Top Considerations for Online Customer Onboarding in Financial Services

Top Considerations for Online Customer Onboarding in Financial Services

What's driving digital banking?

Digital banking is growing. In 2019, 71% of UK consumers had used at least two online financial services, up from 14% in 2015. In the US, adoption grew to 46% from 17%[1]. Savings, payments, borrowing and budgeting are all moving online.

That growth is being driven by a number of factors, with customer experience and convenience appearing high on the list. To compete successfully, financial institutions must ensure that the customer onboarding process for accessing digital services is as effortless as possible, or risk falling at the first hurdle. So how do banks get the all-important onboarding experience right and still meet your KYC obligations?

1 EY FinTech Adoption Index

1 Who's coming into your business?

When onboarding new customers, financial institutions firstly need to know that the person applying for the account is a genuine person, and that they intend to use the account for legitimate purposes. This is a requirement of the Know Your Customer (KYC) guidelines, created to prevent money-laundering and counter terrorist financing.

As digital banking has grown, so has the attention of online criminals. New account fraud (NAF) is a particular threat – in 2018, 3.2 million US consumers were affected by NAF, either through:

- complete impersonation, where criminals acquire stolen identity data to apply for credit cards and other financial services
- synthetic identity creation, where criminals use a combination of potentially valid social security numbers and accompanying false personally identifiable information to achieve the same end

By using Genuine Presence Assurance, financial institutions can verify remotely that new customers are bona fide applicants and not fraudsters trying to spoof their way through the account creation process. Facial biometric authentication technology enables banks to check that an applicant is the right person (matching the photo on the ID document), a real person (not a photograph or mask or other artefact), and authenticating themselves right now (not a pre-recorded and replayed, deepfake video or other). This provides protection against fraud while keeping the process simple and effortless for the user.

2 Take advantage of regulatory changes

Over recent years, banks have faced an increase in regulations, with greater demands on resources needed to keep up with compliance. However, many of these regulations have also opened up new opportunities to enable organizations to complete identity and other checks remotely. In Europe, the 5th Anti-Money Laundering Directive (5AMLD) allows remote verification against trusted sources, while Canada, Japan, Hong Kong, Malaysia and others have also updated guidance based on Financial Action Task Force (FATF) guidelines.

This means that financial institutions are able to offer digital services to customers in a way that maximizes

3 Deliver usability for customer satisfaction

You don't get a second chance to make a first impression. If a customer has decided to open an account with you, it is imperative that the process is as effortless as possible. Today's customers expect to be able to complete even the most secure processes online without going into a branch or contacting a call center, and they expect that process to be simple.

36% of financial institutions have lost a customer due to poor customer experience. Yet there's no doubt that financial institutions face a balancing act between ensuring that the correct and necessary checks are completed with high degrees of accuracy, while keeping it straight-forward for the user. However, innovation in technology means that the process of onboarding is becoming increasingly more seamless for both the customer and the enterprise.

There are also cost savings to be realised. According to research from McKinsey, an improved onboarding experience can deliver a 90% reduction in processing costs. Challenger banks have embraced these efficiencies and are setting a precedent for effortless, automated customer experiences that deliver customer satisfaction and streamlined operations.

So how can banks strike the balance of usability with security and privacy? iProov technology has been designed to deliver an effortless authentication experience. Users do not need to actively move or read out words or numbers in order to prove liveness - a simple illumination confirms that they are the right person, a real person, and genuinely present right now. iProov works on any device or platform, ensuring accessibility and inclusivity, and can be delivered via kiosks as well as to remote users via their personal devices for consistency.

Case study: Knab

Read more >

Challenge: Offer secure, compliant, effortless online onboarding and authentication.

Solution: Genuine Presence Assurance for onboarding, strong customer authentication (SCA), re-binding and step-up authentication.

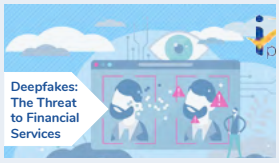
Success: Replaced the need for costly tokens, introducing a fully automated process for customers.

4 Make security a priority

The more technology advances, with organizations moving to online channels and processes, the more advanced hackers become in finding new ways to attack individuals and enterprises. The coronavirus pandemic has contributed to a marked increase in fraud; as of May 28, 2020, according to the FBI, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (about 320,000) as they had for the whole of 2019 (about 400,000).

The introduction of AI and machine learning has seen incredible advances in technology in recent years. However, machine-driven cyber attacks have also accelerated at alarming rates and the threat they pose to the financial services industry is enormous. Regulated organizations need to put machine-driven security in place, that can protect against such large-scale machine-powered criminal activity.

Genuine Presence Assurance technology from iProov provides sustainable security, to continually update your protection against the most sophisticated AI-driven criminal tactics. iProov technology protects against both presentation attacks, where a photo or video is presented to the camera of a device, and replay attacks, where hackers inject a pre-recorded or deepfake video into the software in an attempt to gain access.



77% of cyber security experts in financial services say they are concerned about fraudulent use of deepfakes. Read more about the threat of deepfakes in our report.

Read Report >

5 Privacy concerns from end users must be addressed

In a recent iProov survey, 91% of consumers in the US and UK said that they care about data privacy, citing the risks of identity and money theft as key concerns.

The protection of your customers' identity data is critically important to attracting their business and maintaining their loyalty. Financial institutions need to demonstrate visible privacy protection when onboarding and authenticating users. This creates trust and will avoid huge fines from regulators from potential privacy and data breaches.

The iProov solution for onboarding and authentication offers the highest levels of data privacy protection, being both GDPR compliant and eIDAS conformant. This means that your customers are getting usability, security and privacy in a single unified package.

About iProov

Founded in 2011, iProov is the world leader in online facial biometric authentication, working with governments, banks and other enterprises to remotely verify customer identity. Used for onboarding, log-on, and authentication, customers include the US Department of Homeland Security, the UK Home Office, Knab, Rabobank, ING and others.

iProov's unique patented technology provides **Genuine Presence Assurance**, ensuring that an online customer is the right person, a real person, and authenticating right now. This protects against spoof attacks from photos, videos, masks, replay attacks, and the emerging threat of deepfakes.

For more information or to request a demo, please see www.iproov.com or follow us on Twitter or LinkedIn.

For more information on how to assure the genuine presence of the **right** person, **real** person, authenticating **right** now contact us now at: **enquiries@iproov.com**

enquiries@iproov.com

+44 (0)20 7993 2379

iproov.com