In most cases, you'll need to send:

- a full name
- a scan of an official ID document

The online KYC tool will then perform a real-time check to see if the name and IDs match existing records, or at least give you an idea of how risky the onboarding looks based on their own parameters.

2. Verification

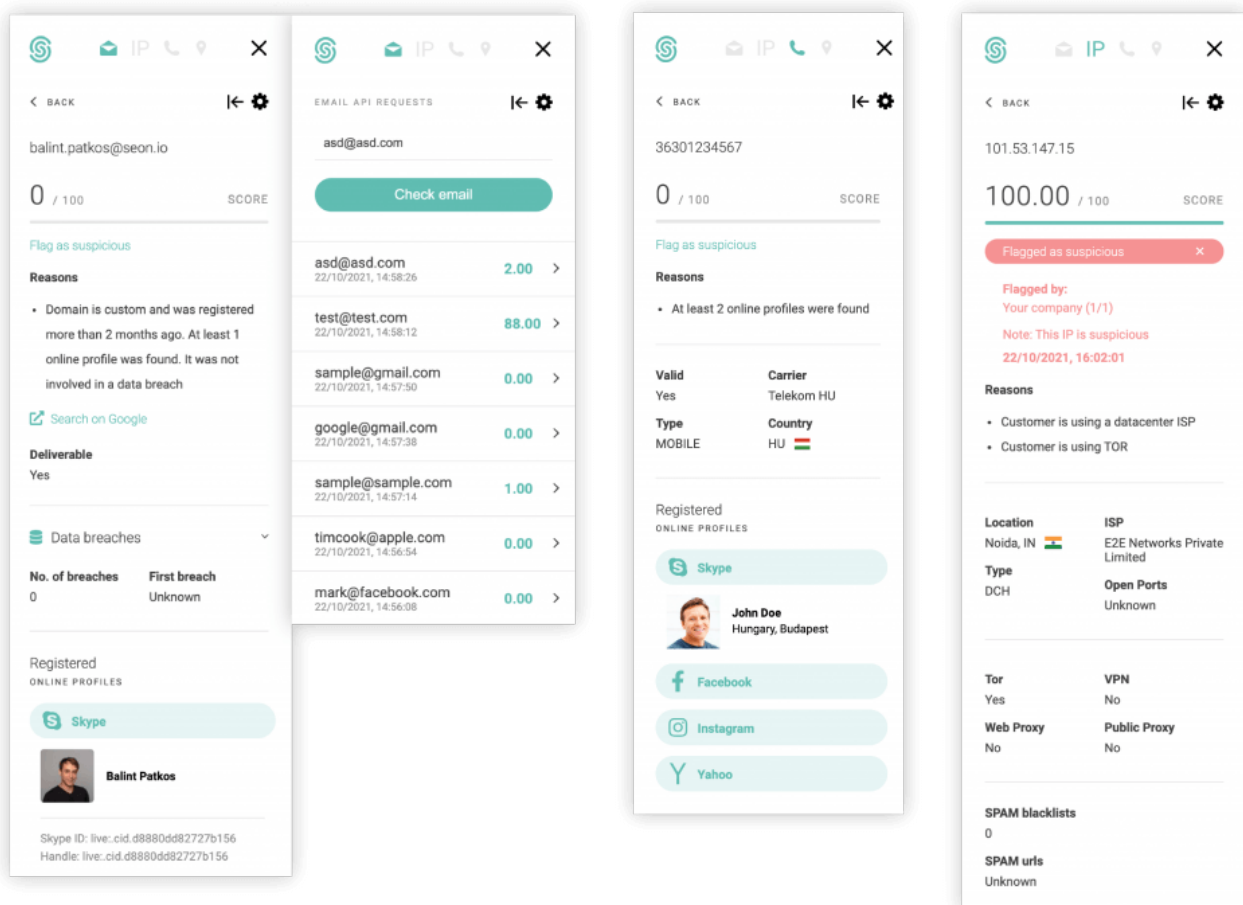
In some cases, you'll want to learn more about users without asking them for any verification. This is absolutely doable thanks to a process called digital footprint analysis, also referred to as "KYC based on alternative data".

You start by collecting data points about the users as soon as they land on your website. This can be based on an IP address or the kind of device they used to connect to it, thanks to [device fingerprinting](#).

To perform this analysis, you will only need basic information such as:

- an IP address
- an email address
- a phone number

The phone number option is particularly interesting as 2FA is increasingly becoming the norm. This pushes fraudsters to use fake phone numbers or virtual numbers, which can be detected by your fraud prevention platform.



With the right data enrichment tools, you can extract enough information to immediately find red flags about bad users. For instance, you might find the below suspicious:

- users without social media presence
- users using VPNs, suspicious proxies or Tor

- those on unrecognized devices
- those whose IPs have appeared on spam blacklists

All this data can help create a risk score, which will give you an idea of how likely the person is to be real or not. You can use that score to automatically approve or decline the onboarding process with **much more confidence**.

How?

- **Device information:** Not only are some devices riskier than others, but repeat offenders can be easily caught by device connections. Similarly, device information can reveal anomalies such as clashing time-zone or language settings compared to who the user claims to be.
- **IP information:** When it comes to fraud, proxies, VPNs, and Tor are the name of the game. By detecting them early on, you can block bad attempts easily – and filter out repeated or automated attempts.
- **Email information:** By performing a reverse email lookup on social platforms and checking against the Have I Been Pwned database of leaked emails, you can quickly evaluate whether the user is an existing person or not. Fraudsters will more often than not use throwaway emails registered for the purpose of identity theft, while good users will have a social media “portfolio”, depending on the target market.
- **Phone information:** While it’s not recommended to rely on SMS for two-factor authentication, a phone number can still be used in risk scoring. You can use CNAM/HLR lookups to determine whether or not it’s a virtual carrier or, better yet, find out the registered name for that number.
- **Password:** Password hashes can yield surprising user connections, whether it’s a phrase that is common in a given language or the favorite passphrase of a fraudster. You can also use password hashes to protect your users from account takeovers by checking them against known leaked passwords and forcing users to choose a more secure alternative.
- **Address information:** The address can be compared to the user’s IP address to determine if the distance between the two is feasible or not.
- **Card information:** It’s increasingly common to ask for user payment details upfront, rather than at checkout, as it makes for a better transaction expe-

rience. You can use this step to verify whether or not the card has funds on it with a trial charge, but you can also perform a BIN lookup to gain information about the cardholder.

By layering the above steps one after another, applying risk scores to each detail, by the time your user finishes registration, you will know exactly who you're dealing with and **whether or not you should let them on your platform.**

This creates a powerful defensive moat around your services even before the users first hit a transaction page. The best part? Good users will not notice a thing as all these checks run in the background without any friction, while fraudsters will see their attempts fail repeatedly, frustrating them enough so they give up!

3. Dynamic Friction

But what happens when the risk score isn't conclusive and you do need to ask for extra information? This is exactly the process we call dynamic friction and, to explain it, it helps to break down the idea of KYC into light and heavy processes.

The advantage of using the dynamic friction method is that you can use the light KYC stage to filter out a lot of unwanted users. Those who are clearly fraudsters using stolen IDs will not make it to the next stage.

If, however, they make it through but still pose a risk, you can then ask for heavy [KYC verification](#), as we outlined above.

Which Tools Should You Use to Complete a User Profile?

Whether it's for your own KYC verification or to reduce applications that use fraudulent data, you'll need to enrich data about users as much as possible.

At SEON, we have a series of tools designed for the job. These include our IP analysis module, for anything related to the connection type; our device fingerprinting solution, which looks at a configuration of software and hardware (device and browser, for instance); our email and phone analysis data enrichment modules, which can



aggregate data from open source databases to gain a 360° view of customers.

The phone and email analysis tools are particularly useful thanks to our reverse lookup feature, which gathers info from 50+ online networks including someone's user picture, bio, social network presence, and date last seen online.

Our clients use that data to estimate underwriting risk, to speed up manual reviews, and even for debt collection.

Conclusion: Creating a Frictionless Digital Onboarding Process

Circling back to our point about friction, we can now see that balancing security and user experience is key in onboarding. Yes, you want to grow your user base as quickly and easily as possible but you don't want the door to be open so wide that anyone can enter.

The answer, therefore, lies in flexible and adaptable security tools for your digital onboarding. Balancing light and heavy KYC processes will help reduce fraud without creating obstacles for those with a clean record.

While there is always an element of trial and error to balancing security and setting up an easy onboarding process, we believe fraud analysts have a large role to play in this important aspect of interacting with your customers.

This is why we have created a wide range of tools that provides organizations with full control over risk thresholds during the onboarding experience, including automated flagging at the identity verification stage and machine learning-assisted decision making for [identity proofing](#).

This is where the key balancing act lies: Add too many verification steps and you can be certain never to pay an AML or KYC fine. But make it too stringent and users will look elsewhere. The key is to deploy a better KYC compliance process that gives you full control over the amount of friction without sacrificing security.



Sources

[Kraken Security Labs](#): Your Fingerprint Can Be Hacked For \$5. Here's How.

[Naked Security](#): A photo will unlock many Android phones using facial recognition

Digital Onboarding FAQ

Why is digital onboarding important?

Digital onboarding enables you to serve your customers better, while simultaneously preventing fraud and fulfilling any legal obligations you might have. Read our section on the [benefits of digital onboarding](#) above for more.

What is onboarding in fintech?

Onboarding in fintech involves signing a new user up for the service as well as [verifying their identity](#) according to local KYC and AML legislation. Fintechs do what traditional financial institutions, albeit with a much more user-centric approach. As fintech companies do handle consumers' money and can be abused for illegal activity, such as money laundering and terrorism financing, authorities expect them to conduct identity verification at the onboarding stage.

How can digital onboarding be improved?

Advanced fingerprinting and footprinting can improve your digital onboarding and add more value to it. At SEON, we examine each customer's digital footprint to give you unprecedented insight into their intentions and help you assess whether they can be trusted. This means you can both prevent more cases of fraud and reduce your identity verification costs, as untrustworthy customers can be stopped from proceeding to the official KYC step.

What is client onboarding in banking?

When a bank first signs up a new customer, they need to verify who this person is, their age, and their address. A bank might also request additional documents depending on local legislation and the organizational strategy. Only once this is complete is the individual ready to trade with the bank in earnest.



Easy fraud detection
for every business

Try for free

