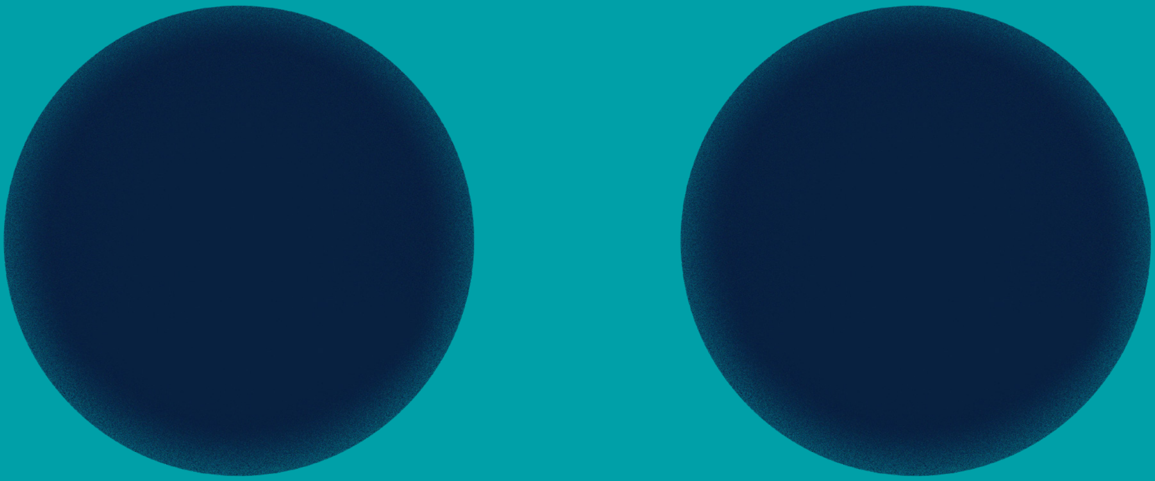
How to stop anti-fraud measures from slowing down your online banking business?

Advices from CISOs



We all know that today unhappy customers can switch banks in **less than 3 minutes** and **a few clicks**.

Customers are often unhappy because of the security measures banks use for their digital services. They are **too intrusive** and **too complicated to manage**.

This is why ensuring a **seamless and fast digital experience** is a top priority for banks and payment providers that want to keep growing their businesses.

But how to do this while **keeping customers safe** from online fraud?

In this document, we share some useful insights from a few banks' **Chief Information Security Officers** that work with Cleafy to understand the impact that anti-fraud measures used to have on their business.

Anti-fraud measures in online banking

Anti-fraud measures in online banking include a variety of **technologies and security protocols** designed to detect and prevent fraud. Banks, usually, use the help of **external anti-fraud platforms** to protect their systems from cyber criminals via:

- **Multi-factor Authentication** (MFA): This requires users to provide multiple forms of identification in order to access their accounts, such as a password, a fingerprint, or a one-time code sent to their phone (OTP).
- **Encryption**: Banks use encryption to protect sensitive data, such as account numbers and passwords, as it is transmitted over the internet.
- **Firewalls and intrusion detection systems**: Banks use these systems to protect their networks and servers from unauthorized access.
- **Risk-based authentication**: Banks use risk-based authentication to evaluate the risk level of a transaction based on factors such as the amount of money being transferred, the location of the user and the device being used, and whether the user's behavior is consistent with their normal activity.
- **Mobile app security**: Banks use various mobile app security measures such as device registration, app shielding, and behavioral analysis to prevent fraud.

Moreover, all CISOs agree that **customers' education** has become more and more relevant to keep people aware of the different ways they can protect their accounts from online banking fraud, like **phishing** and **SIM Swap**.

The impact of the anti-fraud measures on the online banking business

Anti-fraud measures are great to make sure people's money is always safe. But this doesn't come at no cost for banks.

Multiple security measures, in fact, can create **high friction and, therefore, be the main cause of a poor experience** for customers who just want to navigate safely and quickly on their online banking channels. Instead, they keep receiving SCA's notifications or getting blocked because the security systems need to make sure it is the legitimate user.

CISOs underline how higher friction generates a snowball of other direct and indirect costs that slow down the bank's business, including:

High churn and market share loss:
clients want to complete banking activities quickly, and prefer to switch to innovative and smart solutions. For example, if customers find the registration process for online banking too difficult or time-consuming, they may choose to bank with a competitor instead.

Reputational costs:
inevitably, as in all businesses, unsatisfied customers can strongly damage the bank's reputation and the chances to build a loyal client base.

High volume of customer service inquiries caused by the so-called "false positives":
whenever legitimate customers have trouble with using home banking or the banking app, they may contact customer service for assistance, which can drain the bank's resources.

How anti-fraud measures impair the digital experience for online banking customers

If not well managed, anti-fraud measures can have a significant negative impact on the digital experience for online banking customers. Let's see how.

Multi-factor Authentication (MFA):
While MFA is an important security measure, it can be inconvenient for customers to have to provide multiple forms of identification in order to access their accounts, such as a password and a fingerprint or a one-time code sent to their phone.

Risk-based authentication:
Some banks use risk-based authentication to evaluate the risk level of a transaction based on factors such as the amount of money being transferred, the location of the user, and the device being used; without a clear explanation of why further authtentications are requested, it can be confusing for customers.

Security questions: Some banks use security questions as a form of MFA, which can be difficult for customers to remember or provide accurate answers.

One-time passcodes: Some banks use one-time passcodes sent via SMS or email to confirm transactions, which can be inconvenient for customers if they do not have access to the phone or email address to which the code was sent.

Device registration:
Some banks require customers to register their devices before they can use online banking, which can be time-consuming and frustrating for customers.

CAPTCHA: Some banks use CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to prevent automated attacks and bots, which can be difficult for customers to complete, especially for those with visual impairments.

While these measures are necessary to **protect customers' personal** and **financial information** from fraud and identity theft, **increasing the trust** in the bank and the **willingness to use online banking services**, on the other hand, they can hinder legitimate customers who want to complete actions on their accounts.

Banks have then to consider the impact of these measures on the customer experience carefully, striving to **strike a balance** between **security** and **convenience.** This can be achieved by implementing measures that are **user-friendly and easy** for customers to understand. Additionally, banks should provide clear **explanations** of the measures in place and why they are necessary.

The best approach to minimize friction for online banking customers

That said, we wanted to dive deep into the ways **banks can minimize friction** for customers while keeping them safe. According to the CISOs, there are a few strategies that can facilitate the balance between security and convenience, such as:

- **Implementing user-friendly security measures**: Banks should make sure that the security measures they implement are easy for customers to understand and use. This can include re-designing the user interaction for the measures in place and including a clear explanation of why they are necessary.

- **Limiting risk-based authentication requests**: Banks can use risk-based authentication to evaluate the risk level of a transaction based on factors such as the amount of money being transferred, the location of the user, and the device being used. This can help to minimize friction by only requiring additional authentication measures when necessary.

- **Making multi-factor authentication** (MFA) leaner: Banks should consider using MFA methods that are easy for customers and do not require them to remember additional information. For example, using biometric authentication such as facial recognition or fingerprint scanning can be more convenient for customers than having to remember a password.

- **Using advanced fraud detection and response systems**: To ensure all the above are correctly implemented, it is key to integrate advanced fraud detection and response systems that can accurately evaluate the risk in real-time along the user journey; this is the key to reducing false positives, and "disturbing" clients only when really needed.

The game changer for a fast-growing and safe online banking business

What if every micro action taken by the user could trigger the banking app to respond in the most appropriate way for that specific moment and situation?

That would finally mean maximizing security and minimizing friction, wouldn't it?

The thing is that this would require the **right ingredients** for the **magic recipe**:

- a **complete picture** of what's really happening that is continuously updated, virtually with infinite granularity, instant by instant, so that to have always the actual measure of risk
- **granular levels of authorizations**, where every one of those levels is paired with different ways to interact with the banking app for each possible action that can be taken on the app.
- **a way to associate the first two points**: a specific level of authorizations to the precise measure of risk at that specific moment, session, and user.

And that's how the magic happens. Knowing the **exact risk at any given time** to be able to make the banking app respond continuously in an **ultra-tailored way**.

That is actually what Cleafy allows banks to do.

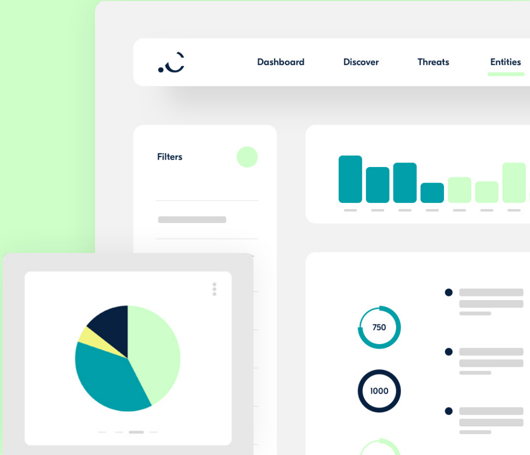
Cleafy can provide a fully dynamic risk-based approach, which allows the banking app to adapt to the customer's behavior dynamically.

This is the secret key to avoiding unnecessary steps for the customer and reducing friction to the bare minimum while keeping security at maximum level.

Stop fraud from slowing down your business

Get a free consultation with our team to identify
the bottlenecks in you anti-fraud strategy
and turn them into business opportunities.

Get a free consultation



Cleafy: a new era in online banking fraud

Latest technologies have done great work shifting from a **pure prevention static paradigm** to a **more flexible way to manage risk** via a Detect&Response approach.

However, fraud techniques have further evolved, and customers' expectations are higher than ever. Today, even the modern detect&response approach starts showing weaknesses and causing serious impacts on the business.

Both detection and response capabilities aren't enough granular, comprehensive, and fast.

Cleafy fills the missing gap, going the extra mile to reach the highest level of visibility and granularity in how the banking app responds to each micro-action taken during the session.

So your business can keep growing, while your customers are always safe.

cleafy.com