THE DIGITAL TRUST REPORT

"Trust is a process not an event"

How can financial services providers build and maintain trust in digital interactions?

11FS + Mitek

CONTENTS

INTRODUCTION

Trust is crucial for digital interactions

People are losing trust in the technology industry

↓9%

Trust in the technology industry has declined

Edelman's trust barometer shows that trust in the technology industry declined by 6 percentage points globally in 2020, and by 9 percentage points over the past 10 years, the largest drop of any industry analysed.

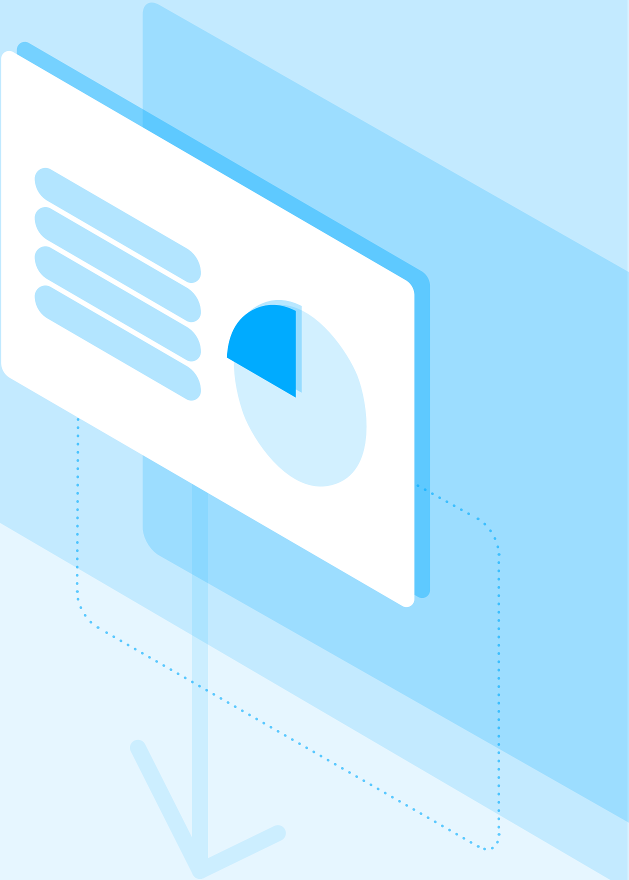
Meanwhile, we are using technology more than ever to carry out daily tasks, thanks in no small part to global events.

↑8%

Trust in financial services providers has grown

Trust in financial services providers on the other hand has grown by 8 percentage points over the past 10 years, more than any other industry analysed by Edelman.

Financial services firms have gradually regained customer trust after the nadir following the global financial crisis of 2008, while trust in the technology industry has fallen sharply.



This presents financial firms with a major problem:

The pandemic means firms have to deliver products and services to customers via technology, yet many customers are increasingly wary of technology.

This report sets out a framework for how financial services providers can counter declining trust in technology and build trust in the services they are delivering via apps and websites.

The framework takes ideas laid out by Rachel Botsman, Trust Fellow at Oxford University's Saïd Business School, incorporates elements outlined by Forrester Analyst Fatemah Khatibloo in her work on trust, adds insight from 11:FS's experts and explains how these concepts can be practically applied to digital financial services along with examples from the brands that are getting it right.

> *"Trust is a confident relationship with the unknown."*
>
> Rachel Botsman
>
> Trust Fellow at Oxford University's Saïd Business School

THE SITUATION

People instinctively distrust new things

Prior to 2020 the use of apps and websites to interact with financial services providers was steadily growing globally, but there were still millions who didn’t use digital touchpoints, often because of a lack of trust in the technology.

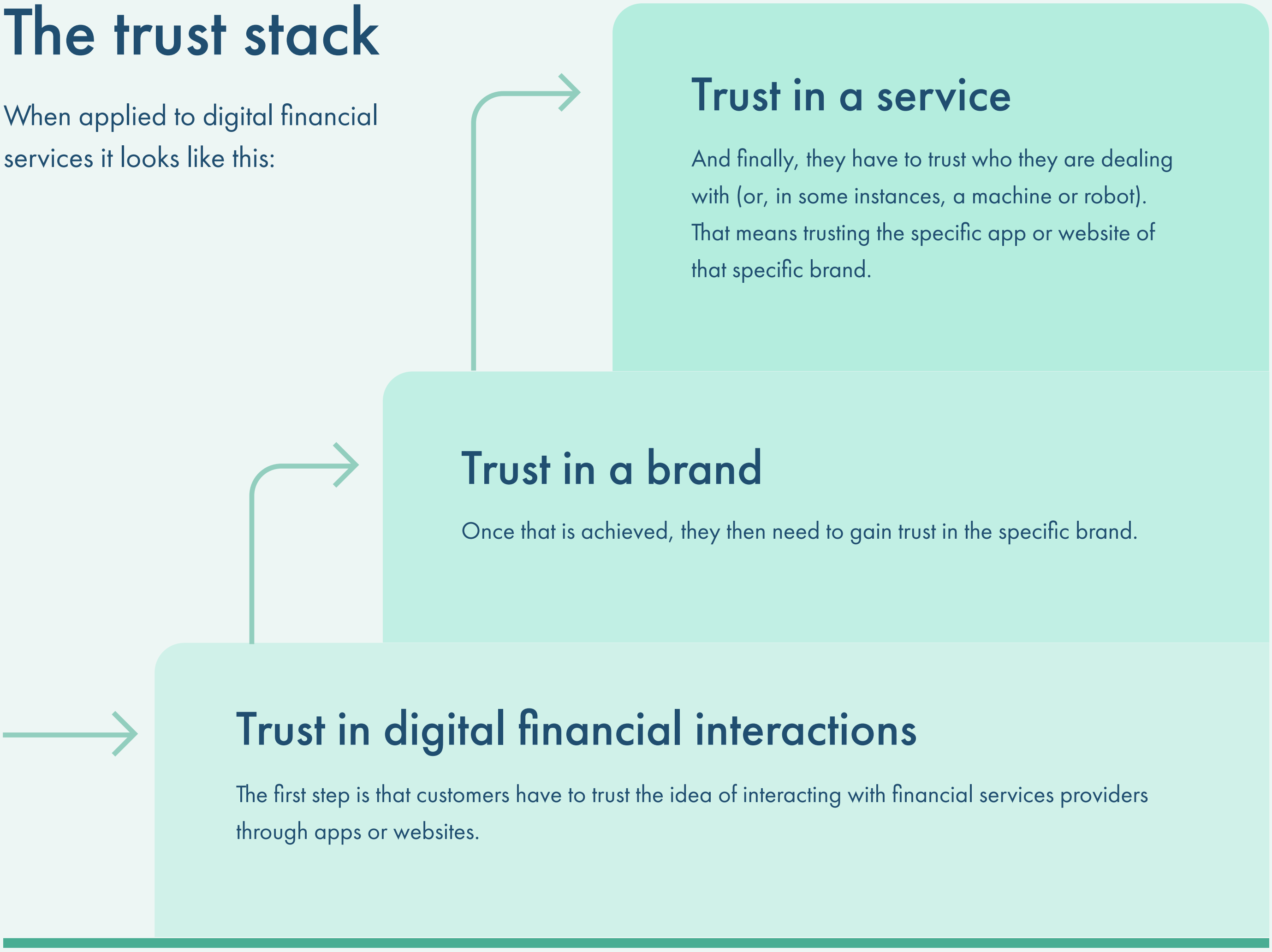
However, lockdowns resulting from the pandemic have forced these customers’ hands, giving them no option but to interact digitally.

For many it was the first time they had done so, while others who were happy performing low-risk interactions, such as checking their balance digitally, had to start using apps and websites for higher risk or less frequent interactions.

These customers were at the first step of the “trust stack”, a concept outlined by Rachel Botsman.

The trust stack

When applied to digital financial services it looks like this:



Trust in a service

And finally, they have to trust who they are dealing with (or, in some instances, a machine or robot). That means trusting the specific app or website of that specific brand.

Trust in a brand

Once that is achieved, they then need to gain trust in the specific brand.

Trust in digital financial interactions

The first step is that customers have to trust the idea of interacting with financial services providers through apps or websites.

There are many reasons for distrust

People distrust digital financial interactions for a large number of reasons, both rational and irrational.

Levels of trust vary widely from person to person, from brand to brand, from country to country and over time.

The factors outlined below will impact customers in different ways, triggering mild caution in some and a deep suspicion of technology and the security of their personal data in others. Some will be unaffected, displaying a complacent attitude to digital financial interactions. All of these groups need to be borne in mind by providers as they add trust-building elements to their digital journeys.

Increasingly common security breaches

In the UK, the data breach suffered by major airline British Airways in 2018 is still the subject of adverts telling people how they can claim, while the Reserve Bank of New Zealand suffered a significant cyberattack in January 2021 that saw commercially and personally sensitive information accessed by a hacker. These breaches are not only hugely expensive (the average cost of a data breach in 2020 was $5.85 million according to IBM), but hugely damaging to customer trust. Only 37% of global customers trusted their bank to look after their data in 2020, according to Accenture, down from 51% in 2018.

Trust in banks handling data fell globally from **51%** in 2018 to **37%** in 2020

Tightening of data protection rules

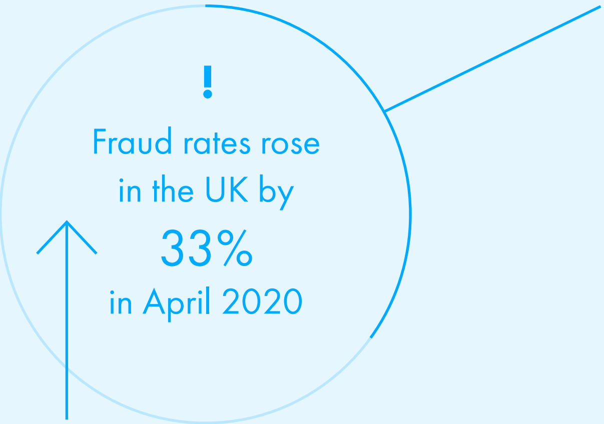
Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 are designed to protect consumers, but in implementing them providers often have to introduce new processes to ensure they are compliant. That means customers are having to adapt to new ways of doing things, such as accepting cookies on every website they visit in Europe thanks to GDPR, which results in them experiencing an unknown, pushing them back towards the bottom of the trust stack.

Increased consumer understanding of "data"

More people now get what their personal "data" is, and how valuable it can be — meaning they are a lot more concerned about what they hand over and to whom. The Facebook Cambridge Analytica scandal of 2018, which revealed that the social network had shared users' data with the consultancy for use in political ad targeting, played a big part in this. Data breaches are being exposed and reported faster thanks to greater use of social media.

! Bad experiences

Some people don't trust digital financial services interactions because of bad experiences they have suffered, or heard of, in the past. That could be any number of things from a successful fraud attack, a genuine transaction being declined due to faulty fraud detection systems, an inability to complete a transaction due to a technical failure, an app or website going down just when they need it most, or being unable to complete an interaction due to poorly implemented technology.



!

Fraud rates rose in the UK by 33% in April 2020

! Lack of human contact in digital-only interactions

Interactions with other people were the norm in financial services for 100s of years, and thus they are "known". Fully digital interactions meanwhile have only existed for decades so to many they remain "unknown". That helps explain why, globally, 47% of people would prefer to open a new account face-to-face, according to Accenture.

! Rising fraud levels

Fraud has long been a problem in financial services, and it's well known that as fast as providers block one avenue for fraud, criminals will find other routes to replace it. A wide range of major fraud types worry providers and their customers (see table below). Financial fraud has been exacerbated by the pandemic — rates in the UK rose by 33% in April 2020 compared with previous monthly averages, according to Experian. More fraud attacks lead to more publicity, and further contribute to distrust of digital touchpoints through which most fraud is being perpetrated.

Types of fraud

Stolen card fraud	A person's card details are intercepted and stolen and then used to buy goods or services.
Push payment fraud	A person is tricked into transferring money into a fraudster's account.
Account takeover fraud	An existing bank account is hijacked and funds transferred to a fraudster's account.
Identity fraud	A person's ID is stolen and used to open or access accounts, or acquire credit.
Synthetic ID fraud	Elements of a real person's identity are blended with fictional data to create a new identity.

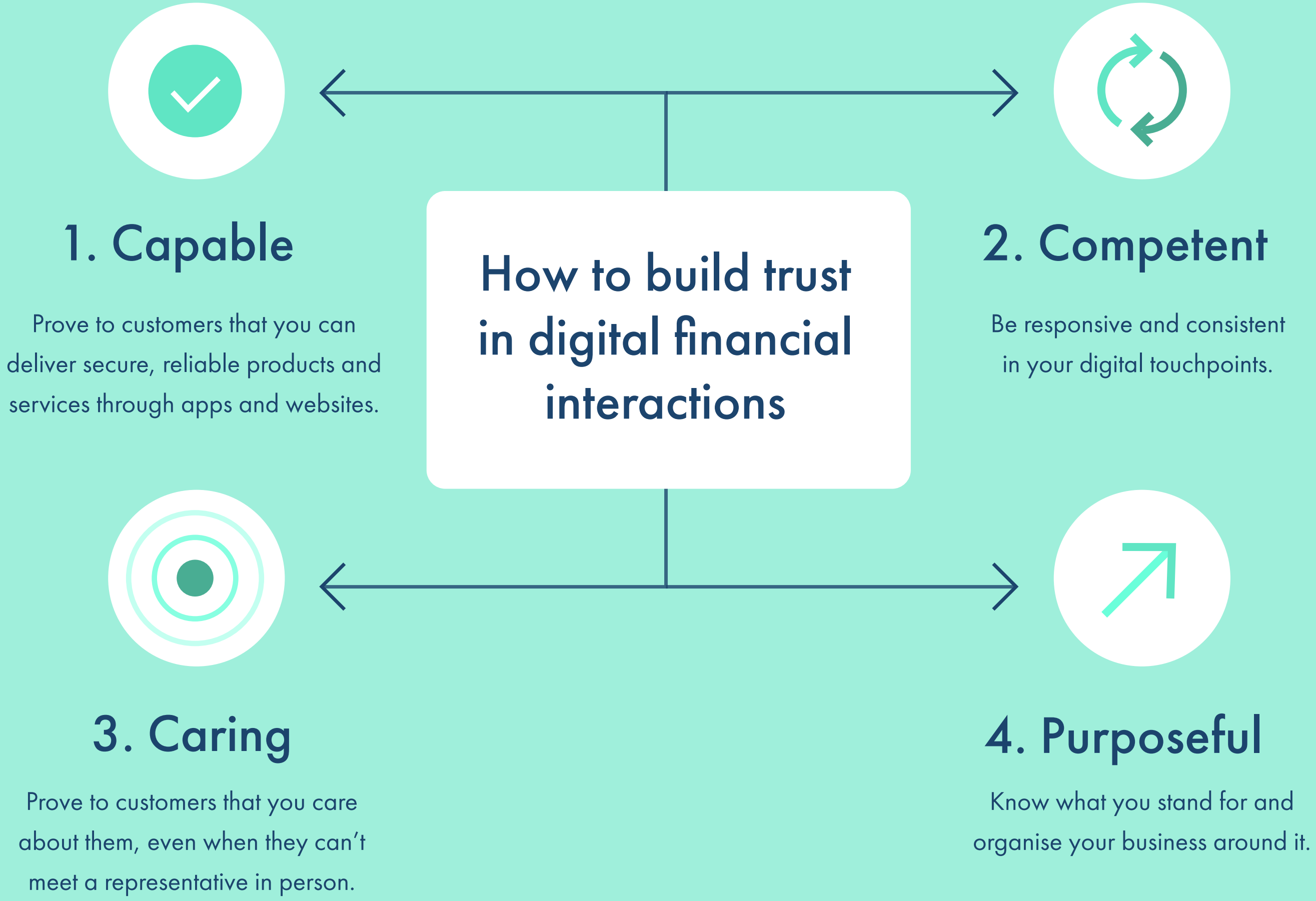
THE FRAMEWORK

Trust takes constant work

The digital interaction trust-building framework

Building and maintaining trust is a process that takes time for each customer, rather than a one-off event. Earning it takes time and effort.

This report gives providers a framework to use to create trust-building moments within digital touchpoints and continually reinforce it through digital interactions.



How to build trust in digital financial interactions

1. Capable

Prove to customers that you can deliver secure, reliable products and services through apps and websites.

2. Competent

Be responsive and consistent in your digital touchpoints.

3. Caring

Prove to customers that you care about them, even when they can't meet a representative in person.

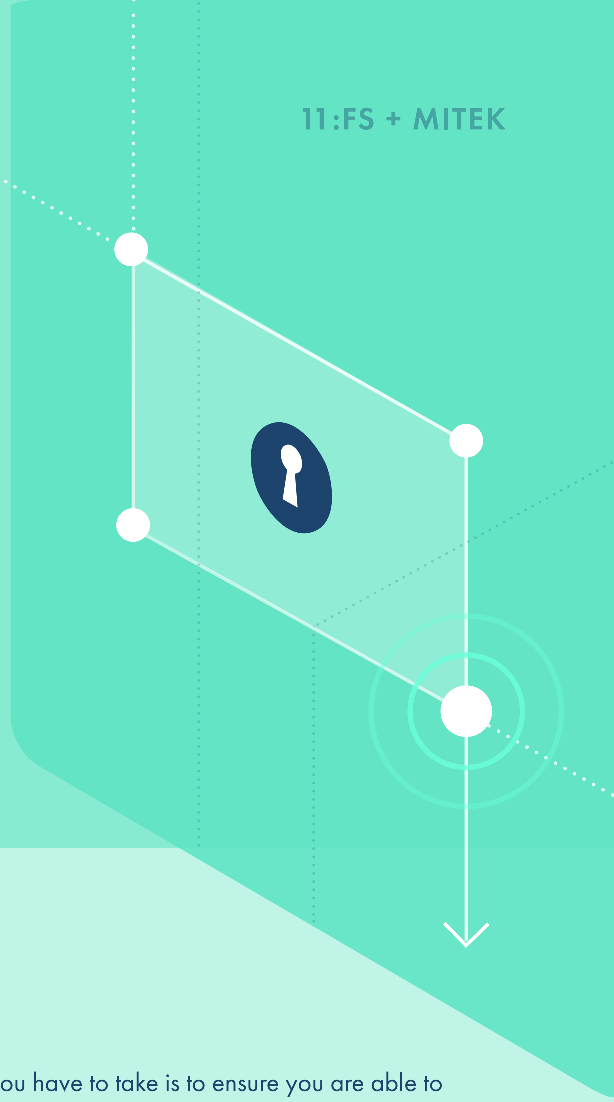
4. Purposeful

Know what you stand for and organise your business around it.

> *"We are being asked to make trust leaps faster and higher than ever before."*
>
> Rachel Botsman
>
> Trust Fellow at Oxford University's Saïd Business School

Financial services providers have to work hard to earn and keep customer trust

As the trust stack shows, gaining trust isn't a one time event, it's a process that takes time.



1. Capable

Prove you can do what you say you can

The first step you have to take is to ensure you are able to deliver products and services via apps and websites.

The second is to reassure customers that you are capable of protecting customers' money and data. False promises about capability will hinder attempts to get customers to trust digital interactions.

Getting Started

When designing digital products and services there are several key steps providers should take to ensure they are creating customer experiences that meet both their needs, and those of their users.

1. Get the whole business on board

Designing new processes will necessarily involve stakeholders from across the organisation including compliance, technology and commercial departments among others.

Providers need to involve people from each of these teams as they create digital capability to ensure products and services meet internal needs. That will enable faster progress in getting completed new offerings into customer hands, allowing providers to start the trust-building journey.

2. Choose partners carefully

Few brands can go it alone when it comes to making products and services digital, a realisation that is growing across the industry. Providers should seek vendors whose commitment to building trust is the same as their own.

For example, a common problem with digital identity verification software, a core component of many digital processes in financial services, is demographic bias. That's an issue that is likely to cause distrust among consumers who experience it, and means brands should actively engage with third parties to find out how they combat the issue.

Demographic bias is an issue that causes distrust among consumers

3. Establish robust data privacy processes

Financial providers' innate caution about allowing third parties to handle sensitive data entrusted to them is not a reason to not use vendors, especially when those vendors can help them create better customer experiences than they could alone.

Instead, robust agreements concerning the security and use of customer data must be in place.

4. Communicate the role of third parties to customers

Providers should inform customers of involved third parties at the relevant point in the journey, allowing customers to find out more about them.

One example of how this can be done was provided by Dick Dekkers, Director of Business Development at Digidentity:

"[A client] had a very clear explanation saying 'Listen, we use an external party called Digidentity to verify who you are and make sure your transactions are secure; they are better equipped to do that than us; we trust them because of...' and then they had a couple of bullets and links to certifications."

> *"Banks are looking to work more closely with stakeholders from inside and outside of the organisation who know what good digital experiences look like. Bringing those different perspectives together not only delivers efficiencies but also helps shape the seamless experiences customers crave."*
>
> Richard Ramsamugh
> Sr. Manager Strategic Development at Adobe

5. Ask for the bare minimum of data

Providers should examine their risk appetites and develop user journeys that ask for the bare minimum of data required to complete processes securely. Asking for irrelevant data makes customers suspicious and less likely to complete the journey — 52% of US consumers are more willing to trust a company that limits its request to only relevant data, according to McKinsey.

52%
of US customers trust companies that request only relevant data

You can seek more data at a later date if you need it for specific transactions such as a credit application or an unusually large payment. This approach puts the request in context, helping customers understand the relevance of the data in question. That builds trust, while removing steps from the initial onboarding or registration journey, reducing the likelihood of customer drop out.

"Don't ask for information just because you'd like to have that information at some point. Don't bother people with providing information that you don't need for that specific transaction; wait until there's actual value." Dick Dekkers, Director of Business Development at Digidentity.

How comfortable consumers feel providing personal information to their current financial services providers:

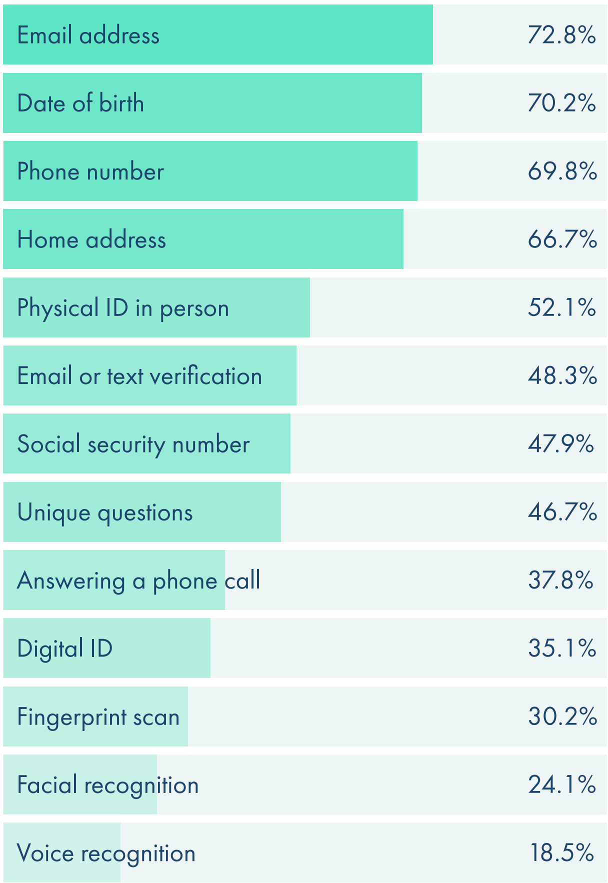


Fig. 1.
Share of US consumers who feel comfortable providing different pieces of personal information to their current financial services providers.
Source: PYMNTS.com

Encouraging usage

Enabling customers to use digital touchpoints for as many routine interactions as possible releases capacity for agents and employees in call centres and branches for more complex interactions.

That means providers must ensure they can offer a range of services securely, while incorporating the trust-building elements laid out at the top of this report into the customer experience.

1. Ensure a journey can be completed

Providers must enable customers to complete the most common interactions in their chosen channel. Being transferred out of an app or a website to finalise a low-risk interaction can create a poor customer experience, and will damage any trust the customer has already built in using digital channels.

2. Increase security with the level of risk

That means building capability for riskier transactions such as high-value payments and credit applications. This can be done securely using a "step up" system of authentication, that introduces more robust methods the riskier the provider deems the transaction to be.

For example, fingerprint or device recognition is suitable for balance checking or moving money between a customer's own accounts, but facial biometrics that check for "liveness" is more likely to reassure a customer that the provider is serious about protecting their identity for life insurance or a loan application.

3. Strike a balance between ease and security

In some instances an extra step in a user journey can be a good thing. Pre-populating information that is already held by a bank, for example for a customer making a payment to an account they have previously paid, is easier for the customer than having to find and re-enter details — and means errors are less likely.

Once transaction specific data, e.g. amount, has been entered then friction can be added to the journey in the form of requiring authentication.

In this instance customers are likely to be reassured by the step up in security, making them more likely to trust the idea of carrying out that particular transaction digitally.

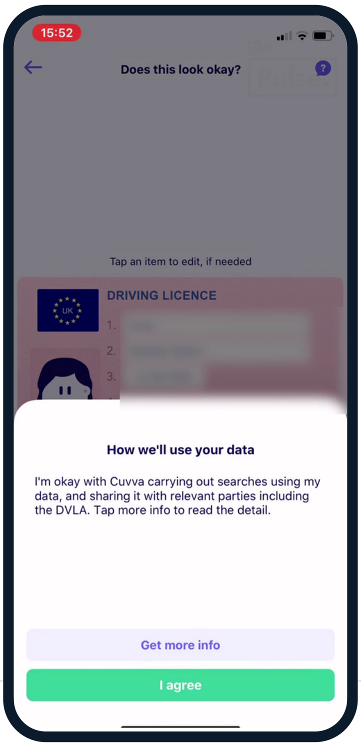
"Taking the identity verification step of the onboarding flow and making it feel like an identity protection benefit is not only possible, it's also very important." Stephen Ritter, CTO, Mitek.

4. Explain how data is used

Some customers want to know exactly what data is being held where, by whom and what it's being used for. That's even more important if third parties are being used for parts of the process. Providers need to make it easy for customers to find information about how their data is being used. For these customers, access to information is vital to their willingness to trust an idea or process.

"If you're using third party suppliers, be transparent about that." Dick Dekkers.

One way to do this is through pop-ups or links that don't interrupt the journey greatly for those who are not that interested in how their data is being used, but provide an opportunity for those who want to find out more (fig. 2). The pop-up can then be closed, returning the customer to the user journey without having to start again.



How we'll use your data

I'm okay with Cuvva carrying out searches using my data, and sharing it with relevant parties including the DVLA. Tap more info to read the detail.

Fig. 2.
Cuvva's onboarding journey includes a pop-up that asks an applicant's permission to use data from their ID document and explains what for, as well as enabling customers who want more detail to quickly access it.
Source: Cuvva, 11:FS Pulse.

2. Competent

Ensure your customers can rely on you

Appropriate timing is key to being considered reliable, and being reliable is key to specific apps or websites being considered trustworthy. For financial services providers that means doing things quickly where required and doing the same things, well, over and over again.

Acting quickly

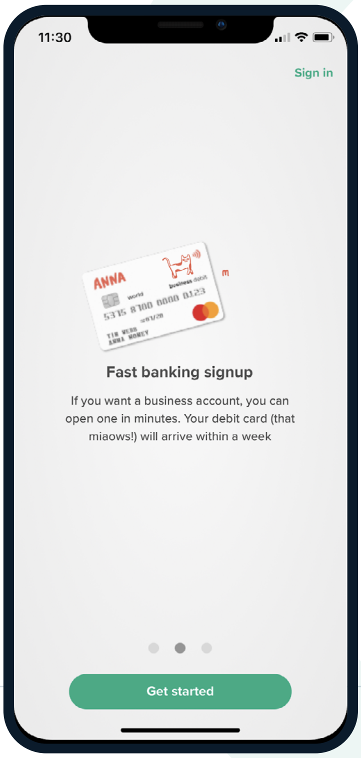
Whatever the interaction, it needs to be completed or resolved in a reasonable time frame. Everyone has their own definition of reasonable, but providers need to consider when a process should be completed as quickly as possible, and when introducing friction leads to a better customer experience.

1. Manage expectations

Whatever a customer's expectations, providers should signpost how long a journey is likely to take at the start, and ensure they can keep to those timelines (fig. 3).

Technology can help shorten timelines for more intensive interactions, such as account opening. Here digital identity and verification can enable user journeys that can be completed in minutes. That gets customers up and running quickly, keeping them engaged, and helping to build trust in the brand by showing it can meet its own timelines — proving itself reliable.

"Pending for hours isn't acceptable." Dick Dekkers.



Fast banking signup

If you want a business account, you can open one in minutes. Your debit card (that miaows!) will arrive within a week

Fig. 3.
Anna Money tells users how long the application process will take, and sets expectations around next steps before any personal information is requested.
Source: Anna Money

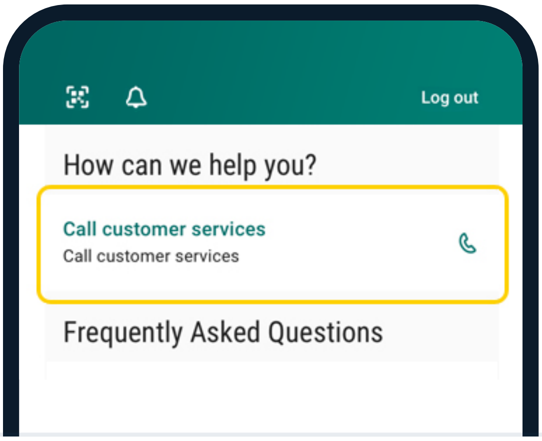
2. Use digital authentication to create better customer experiences

Speed is of the essence when customers have a problem.

At points of heightened emotion, trust can be quickly lost if the right action isn't taken. That means finding ways to acknowledge customer issues as quickly as possible, even if resolution takes longer.

Technologies like device or voice recognition and pre-population of forms can accelerate customer authentication. That lets the support agent get to the heart of the issue faster than if they were using older methods like security questions (fig. 4).

Saving customers having to re-enter personal details creates a smoother user journey, while reassuring customers who feel nervous about having to re-submit personal details.



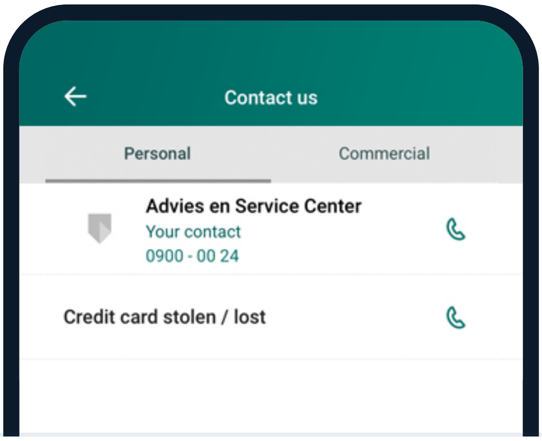
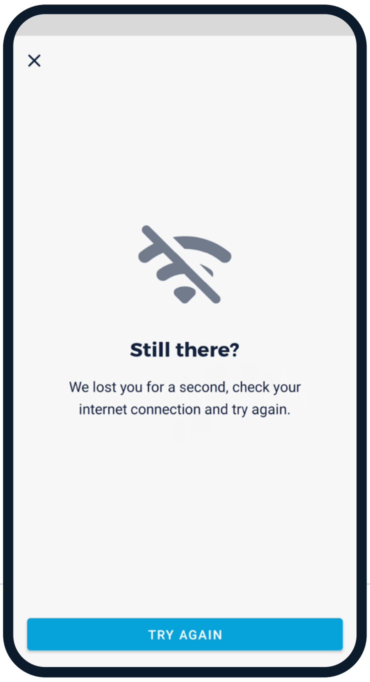


Fig. 4.
ABN Amro's app users can call customer services and ensure they are directed to the most appropriate department from within the app. This prevents the need for reauthentication, getting them through to the most appropriate person as quickly as possible.
Source: ABN AMRO.

> *"When customers call us via the app, we know who they are because we have already authenticated them."*
>
> Ester Merckel
> Director Customer Interaction Enabling & Digitization, ABN AMRO

Delivering consistently

Trust takes time to build, and it needs to be constantly shored up. That means ensuring customers have the same high quality experience every time they interact with you.



Still there?

We lost you for a second, check your internet connection and try again.

Fig. 5.
If internet connectivity is lost while trying to carry out a transaction within Monzo, the user can insert themselves back into the journey at the point at which they dropped out once the connection is restored.
Source: Monzo, 11:FS Pulse.

1. Use digital technologies to deliver consistently.

Manual processes not only take time, but are hard to replicate identically. Automated processes resolve both issues — digital identity verification that uses algorithms and machine learning facilitates scalable, consistent user journeys, for example.

Providers can build customer trust in infrequent interactions by repeating automated processes used for low-risk transactions in more high-risk situations. For example, a customer who is used to taking a selfie to login to an app and is asked to do the same to authorise a credit application will not be being asked to leap into the unknown — the action is novel but the authentication process is not, building trust.

2. Have a plan B

Ensure that if something goes wrong you can react quickly, and that the back up plan has been tested. One way to do this is to use multiple providers — Monzo has used several digital identity and verification providers at once in the past, ensuring customers can complete transactions without knowing there is any issue on the provider's side.

If something does go wrong, enabling customers to try and correct the issue without having to re-authenticate themselves for a short period of time gives them a sense of control and helps to maintain trust (fig. 5). If that's not possible, the customer should be connected to a support agent as soon as possible.

"It takes years to develop trust and a second to lose it."
Stephen Ritter.

> *"We carefully explain what is going to happen in every online process as part of the user experience. We also aim to align all the user experience journeys so that they all look alike."*
>
> Gerald van Veldhuijsen
> Lead Product Owner, ABN AMRO

3. Caring

Put customers' interests first

Being able to do something gets you only part of the way towards maintaining trust over time. Another major component is taking your customers into account, as well as your business. This is key to getting customers to trust digital interactions from your brand.

Saying you care

You can't assume customers think you have their best interests at heart, you have to tell them that you do and then prove it.

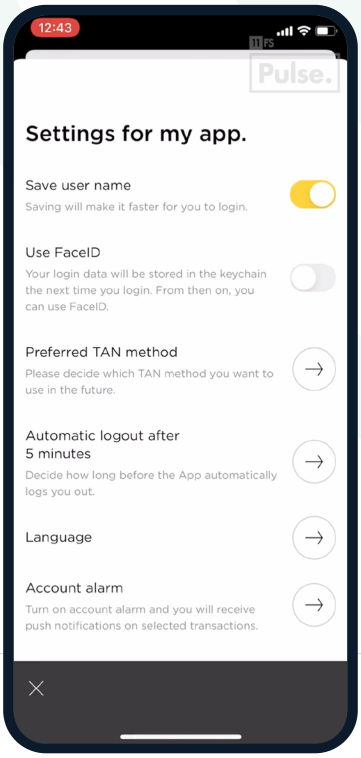
1. Set out an explicit value exchange

Customers need something in return for giving you their money and data. The benefits to the customer should be obvious and explicit (fig. 6).

Many customers are less willing to hand over certain types of personal data, notably biometrics. To combat that unwillingness, providers should explain when they ask a customer to turn on fingerprint or selfie authentication that it benefits them by being more secure than a PIN or password alone. In the US, 72% of consumers are willing to share more personal information if it gets them easier access to accounts in future, according to Experian.

72%
willing to share info
if it delivers easier
future access

"Privacy is not about secrecy, privacy is about consent. We explain that it's fine to pass on information to others so long as you know why, what it's used for and that you can have control over that element moving forward." Dick Dekkers.



Settings for my app.

Save user name ●
Saving will make it faster for you to login.

Use FaceID ○
Your login data will be stored in the keychain the next time you login. From then on, you can use FaceID.

Preferred TAN method →
Please decide which TAN method you want to use in the future.

Automatic logout after
5 minutes →
Decide how long before the App automatically logs you out.

Language →

Account alarm →
Turn on account alarm and you will receive push notifications on selected transactions.

×

Fig. 6.
Commerzbank explains that saving a username will make it faster for customers to login.
Source: Commerzbank, 11:FS Pulse.

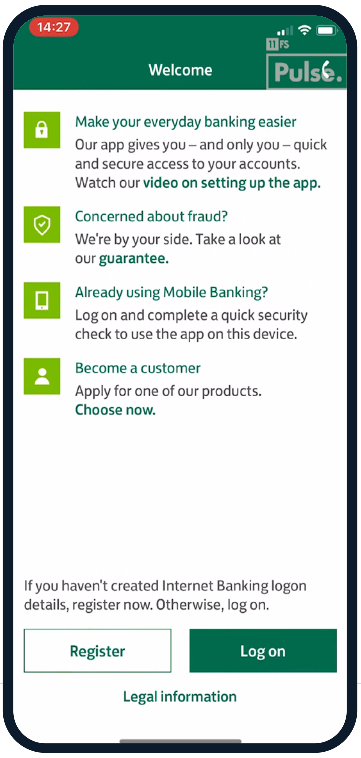
2. Make clear how you protect customers' privacy and security

Customers need to know that their information is being handled sensitively and stored appropriately. Communicating how you care for their data is vital to displaying a sense of empathy and showing that you understand how precious what you are asking for is to its owner.

63% of US consumers would be more willing to hand over personal information if they had evidence that sensitive information was protected, according to a PYMNTS.com survey.

63%
willing to share info
if it's protected

Security promises are a common starting point, but they must be prominent and easily understood to foster trust. Core messages should be reiterated within user journeys — not buried on a page customers have to search for. Short, clear statements embedded early in the user journey reassure customers and save them having to search for information (fig. 7).



14:27

Welcome

Make your everyday banking easier
Our app gives you – and only you – quick and secure access to your accounts. Watch our **video on setting up the app.**

Concerned about fraud?
We're by your side. Take a look at our **guarantee.**

Already using Mobile Banking?
Log on and complete a quick security check to use the app on this device.

Become a customer
Apply for one of our products.
Choose now.

If you haven't created Internet Banking logon details, register now. Otherwise, log on.

Fig. 7.
Lloyds Bank explicitly states it is 'by your side' when customers first download its app.
Source: Lloyds Bank, 11:FS Pulse.

3. Offer more detailed information for customers who want it

Providers should also make it easy for those who want more detailed information to access it through links or pop-ups, while keeping the key messages to the point.

> *"Give the customer the option to 'learn more' about how their data is being used, but also allow them to click straight through if they are less concerned about those details."*
>
> Stephen Ritter
> CTO, Mitek

Proving you care

Once you have clearly communicated to customers you have their best interests at heart, you then have to prove it.

1. Empower employees

Where a customer needs to speak to a customer support agent to answer a query or complete a process, the agent should be able to make decisions based on the situation of the customer in question.

Employee empowerment comes from a business-wide commitment to building trust. Agents should be empowered to make decisions within set boundaries that enable them to show empathy, enabling them to build customer trust that their provider cares about them as an individual.

2. Give customers choice and control

Forcing customers down a specific digital path can make a business more efficient, but it takes control away from the user to the detriment of building trust.

Providers prioritising trust should offer customers choice (fig. 8). Prominent placement of mutually beneficial options and excellent customer experience can encourage usage of these channels, but the need to provide resource-intensive options to some users — to providers' disadvantage — remains.

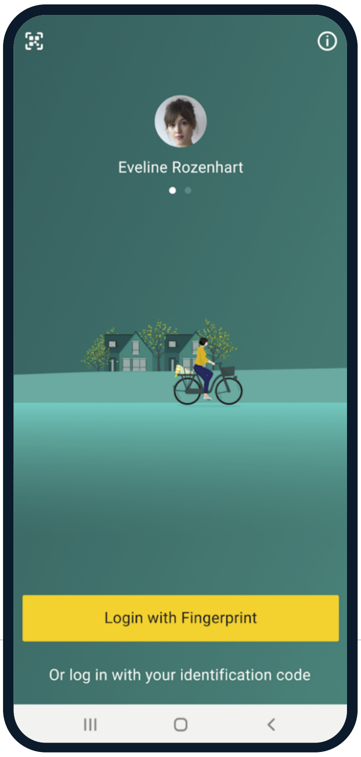


Fig. 8.
ABN AMRO lets customers choose whether they want to login using biometrics or a PIN.
Source: ABN AMRO, Google Play.

> *"It's at those moments where we're able to fix something [for customers] that we're able to really build trust and really build value. For example, we had someone whose card wasn't working — he was in Tesco waiting to pay for his shopping. It was around 8pm in the evening and our banking team was not online to help resolve the issue immediately. He didn't have any other cards with him to pay with, so rather than make him wait for us to fix it the next day, we paid for his shopping."*

Daljit Singh, Chief Design Officer, Anna Money

4. Purposeful

Stand for something

The final element to building trust is proving to customers that you are on their side. Stating what you stand for and proving it through your every action and decision enables customers to feel aligned with your brand and that your interests are complementary.

Define your purpose

Consumers increasingly look for brands that have values that align with their own — according to customer engagement platform Braze, 61% of UK consumers have already stopped using a retail brand because they heard or experienced something they disagreed with.

61%
stopped using a brand due to a clash of values

Meanwhile interest in values-based finance is booming. Assets in sustainable investment funds are expected to exceed those in conventional funds in the next 5 years, according to PwC.

"As a brand, what are you trying to convey and what are you trying to do? If you have some kind of expression in a brand, some kind of personality, you begin to create a relationship between you and your customers." Daljit Singh.

That means there is new urgency for providers to set out what they stand for.

1. Create brand values

Identify what your values are and define core principles that can be upheld throughout the entire organisation. These values need to be clear, widely available and applied consistently.

Scrutiny of providers' actions is greater than ever, and social media and real-time news feeds mean customers quickly find out when firms deviate from their brand values. Making a commitment to inclusivity and then using digital identity verification that is biased against people of colour will see you quickly brought to task once that information gets into the public sphere, for example.

2. Involve employees

A key part of consistent application of values is involving employees in identifying core principles, which will make it easier for them to uphold them. Enforcing values that parts of the organisation disagree with will result in poor company culture and loss of customer trust as Coinbase found out in 2020 when it redefined what it stood for.

"Brand is not just another word for a company, it is that promise that you are making to your customer. Ingrained within it are lots of different things". Daljit Singh.

Be transparent

Customers need to know that you are not doing things that don't align with your brand values, and their own, in order to continue to trust you.

1. Explain yourself

Customers must understand why you are doing what you are doing. That's particularly important for changes in policies, or product and service offerings. Customers need to know why you are making the changes, understand what the changes mean for them and have the opportunity to act on those changes.

If the communication of the changes is done poorly, then you run the risk of customers misunderstanding the impact on them and significant damage to your brand, as WhatsApp found out to its cost in January 2021.

2. Be accountable

Brands need to own their actions, especially when something goes wrong. Attempting to shift blame damages trust in a provider as it's the entity customers hold accountable for keeping their funds and data secure — not any third party that might be involved.

Clear, public explanations of what went wrong and why, and how issues will be fixed are essential. As is outlining what action will be taken to restore lost funds to customers or compensate them for any other negative outcomes such as loss of data.

Being accountable for your actions goes some way to countering the loss of trust that can occur in situations that affect customers negatively.

"Admit when you make mistakes — keeping the customer informed about service outages and potential data breaches helps build trust." Stephen Ritter.

> *"What we have learned as a bank in the last 10 years is that we have to be transparent that the things we're doing are really in the benefit of the customer... It's something that we have to work hard on — making everything that we do as transparent as possible to show what is happening."*
>
> Gerald van Veldhuijsen
>
> Lead Product Owner, ABN AMRO

IN CONCLUSION

Trust requires continuous nurturing

Trust is not a one-off event, it requires continous nurturing

Technology can both help and hinder that nurturing process, depending on how it is implemented. It can provide ease, reassurance and reliability, but it can also come between a provider and a customer.

Successful brands put customers first by thinking beyond pure technical capabilities when implementing digital services, ensuring that they take into account customers' needs and fears and act accordingly.

Providing excellent customer experience should be the focus of any product or service development, and keeping it so will help your customers climb the trust stack and overcome their fears of the unknown.

You can deliver excellent customer experiences by using the framework set out in this report, and ensuring you are:

- Capable
- Competent
- Caring
- Purposeful

11:FS is the challenger consultancy working to change the fabric of financial services. We've assembled the world's top banking, fintech and insurance talent to transform traditional financial services from within, and build new truly digital services from scratch.

We also have a platform called 11:FS Pulse, where users can access thousands of fintech user journeys to benchmark themselves against the competition and gain inspiration for their products.

Digital Identity Verification trusted the world over - secure more high-value customers while reducing risk and costs with Mitek, a global leader and enterprise partner in Identity Verification technology.

Create certainty in today's digital world with Mitek.

Schedule a demo