future identity

VOX POP

Getting identity right from the start

Is secure digital onboarding the key to financial crime prevention?

Powered by:

iproov

Contents

Introduction

Laura Camplisson,
Future Identity Portfolio Lead,
VC Innovations

Every year, businesses across the globe lose significant revenue to financial crime. The human cost, meanwhile, is immeasurable. Financial institutions are under growing pressure to tackle fraud, money laundering and corruption, to avoid facing heavy fines and irreparable reputational damage.

Following the outbreak of the global pandemic, and the resulting national lockdowns, financial institutions witnessed a rise in illicit activity, corresponding with increased use of digital services by legitimate customers. In 2020, the UK alone saw internet banking fraud increase by **117%** and mobile banking fraud by **78%**.

The more financial services are digitised, the more points of entry there are for fraudsters, who make use of all tools at their disposal to target IT systems, employees, and customers. Financial institutions must defend against increased attacks from automated bots, sophisticated synthetic IDs used to pass KYC checks, and clever scripts designed to trick customers into handing over account access.

All too often, fraud prevention methods rely on quick fixes and reactive measures, leaving financial institutions struggling to gain the upper hand. Once a fraudster has successfully created an account using a synthetic or stolen identity, they are able to re-authenticate for future transactions and build a seemingly legitimate credit history.

Meanwhile, if a legitimate customer is not onboarded with a robust identity profile, then any future authentications are left vulnerable to attack. Fragmented, knowledge-based measures to prevent account takeover have only served to generate more data for fraudsters to take advantage of, as well as creating easily exploited customer confusion.

Established methods of financial crime prevention are not sustainable in a digital world. But if a strong verification process can filter out bots, bad actors, and synthetic IDs before they enter a system, could onboarding be the key? Is the customer identity created at onboarding not the most crucial element to the strength of authentication?

This Vox Pop report captures the views of senior industry leaders as they share how they are tackling financial crime in a changing world and whether the key to identity is **getting it right from the start.**

Sol Enenmoh,
Director - Group Digitalisation
HSBC

What potential points of friction exist throughout the customer onboarding journey?

Frustratingly, there are still instances where manual, human intervention is used to validate customer identity information. Excessive back-office processes like this result in a fragmented journey and create friction for the customer.

Looking at your classic digital banking journeys, usually in the retail space, friction often exists due to journey designs which interrupt the journey flow. Requiring the user to leave one screen or device, do something on another screen or device and then juggle their way back to the former device, creates a lot of friction for a potential customer. Especially if they don't have the appropriate authentication modes to hand at the time.

Can you describe the challenges financial institutions face in tackling financial crime and fraud?

The rise of cyber attacks on financial institutions is widely acknowledged but not commonly understood. Many organisations find themselves playing catchup against hacks or ransomware attacks, often only reacting to invest in proactive defences after a nasty incident has occurred. At an individual level, there's still a lot more coaching and guidance needed to educate consumers against very common (but sadly still successful) scams, such as phishing via text, cold calling, or identity fraud linked to the oversharing of personal information on social media.

"In the retail banking space, friction often exists due to journey designs which interrupt the journey flow, asking the user to move to another screen or device."

Over the past two years, have you seen any change in demand for end-to-end digital services?

Demand from customers has heightened, but so has internal demand as part of the overall digitalisation of the enterprise. Looking at the future of the employee onboarding journey from prospective new talent through to new colleague, we picture an ID that builds, learns, and grows with the employee profile.

A credential established when someone converts as a prospective candidate, can then be utilised when they join the organisation, and then for future related assets such as authentication to gain access to personal demographics, salary payments and development classifications.

How do you see the process of identity verification evolving as a part of the overall customer lifecycle?

Any transformation of identity verification will form part of the broader transformation of the customer journey from prospect through to retention. Many financial providers are looking to recentre the decisioning process for onboarding prospective customers around life events or experiences.

Asking what a customer needs will be key to this approach, understanding that someone hasn't come to your financial institution to ask for a loan, they've come because they need the funds to make home improvements for example. This approach will be especially important within the underserved fiscal space, where many prospective customers may not have the 'standard' ID assets we assume they will, for example those new to the country.

"The rise of cyber attacks on financial institutions is widely acknowledged but not commonly understood."

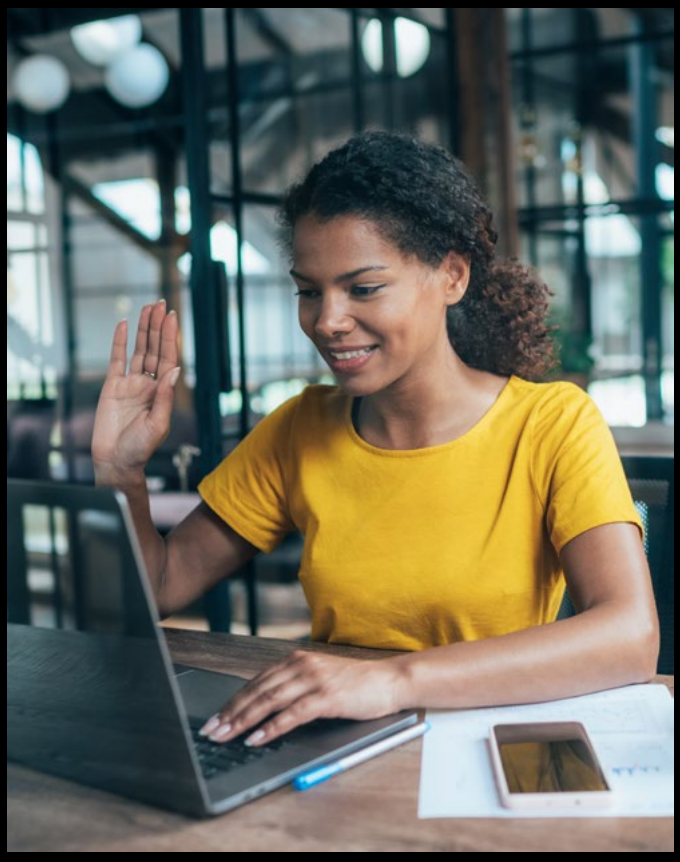
Automated intelligence will make the customer journey increasingly proactive, going from show me and guide me practices, to automated actions based on initial consumer sign up preferences and organic understanding of user identity. That being said, security will reach a crunch point. People have password fatigue, but different levels of security will be needed for different services. I may be ok with using voice biometrics to ask Alexa my bank balance but will want it to be much harder for anyone to make a withdrawal!

What do you think the bank of the future will look like?

An entity which builds for consumer experience first, is technically secure, can understand and explore data optionality, and move with agility to exploit emerging trends. Open finance is going to be a game changer, with entrants not currently classed as part of the fiscal ecosystem enabled to provide financial services that meet evolving consumer needs. Trust will be an even bigger deal, with consumers enrolling with whichever entities they deem most credible and secure.

The pandemic has accelerated a channel shift away from physical banking to mobile. In turn, this has opened broader willingness for adoption of new channels and functionality across blockchain and distributed ledgers, IOT and the metaverse. Lastly data ethics governance will come into play, to ensure that unconscious bias is minimised across the customer journey.

"Open finance is going to be a game changer. Trust will be an even bigger deal, with consumers enrolling with whichever entities they deem most secure."



"Security will reach a crunch point. People have password fatigue."

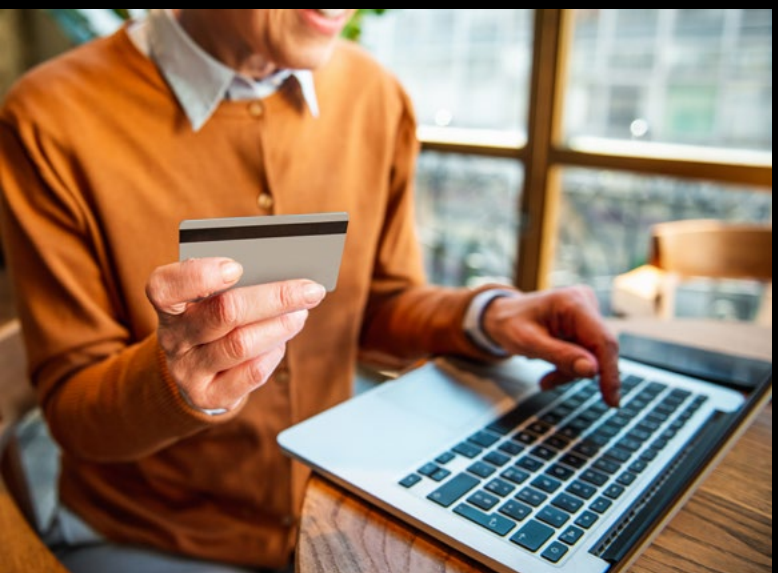
Sergei Fedorov
Head of Onboarding,
ANNA Money

What potential points of friction exist throughout the customer onboarding journey?

There are two major points. The first is when the customer needs to provide/upload/take a picture of any file or document, be it a passport, driving licence, utility bill, or bank statement. Usually, people don't sit surrounded by all these pieces of paper or have a folder with all the files in quick access. So they need to take care to find and provide what is required, which naturally leads to a drop in conversions. The second, less obvious, but very important factor, is the number of questions and their clarity. People want to use your service, not go through endless onboarding questions and give away tons of information.

Can you describe the challenges financial institutions face in tackling financial crime and fraud?

Financial providers are under pressure to prevent fraud and scams, as not doing so can lead to the shutting down of their operations, and allow criminals to damage the economy and ruin people's lives. It is incredibly important to use sophisticated verification techniques and, even better, a whole orchestra of techniques as criminals quickly learn how to bypass certain checks. The sharing of knowledge and data between financial institutions will be key in helping to secure onboarding and prevent financial crime.



"People want to use your service, not go through endless onboarding questions and give away tons of information."

Over the past two years, have you seen any change in demand for end-to-end digital services?

It would have been impossible not to notice the shift working in the financial sector. With the global pandemic shutting down offline points of sale and forcing people to work from home, end-to-end digital provision of services became the only way to move forward, so demand drastically increased. Huge numbers of new companies providing digital services have emerged, while established businesses have looked to expand their capabilities to offer digital onboarding to customers.

How do you see the process of identity verification evolving as a part of the overall customer lifecycle?

We are already seeing financial institutions start to embrace reusable credentials, leveraging the identity created at onboarding for future authentication. This looks like a natural progression. With everything moving towards digitalisation, all those paper IDs and POAs will disappear sooner, rather than later.

On top of that, I think governments should play a huge part in the future of identity, by verifying entities and individuals and providing this status to other authorities. This is a very serious topic, which raises a lot of security concerns due to the sensitivity of the information involved. This in turn, makes it a really interesting challenge.

"Banking will become just a part of people's identity."

What do you think the bank of the future will look like?

In the future a ‘bank’ will be a platform that connects people to various services and financial products depending on their needs and financial capabilities. In other words, banking services should be APIs and customers should have to worry less (or not at all) about credits, overdrafts, fees, BNPL, and other services. Very briefly, banking will become just a part of people’s identity.

“With everything moving towards digitalisation, all those paper IDs and POAs will disappear sooner, rather than later.”

Anouk Moll
Innovation Manager,
ABN AMRO

What potential points of friction exist throughout the customer onboarding journey?

The process of onboarding for many digital platforms is a trade-off between a frictionless onboarding flow, which enables growth but tolerates higher levels of fraud, and a more thorough onboarding flow, which reduces fraud but stifles growth given the friction involved in the onboarding flow. The more steps a user has to take to use a service, the more likely that user is to drop.

This behaviour is understandable – if you want to use a scooter sharing service to enable you to go somewhere for example, you would be annoyed if this were to take hours to complete. You will likely divert to another service. Points of friction are for instance manually typing in information that can be easily scanned from documents, or a slow approval of digitally scanned documents. AI and automatisation tools can help to speed up this process immensely.

Can you describe the challenges financial institutions face in tackling financial crime and fraud?

Like most businesses, financial institutions are increasingly digitalising their services to keep up with market demands. The pandemic played a huge role in speeding up this digitalisation, as physical bank branches had to close due to lockdowns. ABN AMRO has invested heavily over the last couple of years to design robust digital systems to automatically detect fraudulent transactions. State of the art tools are used to constantly analyse suspicious user behaviour.

"Regulations can be complicated for a business to adhere to, in particular start-ups who often don't have the resources to consult GDPR consultants."

"The more steps a user has to take to use a service, the more likely that user is to drop."

Over the past two years, have you seen any change in demand for end-to-end digital services?

We have been witness to both the increase in demand for digital services and the challenges of providing such services, especially within heavily regulated markets. With the rise of digitalisation and privacy concerns we are now seeing the introduction of more legal frameworks to protect consumers in other markets in Europe. These regulations can be complicated for a business to adhere to, in particular start-ups who often don't have the resources to consult GDPR consultants or build digital services to adhere to the regulatory requirements.

As a bank, we can play a huge role by building products for these businesses. As we are compliant with the strictest privacy laws, it is easier for us to build privacy and legally compliant services to offer to digital platforms. Such as ID & pay, a solution incubated within ABN AMRO, where we can store identity data compliant to all GDPR and privacy laws, and offer this service to platforms without exposing the users data.

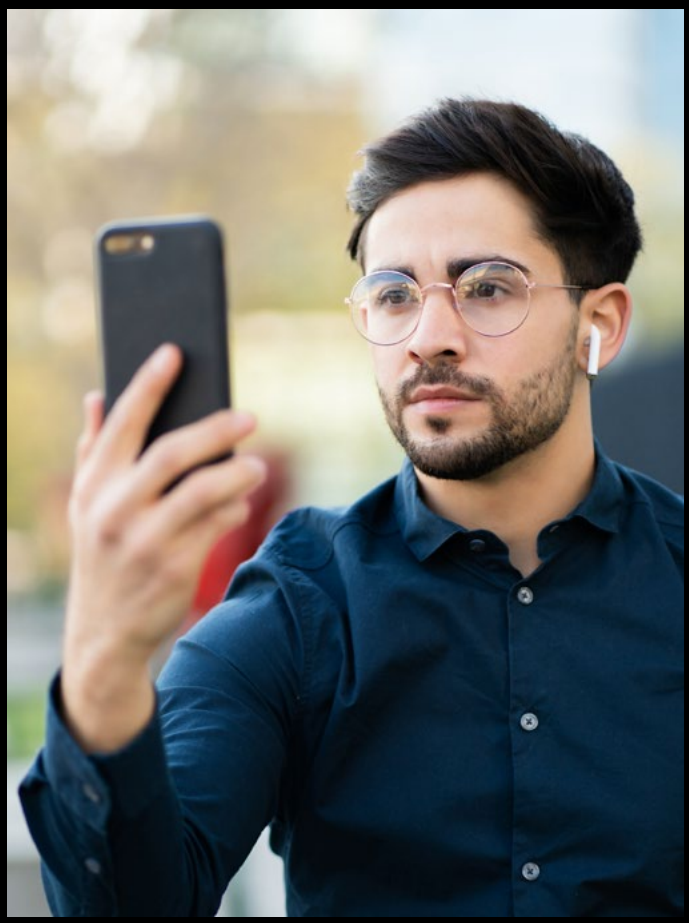
How do you see the process of identity verification evolving as a part of the overall customer lifecycle?

It is evolving at a fast rate - the European Union is now working on digital ID services to make it easy for users to identify themselves digitally. We are seeing a lot of platforms struggle with onboarding and payments. By taking a centralised approach where users make a single account that they can then use to authenticate themselves with various platforms, businesses can take away the pain of a user having to go through a long onboarding flow every time. This is also a lot safer from a user perspective. Rather than sharing your ID with 5 different services, you store it in a single secure digital environment and simply authenticate who can have access to it. As a bank, the benefit of taking the lead on this processes is that we adhere to the strictest privacy laws, meaning platforms can rely on our onboarding without having to store identity data themselves.

What do you think the bank of the future will look like?

Digital first and frictionless. The rise of neo banks is a clear sign of users wanting to have seamless digital processes. However, I would predict banks will still have to keep a sense of personal contact with the user. Our strategy at ABN AMRO is to be a 'personal bank in the digital age'. By introducing video calls with clients, they can still ask questions to an actual person rather than just having an in app chat. We have updated all our services to become a digital bank, but without losing our personal touch.

"A single account that a customer can then use to authenticate themselves with various platforms, can take away the pain of having to go through a long onboarding flow every time."



Conclusion

The way we access financial services is undeniably changing. Whether out of necessity in the face of an unprecedented global pandemic, or as a response to consumer demand, the number of digital-only financial providers and established financial institutions offering digital services, has grown rapidly.

And this is not a trend contained only to the financial sector. Across almost every industry, customers and employees are increasingly keen to access services remotely. Businesses can no longer rely on the need for in-person verification and so, with the threat of fraud never far behind, the need for secure digital identity proofing cannot be ignored.

"We are now seeing financial institutions of all shapes and sizes look at implementing reusable credentials."

However, the line between making access convenient and keeping services secure, is extremely fine. And a fragmented digital verification journey will result in a high percentage of dropouts from potential customers. Requiring customers to provide pieces of evidence they may not have to hand, to manually input complex information, or to leave one screen and switch to another, for example, all create unwelcome friction.

Financial institutions need to understand the action a customer wants to take and support them through the required verification and authentication steps to complete this digitally. Crucially the needs of those customers who are at risk of exclusion from digital access, or face challenges which call for additional assistance, have to be accounted for. This is by no means a static process as customer needs will continually evolve over time.

As a result, and as the Vox Pop interviews within this report demonstrate, we are now seeing financial institutions of all shapes and sizes look at implementing reusable credentials to deliver a streamlined verification and authentication journey. Getting identity right from the start by supporting customers with a credential which can then be used for future access to a whole range of services, drastically simplifies the user experience.

This approach also enables a far more proactive approach to mitigating risk and making decisions about customers, reducing the risk of fraud further down the line. And by embracing end-to-end digital identity, financial institutions can alleviate the operational burden of customer due diligence and allow for human resources to focus instead on relationship building or support for those cases which cannot be managed digitally.

The contributors to this report predict that the bank of the future will be agile, user centric, digital-first and will operate as a platform to connect customers to the products and services they need most. From onboarding to wherever a user's journey takes them, digital identity will play a key role in enabling this vision.

"The line between making access convenient for customers and keeping services secure, is extremely fine."

future identity

ABOUT IPROOV

iProov is the world leader in using biometric face authentication to confirm that an individual is genuinely present during an online interaction. iProov's Genuine Presence Assurance technology is used by governments, banks, and other enterprises globally to verify that a user on a mobile device, computer or unsupervised kiosk is the right person, a real person, and, critically, that they are authenticating right now – not a digitally injected attack using deepfakes or other synthetic media. Established in 2012, iProov is headquartered in London with offices in Maryland and Singapore.

iProov
contact@iproov.com
iproov.com

Laura Camplisson
Future Identity Portfolio Lead,
VC Innovations
laura.camplisson@vcinnovations.co.uk
thefutureidentity.com

Powered by:

iproov