Guide

Frictionless Authentication: Definition, Examples, and How to Do It Right

SEON Technologies Ltd.
seon.io
info@seon.io
+44 20 8089 2900

Table of Contents

Online businesses are constantly balancing ease of use and security. Nowhere is this more apparent than at the identification stage.

The good news? Frictionless authentication is possible – with the right tools.

What Is Frictionless Authentication?

Friction-free authentication is a form of automated identity verification based on risk. Its goal is to allow good users or block risky users without asking for too much personal information.

You may deploy frictionless authentication at the signup, login, or transaction stage. The key to frictionless authentication is that the identification should happen in real-time without adding obstacles to the customer journey.

Forms of authentication that are considered high-friction, as opposed to frictionless, may include:

- **selfie video verification**
- **multi-factor authentication**
- **document upload**
- **manual review of a form**
- **CVV and address verification for payments**

By removing these steps, you may deploy frictionless authentication – but at the risk of accepting more dangerous actions from bad users. There is always a give-and-take between safety and friction.

Frictionless authentication can also let you determine whether further authentication is necessary. This form of dynamic friction works like a traffic lights system. It allows companies to let low-risk users proceed with their actions. High-risk users are immediately blocked, while medium-risk users' actions can be manually reviewed.

Why Do We Need These Methods?

As customer experience increasingly becomes the battleground where business is won or lost, companies have every incentive to improve ease of use. This is true whether you want to allow people to purchase a good or service, onboard to your platform, or log in to access their account.

In fact, research from the open banking platform Tink reported by Business Leader claims that 88% of consumers abandon a purchase if faced with friction.

This is precisely why verifying users' intentions without adding obstacles becomes so essential.

Where Can You Deploy Frictionless Authentication?

You can deploy frictionless authentication at any stage where you need to verify who you are dealing with. This may be:

- **The onboarding stage:** When a new user signs up for your service, you need to verify who they are. In some cases, it is a legal requirement, such as in the case of KYC and AML requirements. It's also a good business practice to reduce rates of application fraud.

- **The login stage:** Authenticating returning customers when they log into their account is also paramount for modern online businesses. You must be able to trust that a stranger (or worse, a fraudster) isn't accessing someone else's account – a process also known as account takeover fraud.

- **The payment stage:** Payments are notoriously difficult to manage when it comes to balancing ease of use and security. A retailer giant like Amazon, for instance, will go as far as avoiding asking for CVVs to speed up the checkout process. Smaller retailers may find this challenging due to the high rates of chargeback fraud.

By making these steps frictionless but still using alternative methods to authenticate users under the hood, you are keeping your operations safe without affecting the user journey.

How Do You Reduce Friction When Authenticating Users?

Authentication and friction go hand in hand. For businesses, the challenge is to reduce risk without slowing users. Here are examples of tools to deploy, depending on the stage of the customer journey.

Data Enrichment at the Onboarding Stage

When identifying users for the first time, it's crucial to ensure you deliver a smooth journey – even if you must have heavy KYC and AML checks in place.

Ideally, you would perform pre-KYC checks, which can alleviate the load on your actual KYC checks, saving costs and manual labor.

Pre-KYC checks work wonders with data enrichment. Not only is the extra data acquired in real-time, but you can also get a ton of information based on:

- **An email address:** Thanks to reverse email lookup, you can learn a lot about each user. How long have they had the address? Is it from a trustworthy domain? What does all this say about who they really are?
- **A phone number:** Similar to the aforementioned email address lookup, but with a phone number. Is it from a landline or mobile? Which country does it point to? Using a suspicious virtual SIM card?
- **An IP address:** Particularly relevant for AML checks related to sanctioned countries, an IP address is also a great way to identify potential red flags. Is the user where they say they are? Are they trying to spoof the data via VPN or Tor?
- **A user's device:** Understanding what kind of device your users connect with isn't always enough to go on. Device fingerprinting looks at hundreds more data points, and will help you learn when someone is trying to fake their data – for example, by using an emulator.

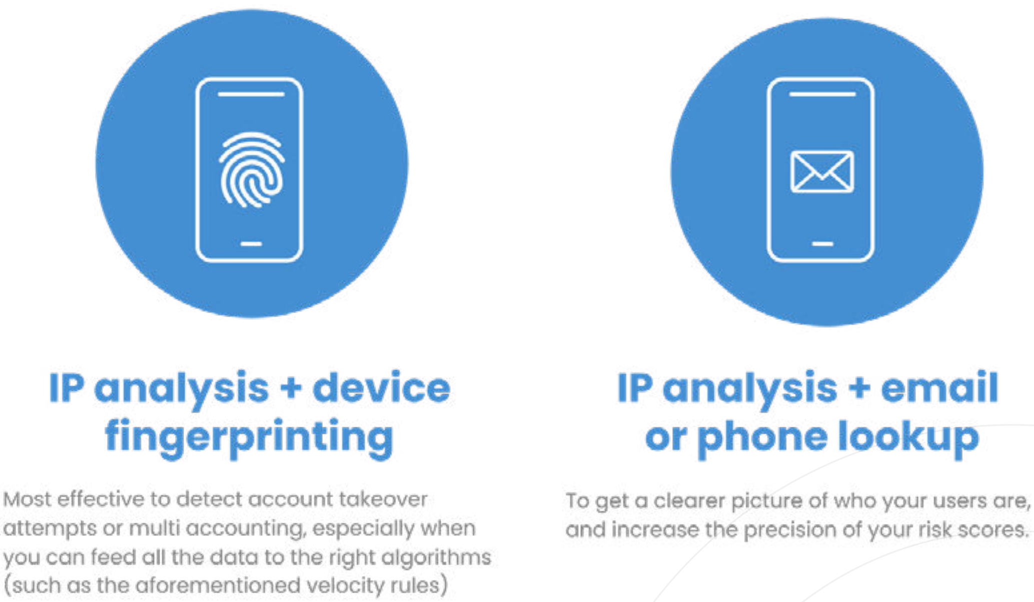
Data Enrichment at the Transaction Stage

With mounting payment regulations (PSD2, 3DS), anyone who accepts credit cards online must verify users as well as possible. But how can you learn more without asking for extra verification checks?

- **Email, phone, and IP lookup:** Similar to the aforementioned signup stage, these simple user data points can reveal a lot about who you're dealing with. It all comes in real-time, so there is no need to ask your customer for extra info.

- **Card BIN lookup:** Even the credit card data itself can be enriched to learn more about the user. Are they using a gift card or prepaid card? Does it point to a suspicious location (e.g., far from the billing or shopping address)?

Data Enrichment at the Login Stage



Authenticating users who log into your platform is all about protecting their accounts. Here's the data you should enrich to find out more about their true identity and intentions:

- **Device data:** Based on the device, cookie and [browser hash](), have you seen this device before on your site? Is it pointing to a suspicious emulator?

- **IP data:** Have you seen it before on your site? Is it pointing to a suspicious location?

But what do you do with all that extra metadata you managed to enrich? You have to feed it through the right risk scoring system. Let's take a closer look.

How SEON's Risk Scoring Enables Frictionless Authentication

SEON's end-to-end fraud prevention and data enrichment module uses risk scoring to assess the hundreds of data points it collects.

- **Enrich all your data points:** SEON lets you enrich email, phone, IP, device, and card data to get a complete picture of your users – even including their public social media profiles, to gauge who they really are.
- **Understand user behavior with velocity checks:** Once you have the data, you can use it to understand how users behave. Too many login attempts within a specific time-frame? Entered six different names in succession at signup? You decide what risk looks like and track it across your site – though there are also handy pre-set rules.
- **Manage dynamic friction:** Our risk scoring allows you to automatically accept, decline, or review a specific user action. Automatically allow good users, block obvious fraud, and escalate verification for medium-risk users only.
- **Improve your efficiency over time with machine learning:** You can get started in seconds with SEON's blackbox machine learning solution to give scores based on your industry. And you can also run it as a whitebox system that learns from your historical data to build increasingly precise risk models.

All are available via a free trial, complete integration flexibility, and zero setup or customer service fees.

FAQ

What is a frictionless transaction?

A frictionless transaction is one where the customer's journey is as smooth as possible. That means reducing obstacles in the form of security questions, 2FA, or extra authentication methods.

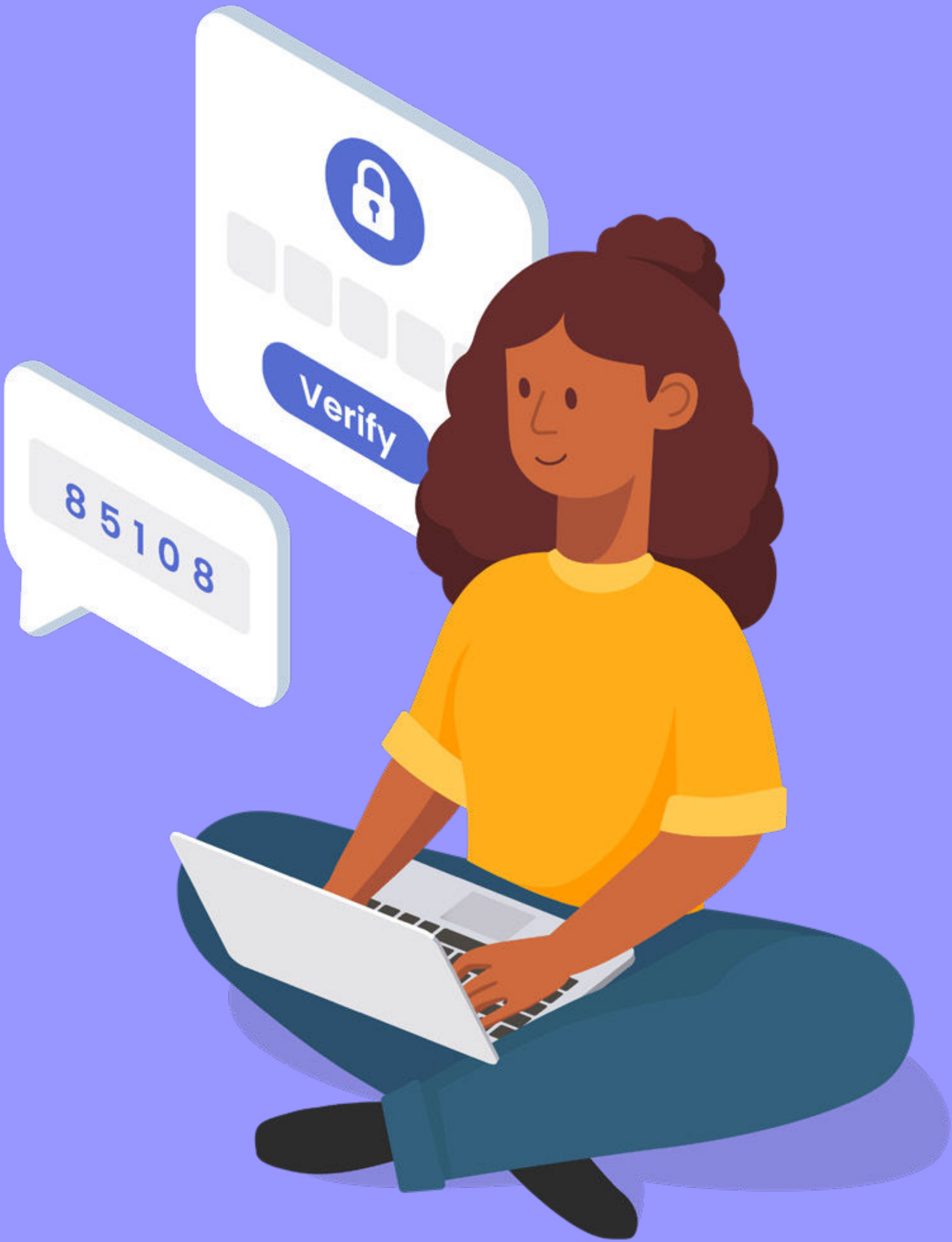
What is frictionless login?

A frictionless login happens near-instantly without having to receive codes via email, SMS OTP, or having to use complicated multi-factor authentication methods. Biometrics login authentication is the most frictionless method.

What is frictionless 3DS2?

3DS2, or 3-D Secure 2, is a security measure put in place by payment companies to reduce fraudulent payments. Because the earlier version of 3DS was notoriously high in friction, the second update aims to reduce it by sending more data behind the scenes, before the actual verification step.

SEON



SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900