callsign®

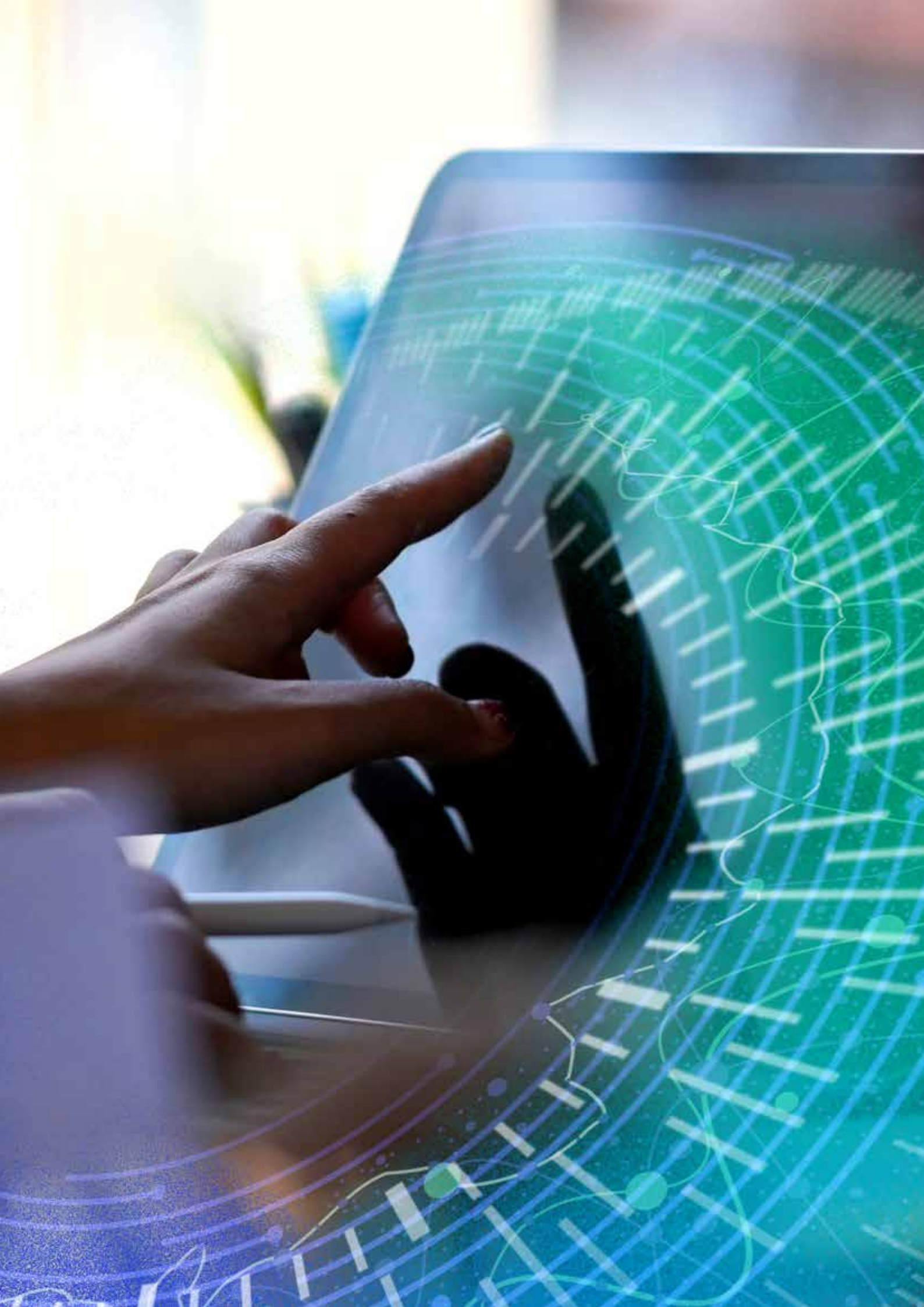
MATURITY PATHWAYS SERIES

BANKING

Maturity Pathway

Understand the technologies and processes required at each stage of your digital transformation journey

Contents



INTRO TITLE

CURRENT LANDSCAPE

The Pathway to digital trust

When it comes to digital identification and fraud prevention, banks and financial institutions face a number of complex challenges.

A lucrative target for increasingly frequent and sophisticated fraud attacks, they're also heavily regulated, with customers who expect total security alongside friction-free experiences.

While banks share the same strategic customer-based business goals as many other organizations – loyalty, reducing costs, trust, market share – their identity requirements and customer dynamics are unique. That makes their challenges equally unique.

The Pathway to success – and digital leadership – is as individual as your business. No two businesses are alike; and resultingly, strategic priorities will vary from organization to organization. Finding a solution that aligns with them means first understanding what those priorities are, and what they mean to your business.

In this e-book, we've mapped out a simple journey to digital leadership for any financial organization: the Maturity Pathway.

The challenges

Compliance
Government intervention in the financial service industry is extremely common. Banks and other financial services organizations are subject to strong and highly visible regulatory demands.

Fraud risk
Anything involving money has a risk aspect, with bad actors constantly working on an industrial scale to access legitimate customers' accounts, data, and assets.

Customer experience
Creating truly positive user experiences is too often viewed as just a happy bonus. Digital disruption is also changing loyalty drivers for consumers. Convenience is their highest priority; smooth user journeys are an expectation, not an option.

Cost
Relying on insecure authentication methods such as SMS OTPs will drive up costs. But there are other factors to consider: if outdated security methods result in a breach, the loss of reputation, trust and customers may have an even bigger impact than the resulting fines.

How to use the Maturity Pathway

Progressing along the Maturity Pathway will bring increasingly robust fraud protection capabilities and more engaging user experiences, while fulfilling all of your regulatory responsibilities.

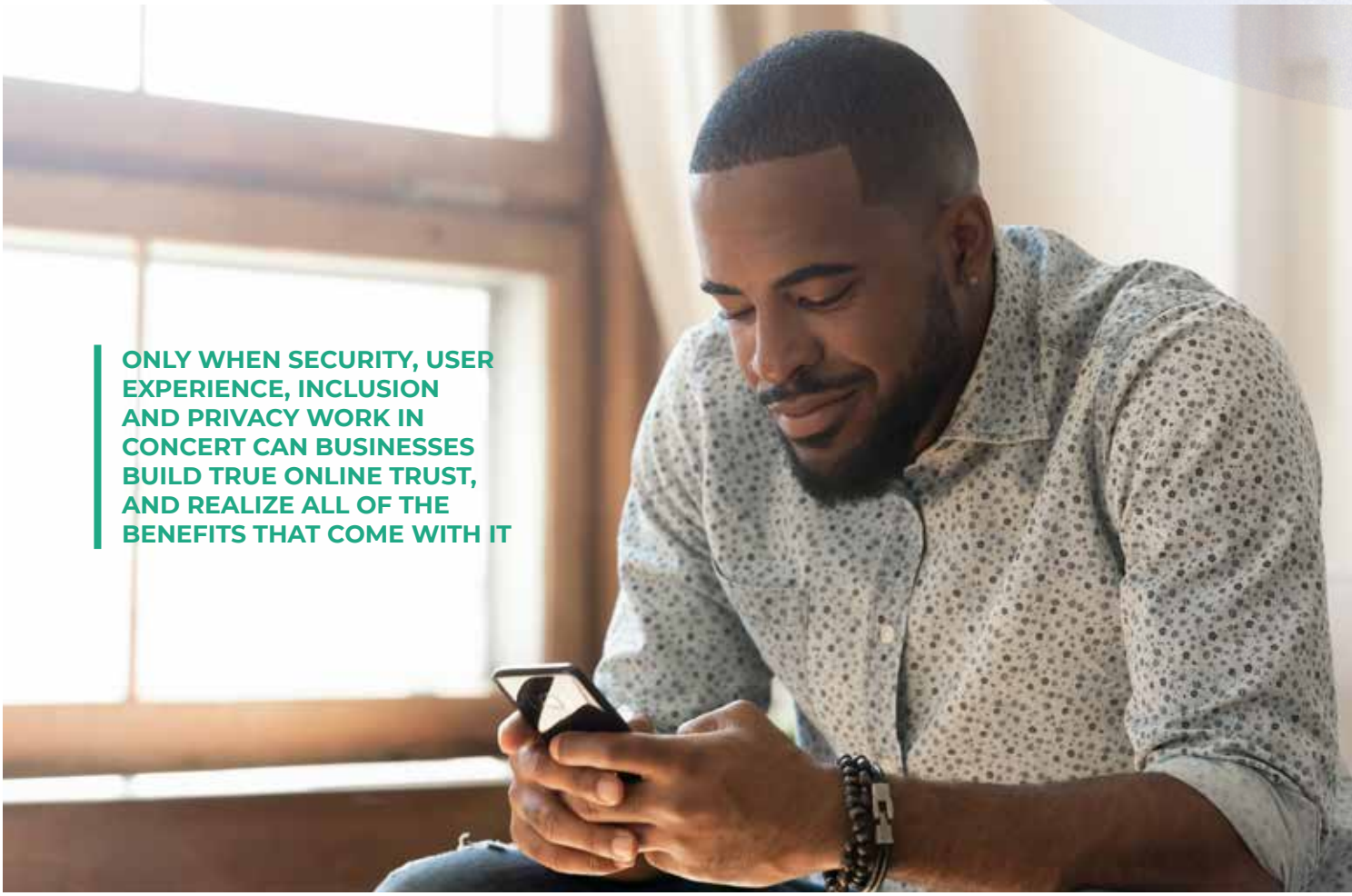
Technology has fundamentally changed how banks interact with customers. Just twenty years ago, the only way to open a bank account was to visit a branch in person, with supporting documents; now, some banks are entirely branchless and allow customers to sign up online in a matter of minutes.

The organizations that have adapted to the digital-first environment are the ones who are reaping significant benefits. But how does a business progress on its journey?

The Maturity Pathway is designed to give you a clear starting point and progression plan, along with guidance on the business attributes and tech capabilities you'll need to develop at each stage.

Each stage of the Maturity Pathway is a Milestone. And whether you're sitting at the very first one, and are looking to modernize fast, or you're just a step away from completing the Pathway, we will help you optimize where you're currently at and guide you through the steps that you can take to move onto the next Milestone – and ultimately, to provide seamless and secure online experiences for your customers.

On the next page we outline the four Milestones that will lead you to digital trust.



ONLY WHEN SECURITY, USER EXPERIENCE, INCLUSION AND PRIVACY WORK IN CONCERT CAN BUSINESSES BUILD TRUE ONLINE TRUST, AND REALIZE ALL OF THE BENEFITS THAT COME WITH IT

Your Maturity Pathway

PHYSICAL FIRST

ESTABLISH DIGITAL CHANNELS

ATTRIBUTES

No personalization

In-person account creation

Compliance risk from siloed data capture & manual processes

Disjointed / non-collaborative operating models

CHALLENGES & RISKS

Application fraud & synthetic IDs

New and existing customer retention concerns

Paper-based processes leading to compliance risks (privacy and regulatory)

Regulatory changes

TECHNOLOGY

Traditional authentication (SMS, OTPs, hard tokens) (minimum)

Behavioral biometrics (preferred)

DIGITAL TRANSACTIONS

IMPROVE FRAUD PREVENTION

ATTRIBUTES

Minimal customer data integration / personalization

Hybrid on- and offline account creation

Compliance challenges with legacy systems

Some synergy between fraud, cyber and digital teams

CHALLENGES & RISKS

Account takeover (lost / stolen / intercepted credentials, SS7 attacks, credential stuffing etc.)

Regulatory changes

Over-reliance on insecure & expensive OOB authentication

Card Not Present payment issues (declines / fraud)

TECHNOLOGY

Threat detection

Basic ID&V capability

Rules engine

Device fingerprinting

Payment fraud dectection

(Comprehensive) AI-powered passive authentication capaibilty

CUSTOMER-CENTRIC

BUILD ON CUSTOMER EXPERIENCE

ATTRIBUTES

Omnichannel banking services

Differentiated customer experience online

Automated application and approval services

Compliance & data security by design

Proactive collaboration between teams

CHALLENGES & RISKS

Scams & social engineering

Cross-channel deficiencies and utilization of data

Cross of settlement and payment service provision

Regulatory changes

TECHNOLOGY

Code-free orchestration capabilites

Location analysis

Third-party data integration (e.g. cellular network operator)

Layered intelligence signals

RAT and social engineering detection

PORTABLE IDENTITY

INVEST IN IDENTITY AS A SERVICE

ATTRIBUTES

Streamlined interbank and retail processes / services

Hyper-personalized experiences with portable omnichannel digital IDs (IDaaS)

Harmonized operational priorities with accountability spanning departments

CHALLENGES & RISKS

Evolution of fraud attacks and new vectors

New compliance risks (privacy and regulatory

TECHNOLOGY

Omnichannel digital identity provider

MODERNIZE ME

Physical first

Despite the rapid evolution and adoption of digital technologies, physical, in-person banking is very much a reality in many places today.

Often, an organization's only digital presence is a website that directs customers to a contact center or a physical branch. There is no way for customers to interact digitally with the bank.

In-branch service may be viewed as more personal, and might appeal to less tech-savvy demographics; but these perceived advantages have to be weighed up against the disadvantages – which are significant. In an increasingly competitive market, a solely physical approach to service provision makes it difficult to win and retain new customers.

Compliance

Identification will be reliant on highly manual, human-centric legacy processes. Onboarding will see customers visit a branch with proof of identity and address; while interactions like loan applications will involve a physical or telephone conversation in which customers will be typically authenticated by physical documents or knowledge-based questions such as their date of birth.

From a compliance perspective, this leaves you with a major headache: with a lack of live verification, paper-based authentication is extremely expensive. Meeting the regulators' demands when it comes to KYC and AML, legislation will be manual, expensive, and fraught with potential losses and errors.

FOCUS ON:

Digital channels

ATTRIBUTES:

- Reliance on telephone banking and in-person customer service
- No personalization
- In-person account creation
- Compliance risk from siloed data capture & manual processes
- Disjointed / non-collaborative operating models

Payment verifications for Card Not Present (CNP) transactions are also likely to be completely reliant on systems and processes that are separate from the bank's own channel. Not only does this add complexity, but in some geographies, it could present a further compliance issue particularly as payment regulation such as Europe's PSD2 take hold.

Fraud & risk

With no live digital authentication, organizations are forced to rely on highly vulnerable approaches such as knowledge-based authentication. Institutions at this Milestone are restricted to in-person and telephone channels, along with cards for payments; only the latter offers robust and modern security, and that's highly limited. With personal details easy to obtain from the public domain, account takeover fraud (ATO) presents little challenge to even unsophisticated bad actors.

This lack of solid verification also leaves organizations open to application fraud; proof of address can be easily fabricated by even unsophisticated bad actors with simple, readily available technology and basic Photoshop skills.

Customer experience

For the majority of customers, a fully-featured digital channel is an expectation. Whether it's account balance checks or loan applications, an app or a web portal is the first and only port of call for today's time-poor consumers. If they need to physically visit a branch to perform basic financial functions, they will very quickly start to look elsewhere.

Cost

The financial weight of reliance on physical services can't be ignored.

Having a human bank operator perform all of this authentication manually is incredibly expensive compared to even the most basic digital alternatives. As well as the costs of providing an in-person service, banks can find themselves paying significant amounts of money on authentication methods for their card channel such as SMS OTPs – which are far from secure – or rely on knowledge-based approaches, that can be bypassed by social engineering, for their telephony and physical channel.

Which steps should you take?

Build out a digital channel that can complement your existing physical presence. By improving your authentication approach in this way, you will also improve user experience.

Ensure that your authentication is secure. How that authentication is delivered is up to you. You may opt for a traditional suite of authenticators, such as SMS OTP or hard tokens, or embrace more advanced technology like behavioral biometrics and device fingerprinting.

Callsign can provide the technology that enables you to be confident that when a user authenticates, they are who they claim to be – and that the evidence you use to establish that fact is gathered in line with both regulation and your internal risk policy.

We've worked with the world's largest financial intuitions and can help you establish a secure web presence that will allow your customers to interact with your business in the most secure, and engaging way possible.

DIGITIZE ME

Digital transactions

At this Milestone, customers can interact digitally – log in, view their account, make payments, apply for products – but these interactions are not in themselves inherently safe and secure.

The channels they use will likely operate separately, alongside other legacy channels like physical branches and telephone banking.

This is a significant advance from Milestone One, but it's not without its own challenges.

Compliance

Introducing a digital element for authentication ensures that your compliance objectives can be met more easily and cost effectively; but there are still shortfalls. Many organizations will find themselves reliant on credit checks and online forms for onboarding customers.

Multi-factor authentication for logging in is a step in the right direction here, but there are still challenges around regulation; not getting exemptions right can lead to customer frustration and increased costs.

And any solution put in place still has to overcome the hurdles imposed by legacy systems. Often cobbled together over many years, you may find that you have disjointed systems and processes, which can leave costly-to-patch gaps that raise the risks of non-compliance.

FOCUS ON:

Fraud prevention

ATTRIBUTES:

Most services managed online

Minimal customer data integration / personalization

Hybrid on- and offline account creation

Legacy systems lead to compliance challenges

Awareness of common synergies between fraud, cyber and digital teams

Fraud and risk

Relying on username and password combinations is highly risky. Step-up authentication methods such as SMS OTPs and hard tokens offer only limited protection. Indeed, there are many ways that bad actors can gain access:

- Hard tokens are reliant on algorithms that can be cracked by determined fraudsters and SMS OTPs can be intercepted through SIM swap or SS7 attacks
- ATO is still a risk, with fraudsters routinely performing credential stuffing attacks using credentials harvested from external data breaches via the dark web
- Remote Access Trojans (RATs) can allow bad actors to access a user's account, even if your authentication technology works perfectly

Onboarding is also at risk from account opening fraud. Fraudsters using synthetic IDs or stolen credentials to create new accounts can bypass the limited identity assurance offered at this stage.

Customer experience

For login and payments, friction is still an issue that can lead to customers abandoning interactions. Hard tokens and SMS OTPs makes for slow and inconvenient authentication journeys, and knowledge-based authentication can also be a stumbling block if customers can't remember the answers that they stored.

Onboarding is often less than smooth at this Milestone. Customers may be confronted with unwieldy forms – and then still be required to perform additional physical verification stages.

And for thin-file customers with limited accessible data on their credit history, previous addresses or employers, a reliance on credit checks can be a decisive stumbling

Cost

Once again, technologies such as hard tokens and SMS OTPS incur a ballooning and ongoing cost pressure. Equally, relying on legacy systems and paper-based processing and checking can also see costs quickly spiraling.

But in an age of social media, reputational damage can be even more costly. Poor UX or the risk of data breaches from weak security can both contribute to driving customers away from you and towards competitors who are managing to successfully balance security and UX – as seen in the next Milestone. block, through no fault of their own.

The Callsign difference

15-20% year one savings

30-40% projected savings over five years

Source: Tier one UK retail bank

Which steps should you take?

Update your technology so that it's more user-friendly. It's also vital to ensure that it's also compliant with global regulatory legislation, so that you can leverage your new and improved authentication events across all areas of your business – and to take advantage of accelerating technologies such as Open Banking.

Technologies such as facial recognition are widely utilized at this stage. Whilst beneficial, they don't offer long-term assurance and aren't as robust as behavioral biometrics, as they differ wildly depending on customer demographics and devices. This is also a

costly approach, particularly when turning to third-party vendors.

When looking to passive authentication, organizations should opt for a solution that offers passive behavioral biometrics. Callsign's layered intelligence combines our unique Muscle Memory Technology – the highest fidelity behavioral biometrics on the market– with device, threat and telco intelligence to positively identify genuine user without adding friction, across all devices and demographics.

CUSTOMER-CENTRIC

Digital leader

In this stage of the Pathway, the organization is becoming a digital leader, with a variety of advanced technologies that give an excellent customer experience.

But these technologies and processes are not yet joined up, leaving significant gaps in both the portability of a customer's identity, and an organization security landscape.

In short, whilst the customer's journey is now highly evolved, it's still potentially limited by IDs that are tied to individual products or services.

Compliance

Despite the adoption of highly evolved technologies, your approach to identity may not be aligned across departments and channels. If you're not presenting a unified front from a compliance perspective, you could fail to meet the regulators' demands – and end up facing steep fines.

Across the world, the landscape is shifting towards a contingent reimbursement model. In countries such as the UK, Singapore and Australia, the onus is increasingly being placed upon financial institutions to reimburse customers who have fallen foul of fraud.

It's a complex situation, and one that depends upon the technologies that you should have implemented at the previous Milestones, as well as a solid approach to orchestration.

Fraud and risk

A bad actor doesn't have to breach the perimeter to do harm. Many are adept at

FOCUS ON:

- Customer experience

ATTRIBUTES:

- Omnichannel banking services
- Differentiated customer experience online
- Automated application and approval services
- Compliance & data security by design
- Proactive collaboration between fraud, cyber and digital teams

using approaches such as social engineering, which has expanded rapidly in the last three to four years. It's far from unusual to find a customer unwittingly verifying a fraudulent transaction themselves or falling prey to a phishing attack.

Siloed data also presents a high security risk. When protocols are different across every journey, and data isn't shared between departments, it means that fraud detected in one area (a bad actor making suspicious payments on a credit card) won't be relayed to another, such as a checking account. The wider intelligence that the business is gathering is therefore not being shared and used to its best effect. Gaps remain that, if closed, can improve security, as well as user experience radically.

Your teams need to be working together to adopt methods that positively identify the customer – helping to reduce false positives and unnecessary friction. As at the previous Milestone, there is a dependency on traditional biometrics such as facial recognition, but these should not be solely relied upon as they do not offer consistent journeys or robust enough security assurances for your entire customer base.

Customer experience

At this stage, layered intelligence allows for to remove friction in the journey. By using layered intelligence across device and behavior, you can deliver seamless and secure customer experiences.

As your customer base grows, so will your demographic reach, and your user journeys need to be sensitive to the needs of all of your customers. That means that you should be employing passive methods of authentication, which are more inclusive and are less vulnerable to phishing attacks and SMS SIM swap attacks which can impact your reputation.

But even with these in place, in the absence of a joined-up approach to authentication, users will need to engage with different processes for every business unit they encounter, which can be frustrating. Despite having a checking account, a customer may need to complete a lengthy application for an investment or share account – which causes friction.

Your fraud solutions should be empowering teams across the organization to work together to leverage identity technologies to drive engagement and personalization.

Managing reputation is also vital. Customers are hard to win, and easy to lose. Poor authentication experiences or cases of fraud can lead to customrs sharing their dissatisfaction across social media.

Cost

A lack of communication between business units is problematic – and costly – on both a conceptual and scale level, since organizations will have to implement different costly point solutions to fix different issues.

Having different vendors and supplier relationships for each business unit is inefficient – and it's a very expensive way to run a business.

Impact of online scams

84% of consumers received a scam message

45% lose trust in the business named in the scam message

Source: Callsign-commissioned research

Which steps should you take?

Callsign's technology is so adaptable that it can be used in channels that have, until now been completely separate. Because we positively identify the customer, Card Not Present payments can be authenticated using exactly the same process that is implemented for a checking account login journey.

A single view of the customer can be built utilizing layered intelligence across device, behavioral biometrics and location data, which can be leveraged by all channels, and product lines in the business via orchestration solutions.

Different areas of the businesses that are using different processes are probably also using different technologies, which can make linking them together seem very difficult – but not impossible. Using Callsign's code-free multi-tenant Orchestration Layer, these challenges are alleviated with full end-to-end journey management across brands and channels, giving all those across the organization the visibility of the customer landscape.

With multiple channels, customer demographics and journeys, it's important that any new journeys (or changes to existing ones) do not damage the customer experiences you've worked hard to build. Our Orchestration Layer offers the ability to test any changes with real-life data, ensuring that the customer experience is central to any business decision.

Protecting customers from evolving fraud threats such as scams and social engineering will be vital. Callsign's dynamic intervention technology can detect the more complex forms of fraud such as social engineering as it's happening and warn the victim in real time.

Taking time to consider and harness the right technologies puts you in a position where fraud is significantly reduced, and compliance is much easier to meet with tailored customer journeys and customer privacy factored in as standard.

With this foundation you're well positioned to embrace future opportunities that digital evolution is bringing, and ready to make the significant step to Milestone Four.

PORTABLE IDENTITY

Digital trust

The final stage in the Pathway sees banks creating portable IDs, which provide seamless user journeys and long-term digital trust for consumers, plus opportunities for banks to leverage ID across their own other organizations, or their strategic partners.

Compliance

Until now, all interactions have been between the customer and the bank. But in this final Milestone we reach the ultimate dream of digital identity: allowing customer to use their own bank-assured digital identity to do other things.

It could be as simple as setting up a streaming account, or as complex as dealing with a mortgage broker. Whatever the case, the value is found in interactions that demand a high level of assurance that a person is who they claim to be, and that the attributes they claim to have (such as their name, age and address) are correct. The best way to do this for all parties involved is to use the bank's information, since it's likely to be highly accurate, given that it has, by law, gone through a regulated KYC / AML process.

You therefore have the information that makes a digital identity, but to make it portable, users need to be able to move information from inside the your system to the outside world. To sum up, for a digital identity to be created, a bank must have three things:

FOCUS ON:

Identity as a service (IDaaS)

ATTRIBUTES:

- Streamlined interbank and retail processes / services
- Hyper-personalized experiences with portable omnichannel digital IDs
- Brand leadership and competitive differentiation through personalization
- Harmonized operational priorities with cross departmental accountability

- The ability to ingest and verify the customer information which is used to create an identity
- A way of sharing it – usually an API or via more complex concepts such as Open Banking protocols
- A consent journey that allows customers to authenticate and authorize what information can be shared

Fraud and risk

This Milestone is dependent on solid authentication mechanisms; without them, portable identity can't happen.

You need assurance that the data you're ingesting and the people you're onboarding are legitimate. You also need an assurance that the consent journey is working, and the user really is authorizing the sharing of their information. And finally, you need secure piping between the bank and the "relying party" who is receiving the identity data.

Customer experience

The main concern for banks at this milestone is, of course, how it's all going to work. And for many businesses, it will be through an in-app journey. The app will provide an API to a third party, such as a mortgage broker, with a button that lets customers choose to share their identity information from their bank account.

The journey within the app is crucial. It must be easier than filling in the form manually. But it should also be informative and let users know what they're consenting to – perhaps via different fields that you can turn on or off depending on what they want to share.

Emerging technologies, such as common Open Banking API standards, and blockchain-powered digital identity wallets are also being watched closely by thought leaders across the world. Regardless of which method wins out, banks need to be ready to respond

What are the next steps?

Our solutions provide assurance at every stage of the creation of a portable identity. Our multi-layered authentication technology ensures you're only onboarding legitimate people, and that the people consenting to the sharing of their ID are who they claim to be.

Meanwhile, our Orchestration Layer allows us to build a secure pipeline between your organization and those you'll be sharing information with.

But what makes us truly unique in this space is that we can provide a solution no matter what other technologies you're using. Our authentication technologies work effortlessly with robust technologies from APIs – including Open Banking – to blockchain digital identity solutions.

LOOKING FORWARD

Beyond the Pathway

Wherever an organization currently finds itself on the Pathway, there is the opportunity to move further along.

Whether that's reaching the limit of your current Milestone, or moving to the next, it's imperative that momentum is maintained. Customer behaviors and tastes are constantly evolving and changing – along with the techniques of bad actors and criminals.

A mature identity strategy gives you smarter ways to authenticate, stronger decisioning, and a single view of the customer, not to mention a seamless and secure experience for them. But it also has the potential to become a strategic driver for a wide range of other business benefits.

Building a full and comprehensive ID strategy is a foundational move. Once your ID strategy is fully in place, the information in your database becomes something you can leverage. ID capability suddenly moves from a cost point to a value driver – the positive disruption caused by progressing along the Pathway and implementing Callsign's technology will accelerate momentum in more areas of the business than just identity.

Putting customer ID at the center of customer strategy will involve a positive and future-focused mindset change, which will ripple out across all areas of the business and embed itself in even seemingly unrelated business priorities.

Lastly, and perhaps most crucially, the digital trust created when businesses complete the Pathway will open up significant and lasting opportunities – from boosting brand reputation and customer stickiness to using ID data to drive value.

Depending on where you are on your journey, some or all of these tasks might seem complex. But you don't have to do it alone.

Callsign is here to partner with businesses to help them choose and implement the right technology for where they are and where they want to go. We want to get to know your business, forming a strategic and collaborative partnership and working together to find the best journey for you through the Maturity Pathway.

To get that started, please get in touch with a Callsign specialist today, and place your business on the path to digital trust.

Book a meeting today
www.callsign.com/contact

callsign®

Balancing security, UX & privacy is easier than you think. Find out how we can help you on your journey to digital leadership – **callsign.com**.

Get in touch for a demo of our capabilities: **sales@callsign.com**