

Onboarding Risk Reduction in Digital Banking

Leading Global Fraud Prevention

SEON.IO

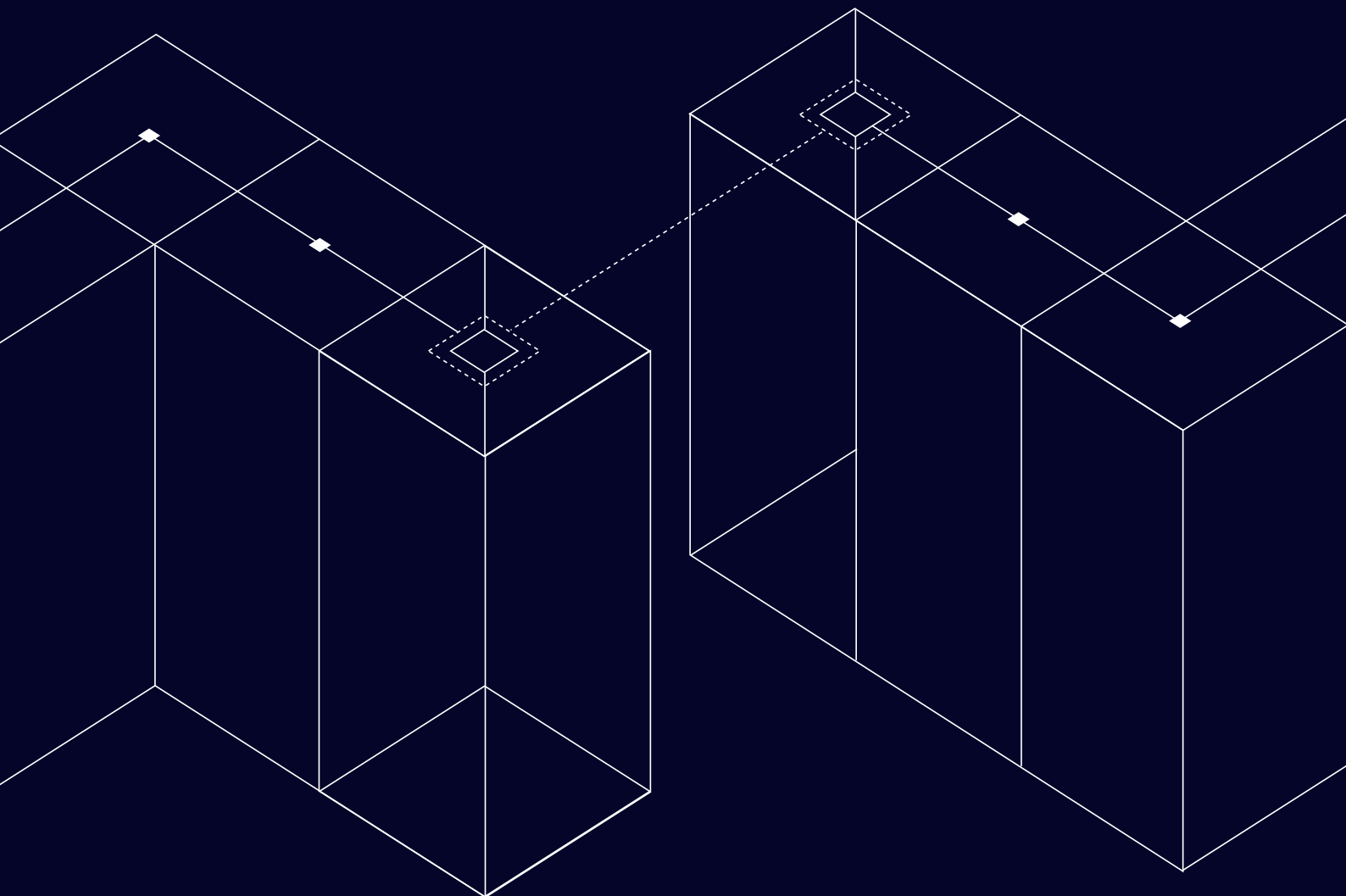




Table of Contents

Introduction	3
The Double Binds of Digital Onboarding	4
Balancing Efficiency & Security	6
Regulatory Pressures: KYC & AML	7
The Cost of Cutting Corners	8
Critical Challenges in Digital Onboarding	9
Identifying Fraudsters & Bad Actors	10
Preventing Onboarding Fraud & Account Takeovers	10
Managing Customer Expectations for Speed and Convenience	11
High Onboarding Abandonment Rates	12
Customer Experience Issues	12
Identification Verification Challenges	13
Technology & Integration Issues	13
Regulatory Compliance	14
Customer Understanding & Retention	14
Competitive Pressures	14
Strategic Solutions & Technology for Reducing Onboarding Risks	15
Pre-KYC Checks: Screening Out Fraud Early	16
Data Enrichment for a Complete Picture	16
Automated Risk Scoring Systems	16
Machine Learning & AI	17
Continuous Monitoring & Adaptation	17
A Smart Approach to Efficient Onboarding	18
Dynamic Friction: Tailoring Security to Risk Levels	19
Device Fingerprinting and Browser Data	19
Real-Time Data Enrichment for Fraud Prevention	20
Shaping Tomorrow: What's Ahead for Digital Banks?	21
Evolving Threats in the Digital Banking Landscape	22
How Technology Will Shape the Future of Onboarding	22



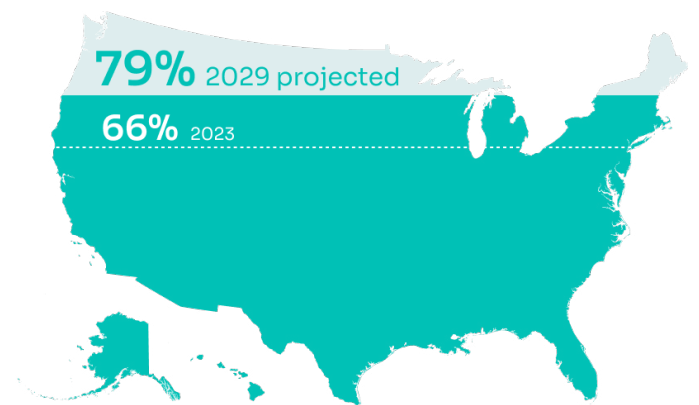
Introduction

The digital banking revolution has radically transformed how financial institutions engage with customers, creating a demand for seamless, fast and secure onboarding processes. Today, 71% of consumers prefer managing their bank accounts through mobile apps or computers, with mobile banking being the primary choice for 48% of US consumers.¹ As digital-first solutions dominate, the onboarding experience has become a critical touchpoint, influencing customer satisfaction and long-term loyalty.

But with convenience comes risk.

The growth of digital onboarding has also introduced new avenues for fraud, identity theft and financial crime, making risk reduction strategies essential for any digital bank. For instance, online banking penetration in the US reached 66% in 2023 and is expected to exceed 79% by 2029². Given this expansion rate, striking the right balance between speed, customer experience and security is more challenging than ever, requiring strategic foresight, regulatory awareness and technological innovation.

Generational preferences further underscore the demand for efficient and secure onboarding. Mobile banking usage is highest among Gen Z (89%) and Millennials (84%), but even Gen X (71%) and Baby Boomers (39%) are increasingly adopting



Online banking penetration in the US by 2029

digital banking solutions.³ With 97% of consumers rating their mobile and online banking experience as positive, banks must ensure that onboarding processes meet user expectations and protect against evolving fraud threats.⁴

This guide will explore how digital banks can reduce onboarding risks without compromising efficiency. We'll examine the unique challenges posed by online account creation, identify solutions to mitigate risks and highlight the role of advanced technology in securing the onboarding process.

¹ Bankrate: Digital banking trends in 2024

² Statista: Penetration rate of online banking in the United States from 2019 to 2023, with forecasts from 2024 to 2029

³ Bankrate: Digital banking trends in 2024

⁴ Ibid.



The Double Binds of Digital Onboarding

Digital banking's core value proposition centers on seamless, efficient user experiences. Customers now anticipate swift online processes for account creation, product applications and transactions – without compromising security.



“Digital banking’s core value proposition centers on seamless, efficient user experiences.”

This expectation creates complex tensions such as:

- How can digital banks streamline onboarding without compromising thorough fraud checks and regulatory compliance?
- What strategies enable rapid growth while mitigating increased exposure to financial crimes?
- How can technological and procedural advancements meet customer demands for speed and regulatory requirements for diligence?
- In what ways can advanced analytics enhance both operational efficiency and risk management?
- What approach provides easier account access without weakening defenses against unauthorized use?

Addressing competing priorities demands a sophisticated strategy, and success hinges on integrating cutting-edge technology, developing nuanced policies and cultivating a deep understanding of evolving customer needs and regulatory expectations. Banks harmonizing these elements will be best positioned to thrive in the digital banking ecosystem.

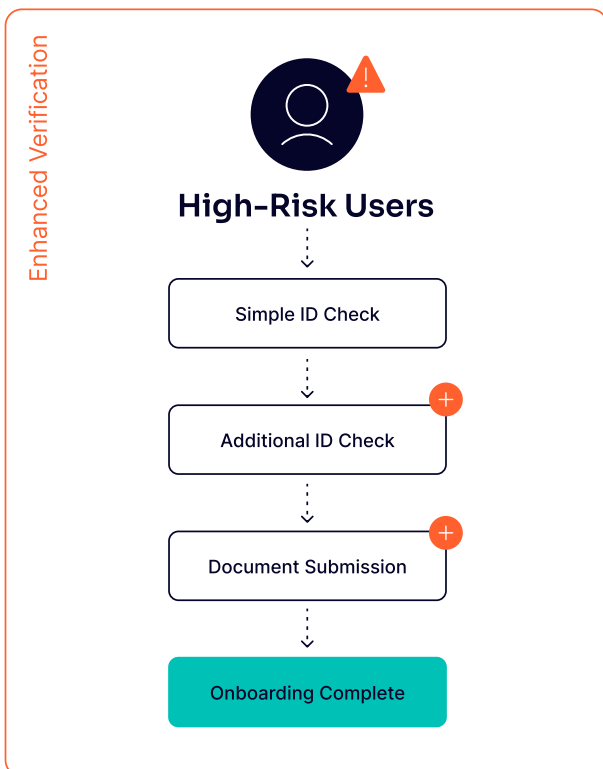
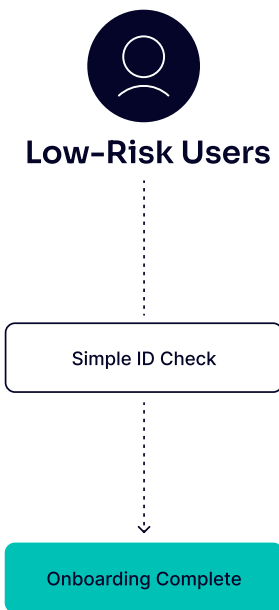


Balancing Efficiency & Security

The pressure to deliver a fast and efficient onboarding experience is immense, especially in the hyper-competitive digital banking landscape. Customers, particularly younger generations, expect a seamless process that enables them to open accounts or access financial products in minutes. Lengthy forms, identity checks and verification processes that were once acceptable in traditional banking are now seen as friction points that could drive users away.

However, speeding up onboarding comes with significant risks. Banks focusing solely on efficiency may overlook critical security measures, exposing themselves to fraud, identity theft and other financial crimes. A smooth onboarding process is only successful if it can weed out bad actors while allowing legitimate customers to join without hassle. Striking this balance is where many digital banks struggle. Success lies in finding ways to automate and streamline processes without sacrificing the necessary layers of protection.

Manual reviews remain a common practice for digital banks aiming to ensure security, but this approach is not without its drawbacks. Large teams are required to handle the volume of manual checks, which slows down the onboarding process and consumes resources that could otherwise be invested in growth and innovation. Automating risk assessments and verification processes allow banks to scale more efficiently, meet user expectations for speed and reduce operational costs without compromising security.



Tailoring Verification to Risk Levels



The key to balancing efficiency and security is dynamic friction. Banks can adjust verification requirements based on real-time data and risk levels. Customers who pose little risk can enjoy a frictionless experience, while those flagged for suspicious activity can be subjected to additional checks. This tailored approach ensures that security measures don't hinder legitimate users while protecting the bank from fraud.

Regulatory Pressures: KYC & AML

Digital banks operate under the same regulatory frameworks as traditional financial institutions, meaning Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance are non-negotiable. These regulations mandate that banks verify the identity of their customers and monitor transactions to prevent illicit activities like money laundering, fraud and terrorist financing. While these checks are essential for maintaining compliance, they can introduce friction into the onboarding process, potentially driving away customers.

The complexity of global compliance further compounds the challenge. Digital banks often operate across multiple jurisdictions, each with its own regulatory requirements. This can lead to a disjointed onboarding experience, where customers face multiple verification steps that feel redundant or invasive. Failing to comply with KYC and AML regulations puts banks at risk of hefty fines, damages their reputation and erodes customer trust.

Many digital banks are turning to technology to meet regulatory demands without negatively impacting the user experience. Automation, machine learning and real-time data enrichment allow banks to meet compliance requirements more efficiently. By automating the KYC process and integrating global databases for screening, banks can verify customer identities quickly and accurately, ensuring compliance doesn't become a bottleneck in onboarding.

“By automating the KYC process, banks can verify customer identities quickly and accurately, ensuring compliance doesn't become a bottleneck in onboarding.”



“Cutting corners opens the door to fraud and puts banks at significant legal and financial risk.”

The Cost of Cutting Corners

The temptation to cut corners in digital onboarding is real. To accelerate growth and meet customer expectations, some banks may reduce the rigor of their verification processes, assuming that any resulting fraud losses can be absorbed, but the long-term consequences of this approach can be devastating.

Cutting corners opens the door to fraud and puts banks at significant legal and financial risk. Failing to vet customers properly during onboarding increases the likelihood of account takeovers, synthetic identity fraud and money laundering schemes. Each fraudulent account is a liability, leading to financial losses, regulatory fines and a damaged reputation. In today's highly regulated environment, digital banks simply cannot afford to take such risks.

In contrast, those who invest in comprehensive onboarding processes are better equipped to prevent fraud and avoid penalties. Technology solutions that leverage digital profiling, device fingerprinting and automated risk scoring can provide a deeper understanding of customer risk, allowing banks to flag high-risk users before they pose a threat. While these measures may introduce minor friction, the long-term benefits outweigh the potential costs of neglecting onboarding security.



Critical Challenges in Digital Banking Onboarding

From preventing fraud and managing customer expectations to overcoming technological and compliance hurdles, these challenges can impact the onboarding experience and operational efficiency. Below, we explore each of these critical challenges in greater detail.



Identifying Fraudsters & Bad Actors

A primary concern during onboarding is the ability to accurately identify fraudsters and bad actors before they gain access to the bank's system. Fraudsters often employ sophisticated tactics like synthetic identities, using stolen credentials and fabricated documents to create fraudulent accounts for illicit purposes. These bad actors usually operate multiple accounts simultaneously, exploiting digital platforms that lack stringent security measures.

To address this, digital banks must adopt fraud prevention strategies before costly KYC checks. One practical approach is leveraging data enrichment tools, which analyze various data points, such as IP addresses, device information and behavioral patterns, to create comprehensive digital profiles. By cross-referencing multiple data sources in real time, banks can identify suspicious activities and block fraudulent actors before they complete the onboarding process. This reduces exposure to fraud and ensures compliance with regulatory requirements, protecting the bank's reputation and bottom line.

Preventing Onboarding Fraud & Account Takeovers

Account takeovers (ATO) are a growing threat in digital banking, particularly during the onboarding phase. With ATOs, fraudsters use stolen credentials or exploit system vulnerabilities to gain control of legitimate customer accounts. Once in control, they execute unauthorized transactions, drain funds or use accounts for further fraudulent activities. With increased automated credential-stuffing attacks, banks with insufficient onboarding security face heightened risks.

To mitigate these risks, digital banks must implement device fingerprinting technology during onboarding. This technology analyzes the unique characteristics of a user's device and browser configuration. This data helps detect anomalies, such as attempts to log in from unrecognized devices or using proxies and emulators, which are common in ATOs. Banks can effectively prevent account takeovers without hindering legitimate customers' onboarding experience by adjusting security measures based on risk levels by using dynamic friction.



63%

quit the onboarding process, especially younger generations like Gen Z and Millennials, who expect to complete account set up within minutes.

Managing Customer Expectations for Speed and Convenience

Customers expect quick, convenient and seamless onboarding, but balancing the need for speed with thorough security checks is challenging. Research shows that over a quarter of customers abandon onboarding because it takes too long, while 63% quit due to friction or complexity⁵. This is especially pronounced among younger generations like Gen Z and Millennials, who expect to complete account set up within minutes.

To manage these expectations, digital banks can implement dynamic friction to tailor the verification process based on each user's risk profile. Low-risk users experience minimal friction, while higher-risk individuals may be asked to provide additional information. By reducing unnecessary steps for trustworthy users and streamlining the process, banks can enhance the user experience while maintaining robust security, ultimately lowering abandonment rates and improving customer satisfaction.

5 Trust Report: [63% of customers abandon digital bank onboarding](#)



High Onboarding Abandonment Rates

One of the primary reasons for high abandonment rates is the complexity of onboarding processes. Lengthy forms, cumbersome verification steps and unclear instructions can frustrate customers, particularly when expecting a fast, intuitive experience. Studies show that one in five users abandon onboarding simply because the process takes too long or is too confusing⁶. With each additional step, the likelihood of users abandoning the journey increases, resulting in a significant loss of potential customers. The issue is even more costly in Europe, where poor onboarding experiences are estimated to cost banks €6.43 billion, or \$6.95 billion annually⁷.

To combat high abandonment rates, banks must simplify the onboarding journey by adopting intuitive user interfaces and automation that streamline the process. Real-time digital profiling can pre-screen users before they hit the KYC stage, ensuring that only legitimate customers proceed and reducing friction. Digital banks can reduce abandonment rates and increase customer conversion by investing in a faster and more user-friendly onboarding process.

€6.43 billion

estimated annual cost of poor onboarding experiences for banks

Customer Experience Issues

Customer experience is at the heart of digital banking success. However, many users report frustration with overly complex processes. For digital banks, ensuring a positive first impression is critical to retaining new customers and building long-term relationships. To improve customer experience, banks should focus on streamlining identity verification processes and minimizing the number of steps involved in onboarding. Dynamic friction is one effective solution for this, as it ensures that security checks are tailored to the individual's risk level, reducing the chances of unnecessary delays.

⁶ Ibid.

⁷ Ibid.



Identification Verification Challenges

One of the biggest challenges in digital banking onboarding is ensuring accurate and secure identity verification (IDV). Customers often need to pay more attention to applications if they must present documents at a physical branch, which contradicts the convenience expected from a digital bank. Moreover, reliable remote IDV can be difficult to achieve while maintaining compliance with KYC and AML regulations, creating a tension between security and user-friendliness.

Banks must incorporate secure yet seamless remote identity verification solutions to overcome this hurdle. Data enrichment tools, such as IP and device data, can analyze a user's digital footprint to assess risk before proceeding with complete KYC checks. By filtering out high-risk individuals early, digital banks can prevent the costs associated with failed KYC checks, making processes more efficient and cost-effective.

“By filtering out high-risk individuals early, digital banks can prevent the costs associated with failed KYC checks...”

Technology & Integration Issues

The technology and integration aspects of onboarding present their own set of challenges. Ensuring new onboarding solutions integrate seamlessly across different digital platforms – including mobile, web and app-based services – is critical for consistent user experience. By adopting flexible, modular fraud prevention solutions designed to be easily implemented into existing systems, digital banks can stay agile while reducing the risk of technical disruptions or security gaps during onboarding.



Regulatory Compliance

Digital banks face a continually evolving regulatory landscape where adherence to KYC and AML requirements is mandatory. Strict compliance measures can introduce friction, slowing the onboarding process and frustrating potential customers. Banks that fail to comply face hefty fines and reputational damage, so implementing compliance solutions that don't impede user experience is essential.

To address this, many digital banks turn to automated compliance solutions that streamline KYC and AML processes. By ensuring compliance without compromising efficiency, digital banks can mitigate regulatory risks while offering a seamless onboarding experience.

Customer Understanding & Retention

A solid understanding of customer needs during onboarding is crucial for long-term retention. Being digital-first, today's digital banks' remote onboarding practices can make fostering relationships and personalizing the user experience harder, as banks may struggle to gather the insights necessary to tailor products and services to individual customers without face-to-face interactions.

Banks can better understand their customers during onboarding by leveraging data enrichment and digital profiling tools. SEON's solutions enable banks to assess customer behavior and preferences early in the process, allowing them to tailor offerings and build trust from the outset. This personalized approach enhances customer retention and fosters long-term relationships.

Competitive Pressures

The competitive landscape for digital banks is more intense than ever, with fintechs and challenger banks offering streamlined onboarding processes that appeal to tech-savvy consumers. Customers are also highly price-sensitive and willing to switch banks for better deals or seamless experiences. To stay competitive, digital banks must continually refine their onboarding processes to attract and retain customers.

SEON's dynamic friction solution helps digital banks offer fast and secure onboarding experiences that meet customer expectations while safeguarding against fraud. By optimizing onboarding efficiency and security, digital banks can stand out in a crowded market and maintain a competitive edge.



Strategic Solutions & Technology for Reducing Onboarding Risks

Reducing onboarding risks and tackling the above mentioned challenges requires a multifaceted approach integrating advanced technology with intelligent processes. Leveraging cutting-edge tools such as machine learning, AI and automation enables digital banks to streamline their onboarding processes while minimizing fraud and operational costs. A key strategy is to filter out fraudsters early, before they reach the costly KYC stage, allowing banks to maintain a seamless and secure experience for legitimate users.



Pre-KYC Checks: Screening Out Fraud Early

Pre-KYC checks are critical in identifying fraudsters and bad actors before they progress to the more resource-intensive and costly KYC (Know Your Customer) stage. Traditional KYC checks can incur high costs, especially when dealing with fraudulent accounts that fail verification. By implementing pre-KYC screening, digital banks can filter out suspicious users, reducing operational costs and ensuring that only legitimate users advance to verification. Tools like data enrichment and automated risk scoring systems allow banks to collect and analyze data points, such as device information, IP addresses and email histories. These early-stage checks can flag high-risk users before they move to the KYC stage, ensuring that banks avoid wasting resources on fraudsters while optimizing the onboarding process.

Data Enrichment for a Complete Picture

To accurately assess a user's legitimacy, digital banks must move beyond basic identity checks and build comprehensive digital profiles. Data enrichment is critical in this process, as it analyzes diverse data sources such as IP addresses, device fingerprints, email addresses and social media activity – giving banks a clearer understanding of their users and allowing for more effective fraud detection and risk assessment.

Banks can leverage real-time data enrichment to gain a granular view of user behavior and online presence. For example, identifying whether a user has an established digital footprint or recognizing unusual login patterns can help flag suspicious activity before it escalates into fraud.

Automated Risk Scoring Systems

Automated risk scoring systems have become an essential tool for digital banks. These systems analyze data in real time, assigning risk scores to users based on their behavior, digital footprint and other factors. By doing so, banks can quickly identify potential fraudsters without slowing down the onboarding process. Automated risk scoring allows for a more efficient and accurate assessment, flagging suspicious patterns and anomalies such as inconsistent device usage or high-risk IP addresses.

Manual reviews can introduce significant delays and inefficiencies, often resulting in higher operational costs. Automating the risk scoring process not only accelerates onboarding but also improves fraud detection accuracy. By reducing the need for manual checks, digital banks can allocate resources more effectively, focusing on growth strategies rather than time-consuming administrative tasks.

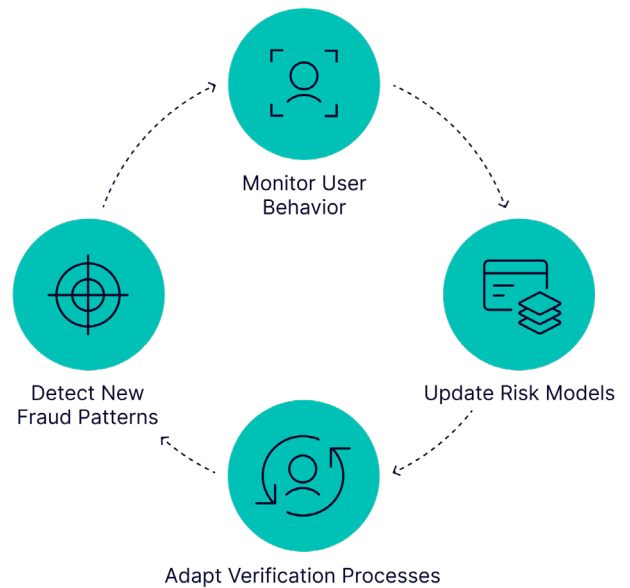


These systems dynamically adjust the level of scrutiny based on a user's risk profile, applying more stringent checks to higher-risk individuals while allowing legitimate users to proceed with minimal friction. By automating the risk assessment process, banks can reduce the need for manual reviews, streamline the onboarding process and lower operational costs while maintaining a high level of security.

Machine Learning & AI

Machine learning and AI enhance risk detection during onboarding by analyzing vast data and identifying subtle patterns and anomalies that traditional methods often overlook. These technologies continuously learn from new data, improving their accuracy in fraud detection over time. By incorporating machine learning into onboarding, digital banks can identify emerging fraud tactics and proactively adjust their security measures.

AI-powered systems can make instant decisions, flagging high-risk users while allowing low-risk users to proceed without friction. This real-time adaptability enhances security and ensures that the onboarding process remains efficient and user-friendly for genuine customers. These systems also allow for the implementation of custom rules and scoring models, enabling financial institutions to create bespoke risk assessments tailored to their specific needs and regulatory requirements. The combination of customization and the ability to process and learn from large amounts of data allows for increasingly sophisticated and accurate fraud detection, striking an optimal balance between security and user experience in the onboarding process.



Continuous Monitoring: Real-Time Adaptation

Continuous Monitoring & Adaptation

In a constantly evolving fraud landscape, static security measures are insufficient. Continuous monitoring and adaptation are vital for maintaining a secure onboarding process. Once users are onboarded, continuous monitoring of their behavior, device usage and transaction patterns allows banks to detect potential fraud even after the initial verification phase.

By adapting to emerging fraud tactics, machine learning and AI can update real-time risk models, ensuring the onboarding process remains secure. Continuous monitoring throughout the customer lifecycle provides additional protection, safeguarding digital banks against ongoing threats while enhancing operational efficiency.



A Smart Approach to Efficient Onboarding

In digital banking, delivering a fast yet secure onboarding experience is essential for attracting and retaining customers. The challenge lies in minimizing friction for legitimate users while keeping fraudsters at bay. By using advanced technologies like dynamic friction, device fingerprinting and real-time data enrichment, businesses can achieve a delicate balance between user experience and security. These solutions offer a streamlined approach to onboarding, reducing operational costs, improving efficiency and ensuring safety from fraudulent activities.



“By tracking and analyzing device and browser data in real time, companies can detect suspicious behavior before it escalates. “

Dynamic Friction: Tailoring Security to Risk Levels

Instead of applying the same security measures to every user, dynamic friction adjusts the level of verification based on the assessed risk. Low-risk users experience minimal checks, allowing them to complete the onboarding process quickly, while higher-risk users are flagged for further scrutiny.

This flexibility ensures that the onboarding process remains smooth for genuine customers while identifying potential threats early on. By evaluating a range of data points, including device data, IP addresses and user behavior, dynamic friction applies stringent measures only when necessary, creating an efficient process that doesn't compromise security.

Device Fingerprinting and Browser Data

Each device leaves a distinct digital fingerprint comprising details like operating system, browser settings and hardware configuration. This allows businesses to detect anomalies such as multiple accounts being created from the same device or using proxies and emulators, which are common signs of fraudulent activity.

By tracking and analyzing device and browser data in real-time, companies can detect suspicious behavior before it escalates. Device fingerprinting helps prevent account takeovers and multi-accounting fraud and ensures legitimate users can onboard seamlessly. Detecting and blocking potential fraud at this stage helps businesses create a safer onboarding process without unnecessary friction for honest customers.



“This process allows businesses to flag suspicious patterns early in the onboarding journey...”

Real-Time Data Enrichment for Fraud Prevention

Traditional onboarding often relies on user-provided information, which fraudsters can easily manipulate. Real-time data enrichment taps into various external sources, such as email histories, social media profiles and IP geolocation data, to create a fuller picture of the user’s digital footprint.

This process allows businesses to flag suspicious patterns early in the onboarding journey, such as users lacking an online presence or displaying unusual geographical activity. Real-time analysis of these data points enables companies to prevent fraudsters from progressing to costly verification stages, helping cut operational costs and improving onboarding efficiency. At the same time, legitimate users benefit from a smoother experience, as they are fast-tracked through the process with minimal friction.



Shaping Tomorrow: What's Ahead for Digital Banks?



Evolving Threats in the Digital Banking Landscape

Digital banks' threats are becoming more complex and more challenging to detect. Fraudsters are deploying more advanced techniques, from synthetic identity fraud to automated credential-stuffing attacks, making it crucial for digital banks to implement robust defense mechanisms. Some growing risks include account takeovers, money laundering schemes and phishing scams. These evolving threats highlight the need for constant vigilance and adaptation in onboarding.

Digital banks must continuously refine their fraud detection strategies to keep up with these sophisticated attacks. This includes leveraging machine learning models to identify emerging fraud patterns, automating processes to reduce human error and ensuring real-time data analysis to detect suspicious behavior early on. Those who successfully combat these threats will protect their assets and build stronger relationships with customers who demand secure, frictionless experiences.

How Technology Will Shape the Future of Onboarding

Technology will be the driving force behind the future of onboarding in digital banking. Artificial intelligence, machine learning and real-time data enrichment will enhance fraud detection and deliver a seamless user experience. As these technologies continue to advance, banks can automate even more aspects of onboarding, allowing for quicker verifications, more intelligent decision-making and reduced costs associated with manual reviews.

Moreover, continuous monitoring of customer activity post-onboarding will become a standard practice, adding an extra layer of protection that adapts to evolving risks. Dynamic friction will ensure that onboarding remains efficient for legitimate users while fraudsters face increasingly stringent checks. In the coming years, we can expect a more integrated approach to fraud prevention and onboarding, where data-driven insights, behavioral analysis and AI-based decision-making become cornerstones of the process. The future of onboarding lies in its ability to be both secure and customer-centric – allowing digital banks to grow, innovate and meet the challenges of tomorrow head-on.

