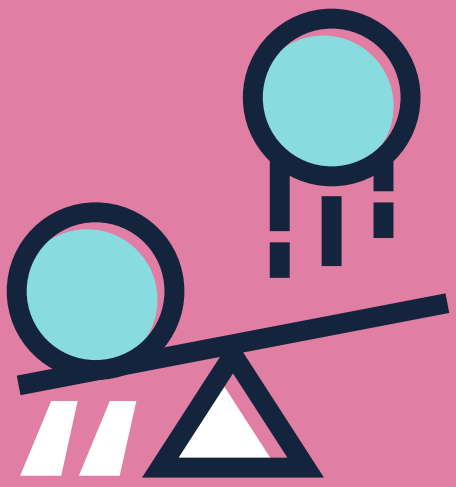
White Paper

Seamless and secure

Putting users at the heart of financial services

Protect customers, prevent fraud, and build better experiences through design and data

hippo



How can financial services providers make sure they offer secure, seamless and customer-friendly experiences?”

Contents

Introduction

A frictionless future for financial services

Traditional financial services providers don't have it easy in the digital world.

Increasingly used to seamless digital transactions from digital-first service providers, customers are demanding better experiences from their financial organisations including banks, building societies and insurance brokers. Whether they're opening an account or making a payment, customers want to interact with service providers quickly, easily and smoothly.

This is difficult, when we consider the legacy and siloed organisational context many providers operate in, and an increase in regulatory requirements such as stronger Consumer Duty obligations. When we combine the need to offer both branch-based operations and online services, with compliance obligations to prevent fraud, keep systems secure, and protect their customers, it's clear financial services providers face significant challenges.

So how can financial services providers strike a balance between security, compliance and a seamless user experience? At the heart of the matter is the complex challenge of digital identity. Providers need a way of establishing that people really are who they claim to be online, understanding a customers' interactions and behaviours across all their services and products, and only granting system access to legitimate parties.

This report is for senior leaders within financial services institutions in the fields of security, risk and compliance, fraud, and data, as well as those in digital, product, innovation and customer experience roles.

Faced with increasing levels of regulation, greater customer expectations, and legacy technology challenges, we'll ask the question: how can financial services providers make sure they offer secure, seamless and customer-friendly experiences?

By adopting innovative approaches to design, data and technology, financial services organisations can offer better user experiences, while fulfilling security and regulatory requirements. They can also find better ways of identifying and supporting vulnerable customers, prevent fraud, and open up new commercial possibilities.

Jim Small
Head of Identity
Hippo

Section 1

Creating a seamless user experience

Today, customers expect their interactions with financial services providers to be seamless, frictionless, and secure. This means they want to use services which enable them to do whatever it is they need to do quickly, easily, and with confidence, whether that's signing up for a new product, checking their balance, or transferring money.

In financial services, this task is made more complicated by the need to make sure interactions are compliant and highly secure. This involves adding verification steps, and therefore levels of friction, to the onboarding and transaction processes. These are touchpoints in a user journey which require someone to prove that:

1. **they are who they say they are**
2. **they have the right permissions to do what they are trying to do.**

Without some friction, services cannot be secure. But with too much, the customer experience becomes time-consuming, clunky and frustrating. With digital-first competitors offering highly seamless experiences, this can easily lead to customers voting with their feet and a loss of business for traditional providers.

Financial services providers therefore need to find a balance between managing security and risk, and delivering services that are easy for their customers to access and use. Two main challenge areas to navigate here are the user onboarding and transacting experiences, which require carefully designed identity solutions to be successful.

> "Financial services providers therefore need to find a balance between managing security and risk, and delivering services that are easy for their customers to access and use."

Digital identity solutions for frictionless onboarding and transacting

Digital identity is a security and business discipline, involving multiple technologies and business processes. Its goal is to help the right people or machines to access the right digital assets at the right time for the right reasons, while keeping unauthorised access and fraud at bay.

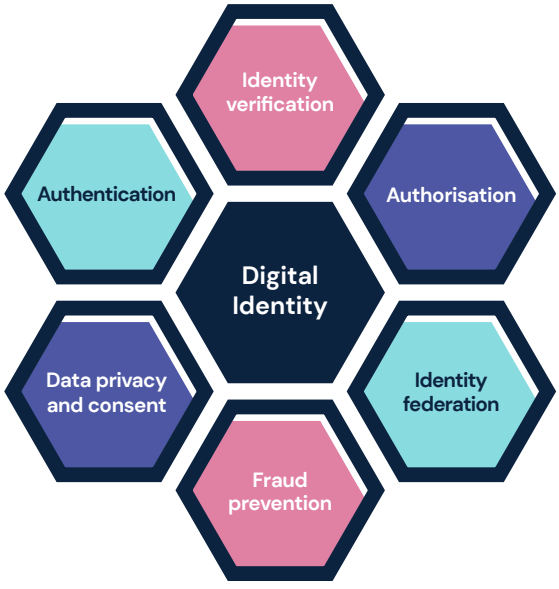
When a customer is onboarded to a service or wants to carry out a transaction, a digital identity solution is used to carry out the following processes:

Identifty verification - how we assess and validate the identity of a person when they interact with us online rather than in real life. This is based on matching the person who is asserting their identity (using biometric data such as fingerprints and facial scans) with the evidence they provide, such as their passport or driving licence.

Authentication - the login stage. Once a party has verified their identity and created credentials such as a username and password, or a Passkey, they can use this information to log in and access a service.

Authorisation - granting an authenticated party permission to do something, such as access an account or make a transaction. Permissions are often based on the user's role, or attributes they hold - such as a customer type, or job title. To keep the system as secure as possible this permission should be strictly limited to the resources they need and not let them access or do anything else

The identity solution must also remain compliant with data privacy and consent principles, and flag potentially fraudulent activity.



Identity verification
Creating and verifying a digital identity (and securely binding it to a real world person or machine).

Authorisation
A security process that determines a user or services level of access to resources.

Identity federation
Allowing authorised users to access multiple applications and domains using a single set of credentials.

Fraud prevention
Use of identity and attributes verification and authentication tools to flag potential fraud activity.

Data privacy and consent
Rules for the processing of personal data based on accepted a legal basis, including user consent

Authentication
The process of determining whether someone or something is, in fact, who or what it says it is, when accessing a service.

Putting users at the heart of solutions for seamless experiences and compliance

To create the right identity solutions, and build secure, frictionless and cost-effective onboarding and transaction processes, financial services providers must look to user centred design (UCD) to ensure products are built to user needs.

User centred design is a design methodology that ensures the customer and their needs are taken into account at all points in the design process. Done well, this results in an improved customer experience that enables users to do whatever they need to do in the minimum time.

Putting users at the heart of a solution involves conducting thorough research to understand who the different types of users of a service are, their preferences, and their needs. It enables organisations to answer the following kinds of questions:

Who are our customers?

What do they want to do?

What needs do they have?

Do they have any accessibility or usability requirements, and how does this impact their use of our service?

Once they understand their users' needs, organisations can consider how to best support them through design decisions as well as the choice of technology. It's also important for solutions to be aligned with business strategy, which requires an assessment of the current organisational context.

In financial services this can be complicated. The business context is often complex, with providers typically navigating legacy technology, data and functional silos, and accessing multiple different systems through interfaces that are bolted on in the back office. These systems often require manual workarounds, adding to the time and cost it takes to complete processes, and introducing the potential for human error.

This is a concern given the pressure on providers to meet multiple regulatory requirements – and to demonstrate their compliance to the Financial Conduct Authority (FCA) and National Crime Agency (NCA). Along with data privacy regulations such as GDPR, specific industry regulations such as the second Payment Services Directive (PSD2), and the Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations require providers to include stronger customer authentication and verification measures in payments and onboarding.

By using a thorough design approach centred around user needs, financial services providers can streamline their services, helping them provide better customer experiences, gain operational efficiencies, and be compliant with this regulation. Redesigning the onboarding process with a focus on user needs, for example, can significantly reduce the time it takes to onboard new customers, slashing processing time for applications from days or months to a matter of hours.

This not only provides a better customer experience, it also reduces costs for providers, and helps them demonstrate compliance with KYC and AML regulation. Well designed, streamlined experiences give providers better oversight of their operations, making it easier for them to both meet and report on regulatory matters.

Case study

NHS login: Delivering seamless access to NHS digital services with user centred design

As a part of its strategy to increasingly deliver services through digital channels and empower patients to manage their own health and care, the NHS wanted to provide a single, trusted way of accessing its 80+ digital services.

The brief? To deliver - within five months - a secure, scalable login solution capable of dealing with 50 million patients.

A previous Discovery/Alpha phase led by an internal NHS team had run into issues, resulting in a failed GDS service assessment. We therefore worked with the NHS team to refocus the project, applying user centred design to increase the emphasis on user outcomes, and providing leadership across product, design and delivery functions.

Adopting a one-team mindset helped us promote collaboration and transparency across the different project teams, ensuring we stayed on track and delivered a scalable, secure login solution within the tight deadline.

NHS login is now one of the UK's most-used digital identity services and is the NHS's first cloud-based identity service. Embedded in the NHS App, the login has resulted in the increased uptake of online healthcare, with 64% of NHS App users having never registered for an online service connected to their GP practice before.

As a highly regulated, complex sector which deals with personal data and legacy technology, healthcare faces many of the same challenges as the financial services industry. Insights and approaches from projects like this can therefore be applied to solve identity challenges and common problems faced by financial services providers.

Key Statistics

At its peak, the NHS login conducted **2 million daily authentications**

There was a **40% reduction time for verification journeys**, including tailored journeys for deaf and non-English speaking users with non-verbal preferences (17% of total)

NHS login is a highly scalable, secure, and robust service using open-source cloud technologies - **reducing hosting costs by 80%**

"Hippo's strong focus and aptitude in designing for and meeting the needs of our users has enabled the NHS to deliver a single simple login for all. [This] underpins the NHS' strategic objectives to protect the NHS front line through the increased adoption of digital services and to enable individuals to be empowered to manage their health and care."

Melissa Ruscoe, Programme Head, NHS login

Section 2

Identifying and protecting vulnerable customers

Verifying and authenticating people through digital identity solutions is at the core of many processes within financial services, and is a key focus for regulatory requirements. This is intended not only to prevent fraud, but to also protect customers in other ways.

The Consumer Duty regulation of 2023 is part of the FCA's aim to set higher standards of consumer protection in the financial services industry. A key element of this regulation is the explicit requirement to protect vulnerable customers, such as those facing financial hardship or illness.

The definition of exactly what it means to be a vulnerable customer is broad, and could encompass lots of different characteristics. Importantly, it's also not static, as people's financial and health circumstances have the potential to change all the time. A customer with no history of vulnerability could suddenly become vulnerable if they fall ill or lose their job, for example, and vice versa.

To support their customers and comply with Consumer Duty, financial services providers therefore need a sophisticated approach to identifying vulnerable people which can account for changing situations and circumstances. This is only possible through data.

The single view of the customer

The solution to understanding a customer's behaviour in greater detail is to create a single, overarching view of who they are and what they do. This is known as a single view of the customer.

It's a centralised record of an individual and all the interactions they have with an organisation, including things like their accounts and products, transaction history, demographics, location, and preferences.

In order to create a single view of a customer financial services providers need to process and manage data effectively.

Financial services providers should ask:

What data do we have now and how do we currently use it to inform our decisions?

What data do we have that we aren't currently using? Why not? What could it potentially tell us about our customers?

What third party data sits outside of our organisation that we could use via APIs to gain a better understanding of our customers? For example, third party mobile phone operator, utility company, credit bureau, geographic, or even car ownership data?

Often, organisations don't use their data effectively because it isn't in the right format or just doesn't seem relevant or useful. However, by investing in data processing, and with a new perspective on data analytics, they can find new ways to uncover previously hidden insights about their customers and their behaviour.

This includes using third party data from other sources or service providers, such as mobile operators, credit bureaus or utility companies, to verify someone's information. Verifying a person's data and trusted status across the different organisations they interact with can help financial services organisations to validate whether or not they are who they say they are, and build a more complete picture of their behaviour.

Understanding customers in this way through a single customer view enables financial services providers to identify vulnerable individuals and comply with Consumer Duty. It also makes it possible to carry out predictive analytics, giving providers the ability to analyse behavioural traits and identify customers who are at risk of becoming vulnerable in the future.

For providers, the ability to demonstrate they're taking this kind of preventative action is extremely valuable in a regulatory environment that is only likely to become more demanding. A better understanding of customers also offers valuable commercial opportunities, to upsell products and services that might be of interest to specific individuals.

Successfully creating a single customer view is typically just as much about cultural change within an organisation around data and data sharing as it is about technology. Although financial services providers do face challenges in dealing with siloed systems and regulation, innovation is still possible, and there are also plenty of examples to learn from elsewhere.

Financial services providers should therefore look to developments in other highly regulated sectors such as healthcare and the gambling industry who are using data effectively.

"Financial services providers should therefore look to developments in other highly regulated sectors such as healthcare and the gambling industry in using data effectively."

Case study

Building a secure, scalable identity tool to support people struggling with gambling

GAMSTOP helps people control their online gambling by voluntarily excluding themselves from all gambling websites and apps registered in Great Britain. Once they've registered with GAMSTOP, individuals are unable to create an account or log in with gambling operators.

Since 2018, we've helped GAMSTOP build and maintain their identity service. At the heart of the service is a matching algorithm, which determines if the person logging in or attempting to register at an operator is the same one registered with GAMSTOP.

This isn't as simple as just comparing X with Y, as data can change over time and is often of variable quality. Our algorithm is therefore designed to manage all possible scenarios. Although the system offers protection to registered consumers, it must also allow operators to provide a normal service to the rest of their customers. This involves providing real-time information to gambling operators so they can seamlessly check their customers' exclusion status each time they register or log in.

Every single day, millions of data-matching requests are processed by the GAMSTOP service. As the platform holds sensitive personal data, we follow security best practice both within the design of the platform and in our processes and operations, as we continually maintain and improve the service.

This kind of identity solution shows the value of connecting data to verify identity in a highly regulated, secure environment.

"We were looking at enhancing the service for the consumer and having met the team at Hippo, we were impressed by both their expert knowledge of data as well as their wide cross-section of experience."

Fiona Palmer,
CEO, GAMSTOP

Section 3

Fraud prevention with identity solutions and data

Along with identifying and protecting vulnerable customers, another important element of Consumer Duty is fraud prevention. This requires appropriate security measures to be put in place to prevent money laundering, block unauthorised activity on accounts, and stop customers from being misled or manipulated by bad actors.

When it comes to fraud prevention, traditional user identity systems that rely on passwords can pose a risk. On the whole, password-based authentication systems are inherently weak as users frequently re-use, share or lose their passwords. Passwords are also vulnerable to being stolen, and can easily be used to gain control of an account and make unauthorised transactions.

With security measures to prevent fraudulent activity inevitably adding friction to a user journey, financial services providers must find a balance between their fraud risk and a seamless customer experience.

Balancing privacy and security – the passkey solution

Passkeys are an increasingly popular identity solution that offer an alternative to passwords to authenticate users.

When a user sets up a passkey on a website or application, they create a private key - a unique digital credential that is stored on their device, and is linked to the public key on the website. This connection between the public and private keys allows the user to access the website or application account using only their biometric, such as a fingerprint or facial scan, or their device PIN.

Passkeys offer high levels of security, and require a minimum amount of data from an individual to access a service. Importantly, a single passkey enables a passwordless experience across all of a users' devices, browsers and operating systems, allowing a user to log in simply by using their mobile phone fingerprint sensor or facial recognition function, or by entering their PIN.

Passkeys don't require individuals to remember login information, and they can be used seamlessly across different devices and platforms. They offer greater privacy as they don't require people to share their personal information with every different party that needs to verify their identity. Instead, this is all processed by the passkey provider.

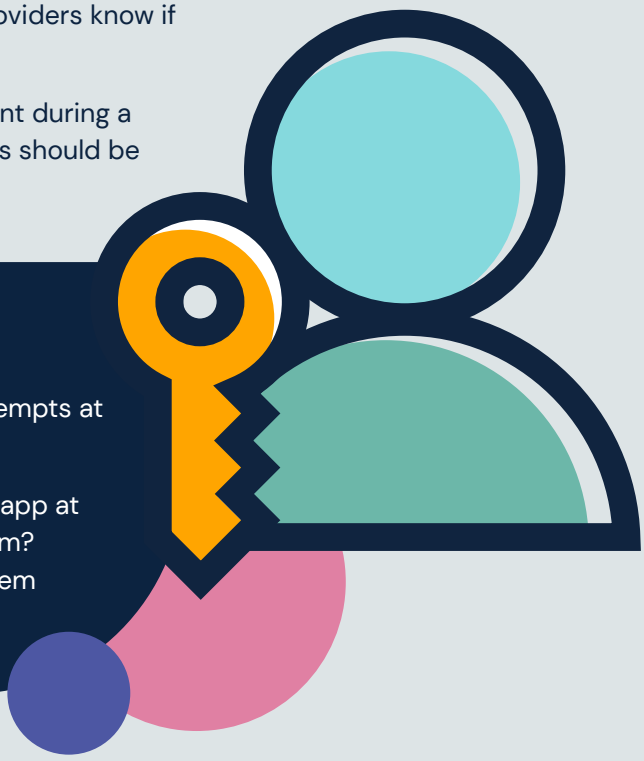
Unlike password-based systems, passkeys can't be stolen. Because access to an account is reliant on having access to both the public and private parts of the credential, passkeys prevent unauthorised access to services. They therefore provide a potential answer to both the usability and security challenges faced by financial services organisations when it comes to authenticating customers.

Using real-time and historic data to prevent fraud

Using passwordless systems such as passkeys, or other multi-factor authentication methods such as a combination of a password and a biometric, can help prevent many common types of fraud that occur today.

More challenging to combat, however, is fraud that happens when the legitimate holder of an account is manipulated into taking certain actions, such as sending money to scammers. Known as authorised push payment fraud, this is becoming increasingly common. It presents a fundamental problem for financial services organisations: when a verified and authenticated individual interacts with a service, how can financial service providers know if they have been influenced to do so?

A solution is to examine real-time data on the account during a transaction. To protect their customers, organisations should be asking things like:



- Where is the account being accessed from?
- Have there been several previous recent attempts at logging in?
- Is the customer on the phone and using the app at the same time? Where is the call coming from? Could it be from a scammer who is giving them instructions?

Data is available in real time to answer these questions. Combining this sort of information with historic information such as an individual's typical account behaviour - how and where do they normally access their account - their vulnerability status, and whether or not they have been a victim of fraud before, will help financial service organisations to identify and stop bad actors in their tracks.

The gaming and health industry are both good examples of regulated sectors which have generally adopted good practices on this kind of data analysis, as they understand the value of their data and use it to gain strategic insights into their users and business operations. The same can be said in the public sector, with the Department for Work and Pensions (DWP) proving that even as the biggest payer in the UK and the provider of the largest payment system in Europe, it can still handle data well.

Financial services providers can therefore look to these sectors to advance their own approaches to identity, ensuring they protect their customers to the best of their abilities and fulfil their Consumer Duty obligations.

"Insights gained from data not only enable organisations to improve their customer experience, they can also help them upsell products and services, and identify valuable new income streams."

Conclusion

Aligning design, technology and mindset

If financial services organisations put their users' needs at the heart of services, and build the right technology and data solutions, they can create more seamless and secure experiences for their customers, prevent fraud, and fulfil their regulatory obligations.

Understanding their users' needs and aligning these with forward thinking approaches to identity technology is crucial. This could be a move towards modern security solutions, including passwordless systems such as passkeys. A more holistic approach to data is also needed, as this will enable providers to create a single view of their customers. This leads to greater insights into customer behaviour, and the ability to protect vulnerable customers and prevent fraud.

A more joined-up approach across services and systems is an important way of gaining operational efficiencies, which are crucial as traditional providers continue to face significant competition from digital-first organisations. Having greater oversight of their operations is also a key step in fulfilling Consumer Duty, Know Your Customer, and Anti-Money Laundering requirements - and in reporting this compliance to the regulator.

There are other benefits too. Insights gained from data not only enable organisations to improve their customer experience, they can also help them upsell products and services, and identify valuable new income streams.

Innovation isn't always about technology, but it does always start with the right mindset. For financial services providers, this means understanding that new approaches are possible. By looking at similar regulated industries such as healthcare and gambling, we can see what's worked well elsewhere, using this experience to solve common problems and improve the speed to market of solutions.

hippo

A trusted digital services partner, designing with empathy and building for impact

We help organisations consistently present and leverage their brands and data to increase customer lifetime value. Our user centred design approach ensures your services are easy to use. Hippo delivers safe, secure and seamless processes for verifying identity and authenticating customers across entities and brands. Harvesting customer data across entities, and feeding this back into what customers experience with personalisation, drives positive action.

Learn more about Hippo ›

Our private sector credentials ›

Driving outcomes across public and private sector clients

BBC

Virgin

Ecology Building Society

GAMSTOP

NHS

Department for Work & Pensions