ABE EBA

EURO BANKING ASSOCIATION

Thought Leadership

DIGITAL TRUST AND THE BANKING SECTOR: TOWARDS A TRUST ADVANTAGE IN THE DIGITAL ECONOMY

EBA Open Banking Working Group

CONTENT

FIGURES

EXECUTIVE SUMMARY

Trust has always been quintessential to the successful operation of a bank and to the functioning of the financial services sector as a whole. However, while trust in the ability of banks to protect funds and carry out financial transactions, thus fulfilling their basic functions on the financial system, is not at stake, their role as trusted providers of comprehensive financial services is being challenged by changing customer expectations, interaction channels, regulation and new players entering the market. This report explores how banks can live up to this challenge and uphold and reinforce their trust role in the digital age, while leveraging it to remain the provider of choice for their customers and even expand their scope beyond that, in the digital data economy. Doing so, this report keeps a focus on retail banking, while many aspects are equally applicable in a corporate banking environment.

While there is not one commonly agreed definition of trust, from a socio-economic point of view, it can be described as one party's willingness to rely on the future actions of another party. Trust, therefore, is a valuable resource. In a transactional context, trust has three components: relational trust, product trust, and process trust. Trust can also be understood as the result of an iterative process of interactions between a trustor and a trustee, where the exhibition of traits, such as ability, benevolence, and integrity, reinforces trust in the other party.

In a digital context, trust, including its relational component, is no less important than in a physical context, but the means to build it are different. In the absence of face-to-face communication, other instruments need to be employed to create trust through digital channels.

In fact, the impact of digital transformation and openness on the trust equation for banks is profound:

- **New interaction channels** and sources of information challenge the authority of bank advisors on financial matters as customers interact through digital interfaces and seek to inform themselves through online resources and peers.

- **Convenience** is a factor that, depending on context, either challenges trust in importance or even becomes a trust factor itself and thus needs to be taken into account in every interaction.

- **Customer attitudes and preferences** are evolving – especially with regard to younger generations who do not have the same history of seeing banks as inherently trusted institutions as the generations before them did.

- **Second Payment Service Directive (PSD2) and the move to openness** in the financial sector can lead to disintermediation, where new players can occupy the customer interface space while leveraging the existing trust in the financial system and changing the banks' role to that of mere infrastructure providers.

- **Data**, and the insights generated from it, occupy an ever-increasing role as source of competitive advantage. Without sufficient data, for example, providing highly relevant, personalised services will become difficult. Consequently, data is increasingly treated as a sought-after currency, albeit not always providing fair and transparent value to customers in return. Overall, surveys support the view that customers trust banks to keep their money safe, but this does not automatically translate into trusting them to provide the best digital service.

To succeed in the digital world, financial institutions and other organisations need to make certain design choices in a range of areas: security, user experience, degree of customer control, use of data, and openness. Financial institutions should make those choices in order to maximise relational, product and process trust.

Especially in financial services, trust is the basis for a more intimate customer relationship and for data to provide superior value, based on fair and transparent standards. Banks have a solid basis on which to build on to achieve this and beyond.

To build and leverage their digital trust advantage, banks should consider three steps:

1. **Build digital trust, based on the bank-inherent trust advantage, to differentiate from other market players.** To do so banks should, as a basis, implement highly robust measures around data security. Pursuing and putting in place principles of consistent customer control and the responsible use of data are further required to build trust. When engaging in Open Banking, banks should develop a stance on how to ensure minimum standards of security, privacy and controls for their ecosystem partners. Finally, all this should be reflected in a consistent and designed-for-purpose user experience.

2. **Become a trusted advisor to their customers, enabled by digital trust.** With the digital trust foundation in place, banks can leverage trust to use customer data in a beneficial way to build relevant customer propositions and engage in Open Banking strategies. They can also ensure superior customer experience across channels, in order to be the prime resource for supporting their customers' financial well-being.

3. **Become a digital advocate providing trust-based services and thus using trust as a direct value driver.** This includes roles such as the provider of digital identity or attributes, using verified customer data to which the bank has access, as well as going beyond to manage non-financial data on behalf of the customer, or provide consent management and data access services to customers, supporting transactions in the digital economy beyond the bank's realm.

Collaborative measures within the non-competitive space in the banking sector can complement these steps and bring value to consumers. These may include:

- common alignment on principles around the responsible and trustful treatment of customer data

- technical standardisation of Open Banking, Application Programming Interface (API) access and data structure

- bank-led co-creation of a soft infrastructure to enable services such as digital identity provision or overarching consent and data access in the digital economy

The recommendations in this report are intended to highlight the value of trust, generate awareness among the banking industry and motivate banks to develop a strategy towards systematically improving their trust position, while exploring opportunities for strengthening sector-wide competitiveness through collaborative approaches to trust-creation that ultimately will benefit end-users.

As this report was being finalised, the Corona pandemic has impacted the world on a global scale, challenging societies not only to find ways

to counter the immediate threat of the virus, but also to adapt to the new realities at an extremely fast pace. From having to embrace non-cash payments in cash-affine countries like Germany and coping with steeply rising online purchases, to the increased use of digital social channels and conducting business meetings remotely from home, the behaviour of individuals across the globe is undergoing rapid digital transformation. Many of these changes are likely to last even after the crisis subsides[1].

The overall shift to digital has been accelerated by the pandemic, including the sharing of health data, be it for contact-tracing or improving treatment research. This further underlines the need for trusted ways of providing consent and sharing data in a controlled manner[2] and increases the opportunity for banks and the financial sector to organise in a role of "digital advocates" as outlined in this report.

As these major transformational developments will lead to a "new digital normal", the topic of this report becomes even more important and its call to action more pressing. The players who take bold steps towards mastering digital services based on digital trust will be best positioned to succeed in the post-crisis era.

1 According to EHI Retail Institute (2020), the percentage of German shoppers preferring to pay cash at the point-of-sale has dropped from 38% to 18% since the start of the pandemic. One recent study finds that in Europe's largest e-commerce markets, the percentage of consumers doing more than 50% of their shopping online has increased significantly (see "Surge in ecommerce will outlive corona across Europe, consumer research suggests," Internet Retailing, accessed March 5, 2020, https://internetretailing.net/covid-19/covid-19/surge-in-ecommerce-will-outlive-corona-across-europe-consumer-research-suggest-21231). The need for businesses to accelerate digital transformation is addressed, for instance, in a recent HBR article, arguing that now, "digitizing the operating architecture of the firm is not simply a recipe for higher performance, but much more fundamental for worker employment and public health. This is creating a new digital divide that will deepen fractures in our society. The firms that cannot change overnight will be left way behind, exposing their employees to increasing risk of financial and physical distress" (M. Iansiti and G.Richards, Coronavirus Is Widening the Corporate Digital Divide, Harvard Business Review, March 26, 2020, https://hbr.org/2020/03/coronavirus-is-widening-the-corporate-digital-divide).

2 See, for example the article "Data sovereignty holds the key to widespread adoption of COVID-19 apps", INNOPAY, accessed May 12, 2020, https://www.innopay.com/en/publications/data-sovereignty-holds-key-widespread-adoption-covid-19-apps.

1 INTRODUCTION

Trust is the centrepiece of the financial system. Without trust, customers would not deposit their money at banks, banks would not lend money to borrowers, and financial transactions would not occur. Even more than in other sectors, trust plays a central role in bilateral relationships between financial institutions and their customers.

Trust in financial institutions has taken a hit since the financial crisis of 2007-08, with respect to the stability of the banking system, as well as in the behaviour of individual institutions or their employees. Some surveys state[3] this trust has not fully recovered to pre-crisis levels. But after government intervention, reform of banking supervision, and industry recovery, trust in the financial system and the institution "bank" does not seem to be seriously at risk. In fact, banks still enjoy a trust advantage over other participants in the economy.

The trust embedded in the financial system and its institutions has allowed the latter to be unique providers of short- and long-term financial well-being of their customers. But, as digital transformation gains speed and the sector opens up, dynamics that have a profound impact on the structure of the bank-customer relationship and on the role and the shape of trust in it kick in.

This report sets out to explore the implications that the age of openness and digital transformation have for trust in the financial sector. It identifies courses of action that financial institutions ought to embark on in an effort to reinforce, extend and leverage their trust positions in the digital economy. While it looks at the subject from a retail banking angle, many of the learnings can also be applied to corporate banking.

In doing so, it takes a look at the basic concepts of trust and how they apply to the financial sector. The report differentiates between trust in the financial system and bilateral trust between a bank and its customers, even though they are not independent. Also, it argues that trust, along the dimensions of relation, product, and process, is the result of an iterative process of continuously exhibiting certain behaviour by financial institutions – competence, benevolence, integrity.

3 E.g. Lawrence White, "British public don't trust banks 10 years after crisis, survey finds", Reuters, August 18, 2018, https://uk.reuters.com/article/uk-britain-banks/british-public-dont-trust-banks-10-years-after-crisis-survey-finds-idUKKBN1L11EL.

The report also identifies how a range of dynamics within the digital transformation of society impact the trust equation for financial institutions. First, the unbundling of financial services through PSD2 and Open Banking allows other players to enter into the financial ecosystem and compete for customers' trust while still relying on the fundamental trust in the system provided by banks. Second, digital customer interfaces replace personal contact, requiring banks to rethink how trust is built up through digital communication. Third, a preference for convenience, or more broadly, great user experience, introduces new trust criteria that need to be fulfilled. Last, but definitely not least, transactions increasingly become about data. The use of data analytics and artificial intelligence (AI) to generate customer insights has converted data into a valuable asset and, implicitly, into a currency that companies can work with, but which also needs protection. How digital data is handled has an essential effect on trust.

Against this backdrop, financial institutions need to determine their sweet spot in order to remain competitive, individually and as a sector. More specifically, a bank needs to combine the principle success factors in the digital economy (openness, security, data analytics, customer readiness, and user experience) in a way that leverages their core assets and strengths to uniquely position itself for customer trust, leading to a **collaborative digital trust advantage**. On the level of the individual institution, it includes using technology, processes and communication to reinforce the digital trust foundation, complemented by sector action to define common technical standards around the usage of customer data. It also involves using available data in the right way for the benefit of the customer. Finally, in a combined effort on an individual and a collaborative level in the non-competitive space, financial institutions may leverage their trust advantage to build services around trust itself and by doing so, play a broader, vital role for the digital economy that would bring significant benefits to consumers. Provision or management of digital identities is one possible application in that area.

This report builds on several of the Open Banking Working Group's previous publications, including the reports on Open Banking, APIs (Application Programming Interfaces), Artificial Intelligence and Digital Identity, and takes a look at these topics from a trust perspective.

The remainder of the report is structured as follows: Chapter 2 introduces basic concepts of trust. Chapter 3 sheds light on the role of trust in the financial sector and highlights the challenges brought about by digital transformation. Chapter 4 identifies the principle success factor in digital business and relates them to trust. Chapter 5 develops the concept of the Collaborative Digital Trust Advantage, makes some recommendations for financial institutions and the sector, and elaborates on specific trust-based use cases for banks. Chapter 6 concludes with an outlook.

2 A BRIEF EXPLORATION OF TRUST

This chapter explores the concept of trust and how it applies to the financial sector. It sets the context for chapter 3 that addresses the specific challenges arising from digitalisation.

2.1 BASIC CONCEPTS OF TRUST

Trust is a complex concept and used in a large range of different contexts. To establish the terminology of trust, this section first defines the general idea of trust as well as different concepts of trust. Second, it zooms in on the concept of transactional trust and describes a basic mechanism of how trust is created.

2.1.1 A definition of trust

In research, trust has been viewed through diverse disciplinary lenses: economic, social, institutional, behavioural, and psychological. Consequently, there is no single and universal definition of trust. In a social context, trust could be expressed as **one party's willingness to rely on the future actions of, and thereby increasing its vulnerability to, another party**, whose behaviour is beyond the trusting party's control.[4] Trust reduces the perceived risk in an interaction, and as such is a highly valuable resource, which takes long to build but can be lost in an instant. It is required in states of uncertainty with limited or asymmetric information. On the contrary, full certainty about an outcome does not require trust.

2.1.2 Trust in transactions

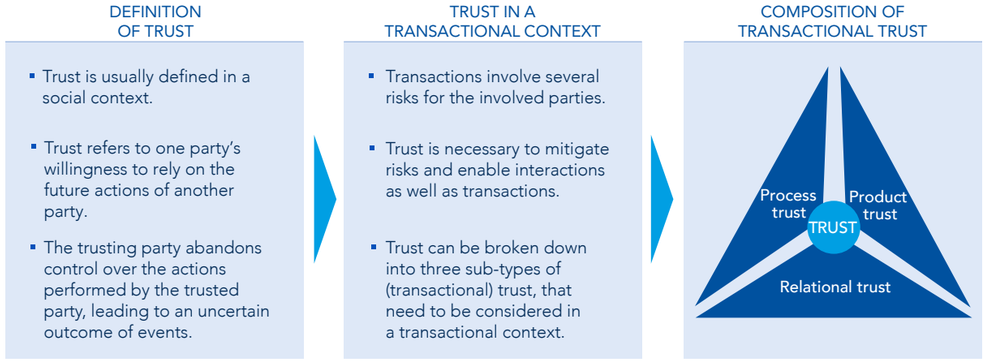
This report uses a transactional concept of trust. Transactional trust has three components, which in sum determine whether parties engage in a transaction, or not. These components are relational trust, product trust, and process trust.

Relational trust refers to the direct trust that one actor has in another. The latter can be a person, but also an organisation. Relational trust is one of the results of an iterative process of interactions and transactions between these two actors. The more "positive" interactions occur between the actors, the stronger the relational trust will become. Likewise, "negative" interactions can let relational trust deteriorate much faster than it

4 Based on a definition by D.E. Zand, "Trust and Managerial Problem Solving", Administrative Science Quarterly 17, (1972): 229 – 239.

Figure 1 – Trust in a transactional context

To enable a transaction, the perceived risks can be mitigated with trust.



Source: EBA and INNOPAY analysis

took to build it. In a physical transaction setting (e.g. buying a bottle of wine in a shop), relational trust is typically driven by the personal interaction between customer and salesman, whereas in a digital setting (buying the same bottle online), it is, for instance, generated by reputation data, such as user ratings.

Product trust relates to the trust that the quality of a product or service meets the buyer's expectations. As the transactional trust components are interrelated, a product meeting or exceeding the buyers' expectations would also reinforce relational trust, whereas failing to do so would have negative repercussions. In a physical setting, product trust may be driven by trying out the product in store. In a digital environment, however, this may be replaced by extensive product comparisons and user reviews.

Finally, **process trust** describes the trust in the transaction process itself, which includes, in generic terms, agreement, payment and delivery. In essence, physical exchanges with instantaneous payment and delivery, process trust is less relevant, whereas in digital settings or delivery of complex services, it is essential. Process trust can be instilled directly by an actor, or through a broader, abstract system that may include regulations, norms and technical infrastructure. The latter means trusting that a given system is functional and reliable, and that the conventions of the system are adhered to.

2.1.3 The basic trust mechanism

Trust, especially relational trust, does not just exist; it needs to be created. It is important to realise that this happens in iterative interactions between two parties, the trustor and the trustee. The trustee exhibits his trustworthiness through factors that include **ability** (a set of skills, competencies and characteristics to exert influence in a certain domain), **benevolence** (the intention to do good to the trustor), and **integrity** (adhering to a set of principles that the trustor finds acceptable).

The way in which the trustor perceives these factors determines the degree of trust for the trustee. Hence, communication plays a key role in influencing the trustor's level of trust. In balance with the perceived risk in a transactional setting, this will determine the outcome.

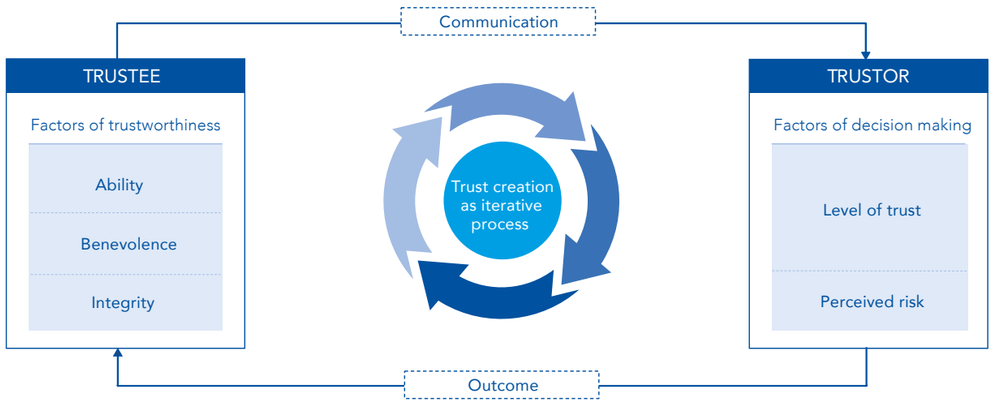
This model, albeit simplified, illustrates the nature of trust creation as an iterative, continuous process, which is determined by actions on both sides, and which is subject to perception and dependent on individual attributes of the trustor.

2.2 TRUST IN A DIGITAL CONTEXT

In the digital domain, transactions are characterised by the physical separation of the transacting parties. In addition, there is usually a time difference between the transaction steps of agreement, payment and delivery, and the use of a digital medium as intermediary between the parties typically replaces physical contact. Frequently, digital transactions also include a middleman in the form of a platform which brings market sides together and facilitates the exchange.

Figure 2 – Trust creation as iterative process

Creation of trust is an iterative process between trustee and trustor.



Source: EBA and INNOPAY analysis, based on Mayer/Davis/Schoorman (1995)

Trust needs to be organised to account for these characteristics of digital transactions. Product trust can, for example, be established through clear product information or comparison websites. Process trust might be created through a clean and straightforward user experience, high levels of security and trusted payment methods.

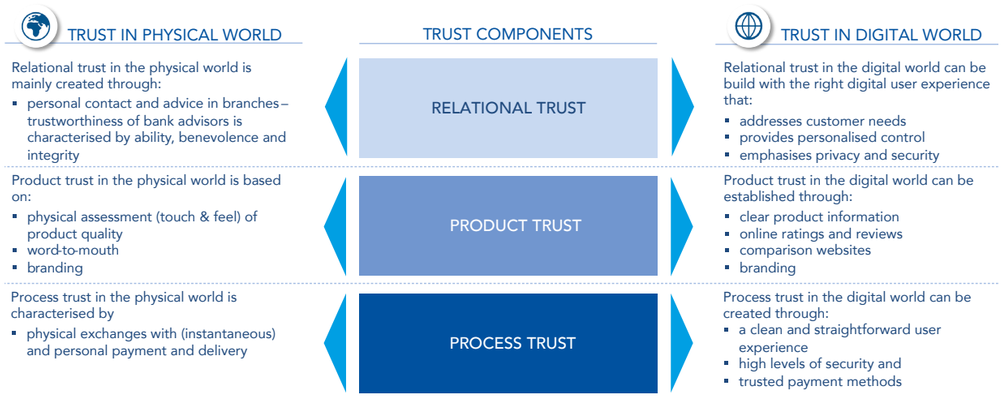
Most notably, the move from physical to digital interactions has profound implications on relational trust, as the most important means – personal contact – breaks away. Against this backdrop, it becomes even more important for companies to use digital means to uphold and further build relational trust and stay close to their customers. In other words, the lack of "physical proximity" needs to be compensated by "digital proximity".

Companies can do so by creating a digital user experience that addresses the customers' needs, provides control, is personalised, emphasises privacy and security and addresses the user through the right channels.

In addition to this, trustful digital transactions also require confidence in the identity of the digital counterparty. This confidence relies on data attributes as a representation of an individual or entity in the digital world, which in turn rely on proper ways of identification and authentication. Therefore, technology needs to be in place that, through these means, allows to reduce the uncertainty implicit in transactions in the digital domain.

Figure 3 – Trust in the physical and the digital world

The creation of trust is transforming in the digital world, changing all 3 trust components.



Source: EBA and INNOPAY analysis

3 THE CHANGING TRUST EQUATION IN THE FINANCIAL SECTOR

3.1 TRUST IN THE FINANCIAL SECTOR

Trust is fundamental for the financial sector to work. This primarily relates to the dependence of any part of the economy on a well-functioning financial system. Thus, trust in the financial system as a whole, of which financial institutions are a part, is crucial. Next to this, there is bilateral trust between individual financial institutions and their customers in the context of business relationships.

3.1.1 Trust in the financial system

The financial system serves a fundamental purpose in the economy in that it facilitates the movement of money, enabling the exchange of goods and services, enables savings and investments, and provides liquidity to the market. For this to function, trust in the system as a whole is essential. This implies trust in the rules, regulations and conventions that govern the financial system, and in the components that make up the system, including the (inter)bank infrastructure as well as the banks themselves.

The nature of financial services explain why trust is so central: First, the steps in financial transactions (agreement, payment, delivery) are disparate in time and space. In an electronic money transfer, whether or when the wired sum reaches its intended recipient is not immediately clear to the sender when initiating the transaction – even though this is changing as infrastructural roll-out and adoption of instant payments is progressing. Second, many bank products are abstract, complex and hard to compare, which makes it essential that at least the party offering the product can be trusted. Third, and most obvious, handling money involves a high amount of vulnerability on the part of the trustor. Financial regulation, adhered-to conventions, technical infrastructure and the institution "bank" ensure that financial transactions are trusted.

3.1.2 Trust in individual financial institutions

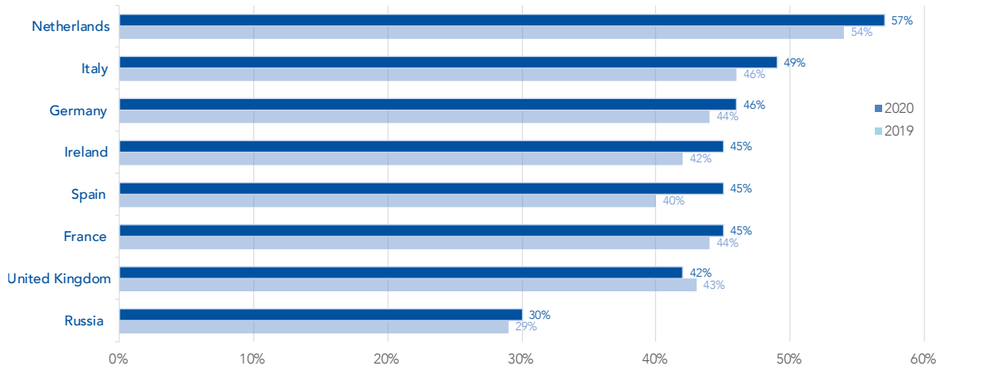
Banks need to convey and maintain this basic trust in the financial system. In this, it is important to understand their dual role for the users of the financial system: as intermediary of financial transactions, and in a direct, bilateral business relationship with a customer.

In their role as intermediaries, banks facilitate a financial transaction between two market parties.

Figure 4 – Trust in financial sector by country

Trust levels in banks increased across all countries other than the UK from 2019 to 2020.

LEVEL OF TRUST IN THE FINANCIAL SERVICES SECTOR IN SELECTED EUROPEAN COUNTRIES IN 2019 AND 2020

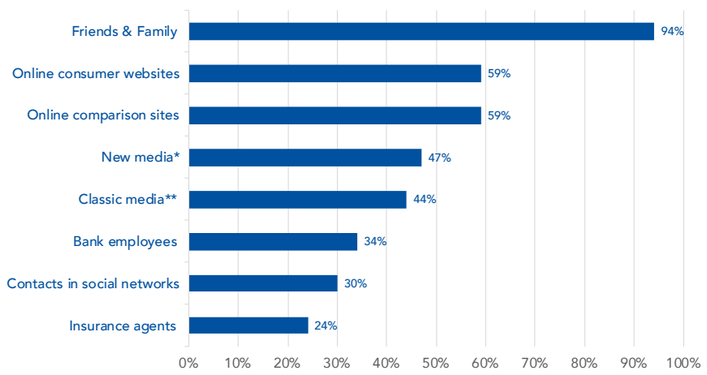


Source: Edelman Trust Barometer, 2020

Figure 5 – Trusted sources for financial information

Friends & family and online resources are trusted more than bank employees.

PERCEIVED TRUSTWORTHINESS OF DIFFERENT SOURCES



- The number of sources that consumers obtain information on financial matters from is diversifying.
- Friends and family as well as different online sources are, on average, considered more trustworthy than bank employees.
- In the digital world, financial institutions need to reach customers via new channels and generate trust via non - personal contact.

* = such as online industry insights, blogs, video-blogs or podcasts
**= such as newspapers, TV or radio

Source: Bitkom Research, 2019; EBA and INNOPAY analysis

Because the market parties trust that the bank as a regulated institution will act in a compliant way, with functioning processes, technology and competent staff, they will transact. Since this kind of trust is placed on all banks in the financial ecosystem – it does not function as an asset that makes one bank stand out from another.

Where individual banks can stand out, however, is in the bilateral trust relationship with their customers. In this, relational trust aspects have traditionally played a fundamental role. It is through actual people that banks have been selling complex financial products to their customers. The trustworthiness – by portraying competence, well-meaning, honesty and adherence to moral principles – of bank employees surrounded by the trust-inspiring walls of a physical bank, have been quintessential to financial institutions' success.[5]

In the course of the financial crisis, the banking sector as a whole has been subject to considerable loss of trust, as evidenced by a whole range of studies. These suggest that, while on the recovery path, trust today is still not back at the pre-crisis levels, which may have an ongoing adverse effect on "the banks". At the same time, these and other studies suggest that consumers still trust their bank more than other types of institutions when it comes to, for instance, security.

While both views, trust in the financial system and trust in individual institutions, are intertwined, the distinction between them is important. Trust in the financial system is jointly created by financial institutions, while individually, they need to build trusted relationships with their customers. The latter aspect is increasingly under pressure through the opening-up of the ecosystem, new channels of interaction, changing customer behaviour and the increasingly important role of data.

5 How this changes with digitalisation is discussed in chapter 3.

3.2 THE IMPACT OF OPENNESS AND DIGITAL TRANSFORMATION

The digital transformation of our society and the economy has a profound effect on how customers and businesses interact. This is expressed in changing customer behaviour and expectations, the use of mobile devices at the frontend and cloud applications in the backend, restructuring of value chains through use of APIs and an exponentially increasing availability of data.

In the financial sector, several drivers embedded in the process of digital transformation have a profound impact on the trust equation for banks.

3.2.1 New channels of interaction and sources of information

Customer interactions increasingly happen through digital interfaces via mobile or online banking, or in a contextual setting along the customer journey in, for example, an online buying process.

Bank customers have access to a multitude of digital sources of financial information and no longer consider bank employees as the only trustworthy source for financial advice. For example, as one recent survey found, consumers consider friends and family, online comparison websites and new media, among others, as considerably more trustworthy for information about financial matters than bank employees.[6]

Financial institutions need to find ways to transport trust into a new, digital setting where physical contact is replaced by digital interfaces. Relational trust factors such as digital branding will become more important, as will the digital creation of

6 According to a survey conducted by Bitkom Research (2019) among German consumers. See Bitkom, "Digital Finance 2019 Die Transformation der Finanzindustrie in Zahlen", October 2019, https://www.bitkom.org/sites/default/files/2019-10/20191001_digitalfinance2019.pdf.

products (e.g. through transparent conditions) and process trust (e.g. through seamless digital onboarding).

3.2.2 The role of convenience

Beyond doubt, convenience or usability is an important determinant of success of any digital service. Some claim that convenience indeed beats any other factor and use the term "digital impatience" to describe the tendency of consumers to expect immediate reward and ease of use at almost any cost. For example, most online shoppers would abandon an e-commerce website, if it was not fully loaded almost immediately.[7]

In financial services, too, the importance of convenience must not be underestimated. One study found that, while not the only factor, ease and convenience of service was the most important one for a retail customer to choose a bank (even before trust in the brand and price).[8]

Ideally, convenience and trust complement each other. For instance, a survey among users of the Swiss e-invoicing platform eBill found that, when paying invoices online, users list the ease-of-use and simplicity of the payment methods, as well as its trustworthiness and confidentiality as the most relevant aspects.[9] In the case of the online shoppers cited above, most of them felt that speed of loading directly impacts the trust they would accord to the online merchant. Meeting the expectations of digital customers in terms of a good digital user experience is a central component of trust.

3.2.3 Changing attitudes of younger generations

Every generation has different views and needs. It is essential for any business to carve out these differences and understand the preferences, motivations and fundamental beliefs of their customers. For instance, the World Economic Forum (WEF)'s Global Shapers Survey draws a rich and powerful picture of the millennials' perspective on the world.[10] Millennials, adults born between the 1980s and early 2000s, carry deep concern for the future – in their eyes, climate change is the most serious global issue we face. This goes hand in hand with a sense of responsibility, as in their view, individuals, not governments, have the greatest role in making the world a better place.

Alarmingly, the trust levels of young people in most institutions are low. According to the WEF survey, only 28% of young people, aged 18 to 35, trust banks to be "fair and honest", whereas 45% do not trust banks in this way. Other types of institutions receive similarly low scores on trust. At the same time, young people across the world show a decided optimism towards technology. In the views of many young people, technology, including the use of artificial intelligence (AI), has great potential to improve people's lives across many economic sectors.

In summary, banks cannot rely on the trust that customers have traditionally put in them – they need to work hard to convince the young people and future generations to trust them by addressing issues that matter to them and putting the correct measures in place. Digital technology needs to be at the heart of these efforts.

3.2.4 Unbundling of financial services through PSD2 and Open Banking

Banks provide the trust in the financial infrastructure and are required to operate the financial system and enable monetary transactions in the economy. They also bear the cost of this in terms of infrastructure investments and regulatory compliance. In the past, this position has exclusively enabled them to build financial propositions on top of the infrastructure. Personal trust relationships were an important cornerstone in how banks marketed their products and services to their customers. In recent years, however, third parties have developed 'overlay services' that piggyback on those interbank rails and by doing so, have challenged banks' value propositions.

The unbundling of the financial services industry through PSD2 and Open Banking has accelerated this change. Through mandated access-to-account interfaces, complemented by other APIs, third parties are now able to enter the financial ecosystem by plugging into basic banking functionality and obtaining account data in order to build compelling customer propositions. In other words, banks lend their systemic trust to new entrants and bear the risk of losing trust if something goes wrong.

3.3 THE CHANGING ROLE OF DATA

3.3.1 Data as asset and currency

With digital transformation, more data becomes available by the day, driven by a growing number of people around the globe creating digital profiles and digital transactions in the Business-to-Consumer (B2C), Business-to-Business (B2B) and Internet of Things (IoT) spaces. It is estimated that the amount of data in the global datasphere will increase by more than 400% from 33 zettabytes in 2018 to 175 zettabytes in 2025.[11] More and more of this data will be available for financial service providers to potentially put to use.

As the EBA Open Banking Working Group (OBWG) report on "Artificial Intelligence in the age of Open Banking"[12] points out, machine learning can help convert data into valuable insights, which in turn can be leveraged to provide highly personalised customer propositions. But to do so, high quantities of high-quality data are required. Hence, data becomes more valuable, and its value increases with its relevance and reliability.

The personal experience of the user of data will improve with the degree of data structure and data quality. Digital organisations can only succeed in bringing value to customers when products and services are matched with what the customer requires. This means that algorithms that use data to offer service need quality input to create an optimal offer. If the customers are

7 Olaf Kolbrück, „Ungeduldige Online-Kunden: Drei Sekunden bis zum Abbrucht", e-tailment, 16 February 2015, https://etailment.de/news/stories/Ungeduldige-Online-Kunden-Drei-Sekunden-bis-zum-Abbruch-3070.

8 See Capgemini and Efma, World Retail Banking Report 2018; 47.3% of respondents indicated that ease and convenience of service had high or very high influence on their decision, vs. 44.6% for trust with the brand and 43.4% for price/rate.

9 Source: SIX, Non-public survey provided to author, 2019. Together with mentioned factors, providing a complete overview over one's invoices is also among the most relevant aspects for users.

10 The survey comprises a sample of 24,766 respondents in the age of 18 to 35 from around the world. See World Economic Forum, Global Shapers Survey 2017. http://www.shapersurvey2017.org/static/data/WEF_GSC_Annual_Survey_2017.pdf.

11 IDC White Paper, "The Digitization of the World. From Edge to Core," November 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. 1 zettabyte equals 1 billion terabytes or 1021 bytes.

12 https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/management-summary-artificial-intelligence-in-the-era-of-open-banking/

RECENT RESEARCH ON TRUST AND DATA IN A PSD2 CONTEXT

In a recent series of papers, researchers at De Nederlandsche Bank (DNB) investigated the relationship between trust and data-sharing in the consumer-bank relationship in the context of PSD2. In the first paper, they examined the attitudes of Dutch consumers towards different uses of their payment data by their bank. It turned out that the result was highly dependent on both the usage and type of user – sharing data for security reasons, unsurprisingly, was much more accepted than passing it on to third parties for special offers. The research also shows that banks need to be very careful how they use data. For example, selling consumer data would result in high losses of trust and trigger consumers to switch their bank.

In the second paper, the researchers investigated consumer attitudes towards sharing payment data with and using different types of providers that employ PSD2 services. The propensity to use these services, the research suggests, is largely driven by the trust of the consumer in the provider. It turns out that banks have a trust advantage over BigTechs, resulting in consumers being more open to services provided by the banks. Financial incentives however, the researchers found out, can drive consumers to prefer other providers over banks.

Source: See DNB Working Papers

convinced that a better offer will be made if better data is available, they might share data with third parties or their own financial institution more willingly.[13]

3.3.2 The data-benefit balance

When providing products and services based on insights, digital transactions are increasingly about data, rather than about money. Likewise, personal data is increasingly and implicitly accepted by companies as a valuable currency instead of money. Often, consumers are unaware of this concept and of the value of personal data they implicitly pay with when, for example, signing up for “free” services. Pre-eminent online search and social media platforms operate under this principle, among many others. This is illustrated in the “data benefit balance” model.[14]

In the digital world, knowing who you are and where you are going at all times is now worth more than ever. Yet, control over this data is often just given away by the consumer without getting proper compensation in return. This means that the balance between the amount paid and the product delivered in the digital world is in favour of platforms and corporations. The consumer does not know what happens with the data that is left behind after obtaining a product but is targeted again later on based on the earlier transaction. This imbalance in use and transfer of data does

13 M. Bijlsma, C. van der Cruijsen and N. Jonker, “Consumer propensity to adopt PSD2 services: trust for sale?,” DNB Working Paper No 671, 2020, https://www.dnb.nl/en/binaries/Working%20paper%20No.%20671_tcm47-387219.pdf.

14 As proposed by C. Liezenberg, D. Lycklama, and S. Nihland, Everything Transaction (2019).

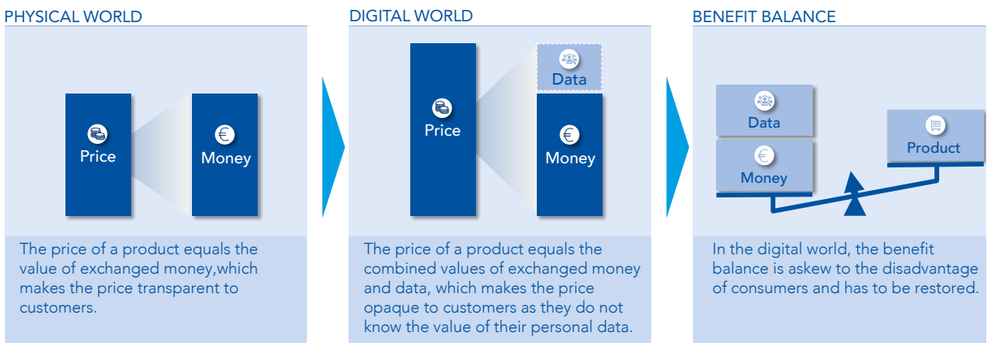
EXAMPLE: MYDATA

MyData is an international non-profit organisation with the goal to empower individuals by improving their right to self-determination regarding their personal data. As organisations around the globe are busy exploring the opportunities of personal data, the core idea is that individuals should have an easy way to see where personal data goes, specify who can use it, and alter these permissions over time. Thus, MyData aims to be both an alternative vision and a guiding technical principle for how users can have more control over the data trails left behind in everyday actions. Data sharing should be facilitated by “Personal Data Operators”, which enable individuals to securely access, manage and use their personal data, as well as to control the flow of personal data with, and between, data sources and data-using services. Ultimately the conscious data sharing should lead to individuals gaining better services in exchange for the data provided.

Source: Public Website, MyData, accessed April 30, 2020, https://mydata.org.

Figure 6 – The data benefit balance

Paying with data shifts the benefit balance of a transaction.



- Achieving a benefit balance is key to a good consumer relationship

Source: EBA and INNOPAY analysis

not facilitate trust based on an equal relationship between buyer and seller. To be able to restore this trust, the data benefit balance needs to be restored, as is also advocated to a less explicit extent by legislation like the General Data Protection Regulation (GDPR).

In the end, the consumer should be empowered to be in control of their own data as well as data submitted to other parties to be able to benefit from what is legally theirs at all times. When the consumer can trust others to be compliant and balanced in how data is handled and used, a world of opportunity opens up for institutions to further establish a trusted relationship with the consumer. This relationship can be used to further optimise use of data in propositions useful to the consumer.

Banks need to strike a sensitive balance of their own with data usage on the one hand and data protection on the other: not carefully treating data as the valuable currency it is will put the reputation and trustworthiness that banks hold at risk. Not using data to improve their customer propositions, might mean they miss out on being able to offer their customers the innovative, value-added products and services they want.

DATA MONETISATION INITIATIVES BASED ON DATA SOVEREIGNTY

The value of data becomes most explicit when it can be monetised directly. While this is a field still in its infancy, first initiatives are on the way. UBDI (short for "universal basic data income"), for example, is a fintech start-up based in the US and Bosnia-Herzegovina which provides a platform that allows users to share their data with companies for purposes of market research. In return for their data, which is shared anonymously using digi.me, a privacy-enforcing sharing app, users get paid in cash, thus combining direct monetisation of own data with privacy.

Source: Public Website, UBDI, accessed April 24, 2020, https://www.ubdi.com.

3.4 THE OPPORTUNITY FOR FINANCIAL INSTITUTIONS

The challenges described above are profound and could significantly alter the way banks form lasting and profitable customer relationships.

New market entrants such as fintechs and BigTechs use their digital DNA to provide flawless digital user experiences to consumers, and some of them possess the amount and quality of data as well as the analytical capability to create customer insights beyond the reach of any bank.

Clearly, banks need to be particularly sensitive in how they use customer data, yet they should learn from and apply best practices in digital business (addressed in chapter 4). On top of that, there is a clear opportunity to build on the trust that financial institutions enjoy, reinforce it by building an infrastructure that encompasses trust around data, embed it into their inner fabric, build compelling propositions based on data and explicit customer consent and, finally, leverage trust as an asset towards the rest of the digital economy (addressed in chapter 5).

4 DIGITAL DESIGN PRINCIPLES AND THEIR LINK TO TRUST

Over the past decade global technology firms have grown rapidly and achieved unprecedented reach and influence by building digital platforms and successfully serving two-sided-markets. Although recent privacy controversies concerning the mistreatment of private customer data have damaged gained trust, their growth has largely been unencumbered.

At the forefront of such tech companies are some of the world's most valuable organisations whose success lies in their ability to identify potential customer needs and fulfil them. Their ability to build easy-to-use products, handle customer data effectively and provide timely responses and resolutions when issues arise has set the bar high for financial institutions who want to improve their customers' digital experiences.

4.1 FIVE DIGITAL DESIGN PRINCIPLES

Any digital business needs to follow certain design principles when making choices that impact trust:

4.1.1 User experience

User experience is how a user perceives the use of a digital product or service and as such, is directly related to trust. While convenience and ease-of-use are important elements, it also includes how directly a product or service meets the needs of the user, whether user interface and content are in line with the users' expectations, and whether a service is reliable. User experience starts with customer onboarding: getting the first step in a customer relationship right will set the tone for subsequent interactions. Businesses that ensure a consistent user experience that is in line with their brand positioning and overall proposition throughout the customer life cycle will increase trust.

4.1.2 Customer control

Customer control is about the degree in which customers are in control of nature and timing of their transactions with businesses and of their personal and transaction data. Digital customers expect to receive service 24x7. In terms of control over their data, at a minimum, businesses need to comply with regulation. While some business

Figure 7 – Digital design choices and their impact on trust

Digital design principles require business to make choices that impact trust.

ELEMENTS OF TRUST AND DIGITAL SUCCESS	EXPLANATION
User experience	How a customer perceives the use of a product or service, including convenience and ease-of-use, brand perception, and in how far it meets the users needs
Customer control	Degree in which customer are in control of how and when they transact with a business, and are in control of their personal and transaction data
Openness	Degree to which a business exposes or consumes APIs around data, functionality or products to enrich own propositions or add to those of 3rd parties
Use of data	How and to what degree customer and other data is aggregated, analysed and applied to generate insights about customers and, e.g., personalise propositions
Security	How and which data protection and cybersecurity measures, in backend and frontend, are applied to protect customer data and prevent attacks

▶ Using the factors of success the elements of trust and therefore the creation, defence and upkeep of trust can be broken down into real world objectives ready to be incorporated into conclusive trust strategies

Source: EBA and INNOPAY Analysis

models are based on less, rather than more control, providing transparency and proper control tools whilst ensuring ease-of-use is likely to have a strongly positive impact on trust.

4.1.3 Openness

Openness is the degree to which companies expose and consume APIs in order to embed their services directly into the customer journeys outside their own realm, where they are most relevant, or provide data and functionalities as building blocks for third-party products. Likewise, products, functionalities or data from external parties are integrated into their own offering to enrich their platform offering, augment own products or their datasets. Openness has the potential to add substantial value for customers, but needs careful handling to ensure security, user experience and branding, among others, are at the required standard. Not handled properly, openness may also have a diminishing effect on trust.

Additional to functional openness, technical openness, e.g. through use of open source, open documentation and platforms like GitHub, allows banks to interact with developer (and user) communities. This community engagement, especially well managed by neo-banks, provides another level of trust into service.

4.1.4 Use of data

Through aggregating and analysing data with the help of artificial intelligence, digital businesses are able to generate customer insights which have the power to result in more personalised experiences, superior products and services, and ultimately more value for the customer. How and to what degree banks/financial institutions use their customers' data is essential for building and maintaining trust relationships. Applied in a transparent way that leaves customers in control and adds clear value, the use of data can increase trust with customers. Used in a non-transparent, too extensive or even incompliant way, it can have a detrimental effect on trust. Inversely, existing trust can make the use of data more acceptable for customers.

4.1.5 Security

As customers disclose personal information with which they engage online to companies, they expect them to keep their data safe. Consumers hold businesses responsible for data breaches, and businesses run a serious risk of losing customers if a cyberattack or a data breach occurs. Indeed, the majority of consumers indicate that they would abandon a business relationship in such a case.[15] Consequently, digital businesses need to have strong cybersecurity and data protection measures in place so they can give consumers the knowledge that their data is safe – a fundamental element of trust.

Financial institutions need to take these design principles as a starting point and define their sweet spot to build and leverage their trust advantage.

4.2 IMPLICATIONS FOR BANKS

There are various ways in which successful digital business models combine these principles and weigh them with respect to each other. Some may potentially be conflicting, such as user experience and security, or use of data and customer control. All of them have impact on certain aspects of trust.

For banks to succeed in digital business, these principles must be aligned to reinforce digital trust as the prime objective. That way, they can build a foundation to serve as a basis for creating trusted digital services and being the partner of choice for their clients when it comes to matters of financial well-being and potentially beyond.

15 According to a Gemalto (2016) report 58% of consumers would stop banking online if a data breach occurs at their bank; overall, 66% of consumers would be unlikely to engage with a business that had experienced a breach of sensitive data. See Gemalto, "Data Breaches and Customer Loyalty Report", 2016.

TOWARDS A DIGITAL TRUST ADVANTAGE FOR BANKS

5

Digital technologies, new communication channels, social media, changing customer expectations and an ever-growing flow of digital data might be a challenge for financial institutions – yet, banks are in a position that works to their advantage. As data abounds, security and privacy issues as well as consumer uncertainty increase. Banks are naturally positioned to provide trust in the digital age by combining rigorous focus on data protection and privacy with customer orientation. This provides banks with the basis for both creating a close/strong (digital) customer relationship and providing digital trust services that go beyond the financial well-being of their customers.

This chapter describes a framework to attain this digital trust advantage, proposes a series of steps and provides concrete examples of actions that financial institutions can take in furtherance of this goal.

5.1 BUILDING THE BANKS' DIGITAL TRUST ADVANTAGE

There are three principle steps that financial institutions should consider in order to fully reap the benefits of the digital trust opportunity:

1. build sustained digital trust based on the bank-inherent trust advantage to obtain a clear differentiator versus other players in the market

2. create close and valuable customer relationships, enabled by the trust created, by leveraging data to the customers' advantage

3. leverage customer trust and data to support customers in conducting transactions – including non-monetary ones – in the digital economy in a safe and secure way

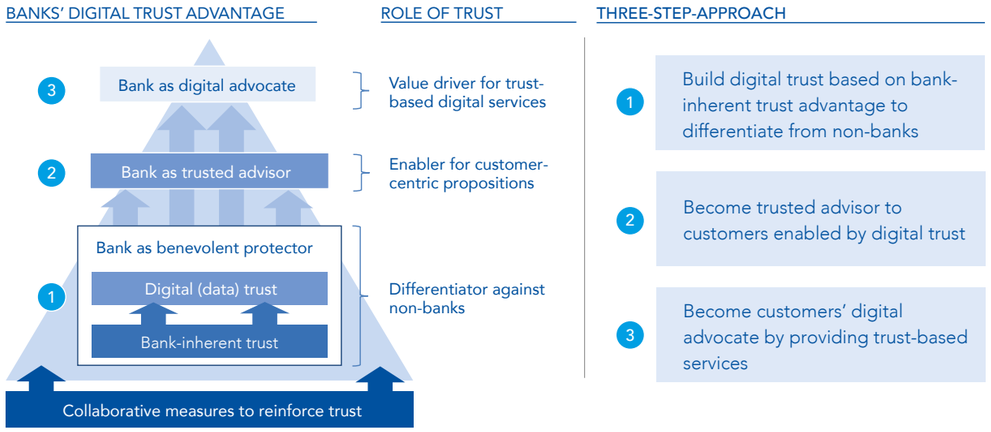
The creation of sustained digital trust is a basis for successful customer relationships in the digital economy and involves the evolution of a bank from an institution that is trusted with money to one that is trusted with data, assuming the role of a "benevolent protector". The inherent trust in banks is an excellent foundation on which to build and implement additional measures that include fit-for-purpose user experience across channels, clear data security and privacy policies and measures, putting customers in full control of their data and generally respecting, protecting and enforcing customers' digital rights in their bilateral relationship. This is where banks can clearly distinguish themselves from BigTechs and other digital players in the market.

Digital trust, once established, enables and legitimises banks to assume the role of a trusted digital advisor that creates customer value through intimate knowledge of their customers' needs and by offering relevant propositions around their financial well-being. As trusted digital advisors, banks' propositions can use the opportunities of Open Banking – for instance by providing a comprehensive financial platform that includes their own as well as endorsed third-party services. Nurturing the customer relationship with relevance and added value will further increase trust – provided it is founded on the principles of the "benevolent protector" role, including the pursuit of a proper data-benefit balance.

Finally, the trust established between customer and bank not only enables value-adding propositions around financial well-being. It can also be leveraged by banks to facilitate and instil trust in other digital transactions, thus helping them to provide trust services to the broader digital economy. Using verified identity data and their available consent/authentication mechanisms, for example, banks can help their customers conduct non-bank transactions more safely and more efficiently. Also, banks can go even further to support and enforce their customers' digital rights in the digital economy per se. These functions are encapsulated in the "digital advocate" role.

Figure 8 – Building the digital trust advantage

Trust can serve as differentiator, enabler and value driver.



Source: EBA and INNOPAY analysis

All steps, from creating the digital trust foundation to becoming a digital advocate, should (and partially must) be accompanied by a range of collaborative efforts on behalf of the banking community in the non-competitive space. These efforts can range from a collective pledge to protecting customers' data rights to establishing a common digital identity scheme or consent infrastructure.

The following sections explore each step in more detail, outlining major components and actions for the banks' trust advantage to materialise.

5.2 BENEVOLENT PROTECTOR: REINFORCING TRUST IN FINANCIAL INSTITUTIONS

As outlined in previous chapters, various surveys suggest that financial institutions still carry a level of inherent trust which is superior to many other types of institutions. Customers feel confidence in financial institutions because they are regulated entities with secure infrastructure subject to supervisory scrutiny. That and the trust built by the classic bank user experience give customers the confidence that banks will keep their money safe. While this is a solid trust base for banks to build on, the trust in the financial system in general and the trust built by classic banking experience in particular, may not be enough for younger generations of customers. The next generation of bank customers has grown up with the internet economy: young customers have different perspectives, needs and behaviours and they tend to show more scepticism towards banks and other institutions while having a stronger belief in technology. In the digital domain, the loss of trust can occur much faster through social media and other channels. To extend the financial institutions' trust advantage into the digital economy, cater to changing customer expectations and reduce the likelihood of losing trust, financial institutions should look at a range of measures to drive digital trust and further differentiate from other players in the digital economy.

5.2.1 Enhanced data security

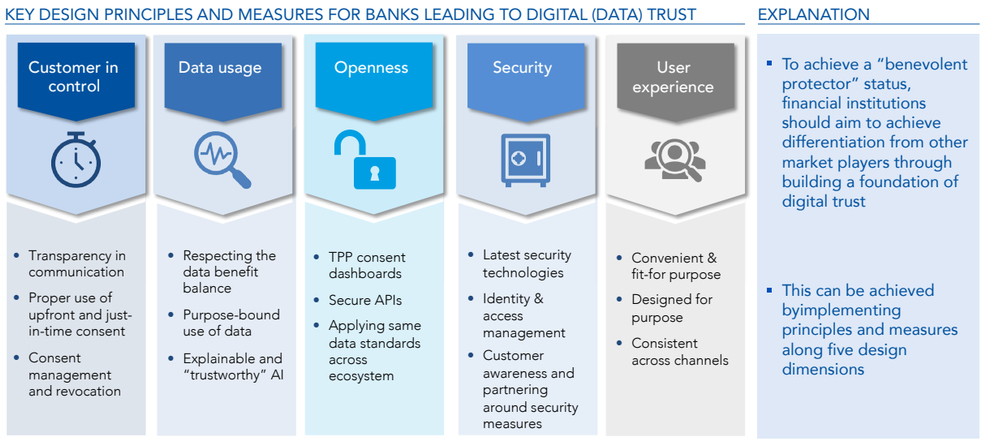
While security is the basis for people's trust in financial services, bank customers only become aware of their bank's security when it is breached. They do not receive a notification every time their bank's security systems prevent service interruption and data or money theft. Yet, a single security incident can impact trust in an organisation for years to come. More awareness about the investments in security that are made by financial institutions and the actions needed by both the institution and the customer to stay secure can help build trust.

Given the regulatory requirements around security for financial institutions and the historical investments made in it, their security foundation is solid. One of the security measures that stands out most for financial institutions is their authentication framework and the way transactions are monitored. Strong customer authentication as mandated by PSD2 can enhance trust if explained well and implemented using user-friendly technologies. Transaction monitoring systems are key to intercept potential fraud and crime and need to be updated continuously to be able to provide institutions with correct insights.

Security's weak spot often is the human factor interacting with a system. It is therefore of great interest to financial institutions to have the customer aware of the security measures put in place and involved in the process of making products and services more secure. Actively partnering with customers on enhancing security may involve, for instance, encouraging them to set limits to payment amounts or geographical boundaries of

Figure 9 – Aspects of building a digital trust foundation

Benevolent protector: Financial institutions should expand on their trust position in the digital domain.



Source: EBA and INNOPAY Analysis

payment card usage. Likewise, institutions can update customers about new cases of fraud, push messages to validate transactions and being in control of their own spending limits at all times.

5.2.2 Consistent customer control

To safeguard and further develop the trust many consumers put in financial institutions, banks should go beyond mere compliance with relevant regulation such as GDPR and PSD2: they should fully embrace and consistently apply the principles of transparency, consent and control to promote and defend the data rights of their customers. Financial institutions need to guide all activities related to collecting and processing customer data, leading up to highly responsible data-privacy practices that drive customer trust. The assumption of customers owning their data – and banks taking good care of them – should, just like the assumption of customers owning their money, be embedded in all the bank's actions.

The principle of transparency encompasses clear communication and education of bank customers about which data is collected, how it is used, and the consequences of its use. Banks should do this in a language that is concise and easy to understand, and within a relevant context. For example, in customer journeys such as account openings or credit applications, information boxes should explain in plain language why certain information is asked from the customer and in what way it will impact the outcome. In another example, when cross-selling products such as a loan, the financial institution should explain on which basis it has assumed that this may be valuable for the customer. Pursuing consistent

transparency around data will increase data literacy of customers as well as relational trust.

Consent is defined by GDPR as the "freely given, specific, informed, and unambiguous indication" of a customer's wishes with respect to the processing of personal data. Where consent is required, rather than merely complying with the regulation, financial institutions should ask for consent in a way that is meaningful, comprehensible and valuable for the customer, using both "upfront consent" and "just-in-time consent" in an appropriate way. Ideally, upfront consent, i.e. preemptively asking for permission to use data at the beginning of a customer relationship, should be limited to what is absolutely necessary. Consent to use specific data should be obtained just-in-time when the need arises, together with a clear statement of the benefit of sharing the data.

Lastly, financial institutions should give customers full control of their data by enabling them to manage and revoke their consents. Moreover, it matters how the management and revocation of consent is implemented. First, the option to manage consent should be readily accessible in the digital customer interface. Second, changing consent should be sufficiently simple. Third, the effect of a change or revocation in consent should be as immediate as the effect of initially providing consent. Finally, the granularity of consent should be sufficient to accommodate varying degrees of willingness to share data. As with the provision of consent, financial institutions should be vocal and transparent about the effect of changing, or fully revoking, consent (for instance by indicating in how far the quality of certain functionalities is impacted by not sharing certain data).

5.2.3 Responsible use of data

The use of data is essential for banks to provide the tailored experiences customers expect in today's world. However, banks, maybe more so than other digital businesses, have to be very careful about which data to use and how to use it to reinforce the trust of their customers, rather than put it at risk.[16]

Chapter 3.2 explained the need to bring back a **data benefit balance** between customers (initial owners) and institutions (users and owners of the outcome of data use). Financial institutions should fundamentally embrace the idea of creating a fair value exchange based on data with their customers. Every use of customer data should occur with the customer benefit in mind. Consistently delivering value on data and being transparent on how data is used in the process can become a key pillar to build trust with customers in the future.

Data used for financial purposes should be purpose-bound, i.e. financial institutions need to be able to define what data is needed and why. Based on providing customers with the benefits of their own data, it can be argued that apart from GDPR, customers have the right to know why certain data is relevant for performing a specific transaction. Making the purpose of data used specific both internally and to the customer helps provide maximum value while minimising the amount of data required.

Related to transparent and purpose-bound data use, the nascent area of **explainable AI** will become highly relevant. Undoubtedly, artificial intelligence already plays an important role in generating insights from large amounts of data and financial institutions cannot afford to ignore it.[17] Explainable AI strives for making the black-box decision-making of machine learning transparent by inspecting and understanding the steps involved. This includes comprehending how conclusions are reached as well as establishing traceability and possibilities for inspection. While still an emerging field, explainable AI has great potential to increase trust in the use of automated insight generation from data.

5.2.4 Controlled openness

Opening up to third parties is a given for financial institutions today. PSD2 requires all banks within the European Union (EU) to provide access to third party providers and engaging in Open Banking beyond regulation is a useful strategy for many banks. At the same time, openness presents challenges regarding data trust, which banks need to address.

Sharing data with third parties through APIs presents new attack perimeters for cybercriminals.[18] Third parties may have less strict security measures in place and less resources dedicated to the topic, making them an easier target for data theft. Also, in a more complex ecosystem, phishing attacks may increase. While banks have limited control over the domains of third parties, they need to protect their APIs with secure access protocols and should exercise appropriate scrutiny in identifying, admitting, and monitoring

16 The Finnish innovation fund Sitra initiated the IHAN fair data economy project to establish a blueprint, defining legal, business, technical and administrative rules that organisations need to comply with when sharing data. In addition to privacy and data protection requirements, it particularly devotes attention to ethical principles.

17 For further insights on the use of AI in the financial services sector, consider the previous OBWG publication EBA Open Banking Working Group, "Artificial Intelligence in the era of Open Banking," June 2019, https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/management-summary-artificial-intelligence-in-the-era-of-open-banking/.

18 See, for example, Feike Hacquebord, Robert McArdle, Fernando Merces and David Sancho, "Ready or Not for PSD2: The Risks of Open Banking", Trend Micro Research,2019, https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf.

EXAMPLE: BOSCH CODE OF ETHICS FOR AI

Bosch Group, a leading global supplier of technology and services, predicts that by 2025 all its products will have AI embedded or be produced using it. In February 2020 Bosch Group issued a code of ethics for AI on the grounds that trust in AI will be essential for success, and that it will not be trusted if it is a black box. The code is based on the maxim that humans should be the "ultimate arbiter of any AI-based decisions". It defines red lines that will not be crossed (such as trade-off decisions on human life), guiding principles to be followed and criteria for the use of AI. Also, it commits to three approaches to the role of AI in decision making:

"Human-in-command" (HIC) – AI is only a tool and humans make the decisions; "Human-in-the-loop" (HITL) – people can directly influence or change decisions made by AI; and "Human-on-the-loop" (HOTL) – people define the parameters of decisions delegated to AI, while those affected of AI decisions are able to apply for review.

Agreeing and publishing such an ethical code helps Bosch as internal guide for actual development and application of AI. It also sends an external signal to strengthen the trust of their customers.

Source: Bosch, "Bosch code of ethics for AI, press release, 19 February 2020, https://assets.bosch.com/media/en/global/stories/ai_codex/bosch-code-of-ethics-for-ai.pdf.

third parties consuming their APIs. Likewise, in banking-as-a-platform plays, banks should ensure that any third-party service offered to their customers adheres to similar data protection and privacy standards as those of the banks itself.

In a PSD2 context, banks should think about the role they want to play in third party provider (TPP) data access and whether to actively support their customers in managing it. Some banks may choose to leave the provision and revocation of consent for account access entirely to the payment services user (PSU) and the TPP, limiting themselves to providing access to TPP when formal requirements are fulfilled. In an endeavour to drive trust, banks could also opt for a more active stance, provided that national competent authorities (NCAs) allow them to do so. This can include providing an overview of all active and historical consents given to TPPs to their customers, e.g. in the form of a dashboard. To go one step further, banks could implement a privacy dashboard that allows setting more granular permissions and, for instance, enables customers to block the sharing of certain types of transactions for privacy reasons, thereby providing a concrete means to operationalising GDPR.

Some NCAs currently bar banks from cutting access by a third party to a customer's account, even if requested by the customer, due to concerns that it might be done inappropriately. They require customers to directly approach the third parties. This, however, undermines customers' ability to effectively exercise control over their data and who is using it. This limitation would need to be remedied before such customer dashboards can be implemented in concerned jurisdictions.

5.2.5 User experience as catalyser

With ever increasing use of technology, a large part of trust manifested in every interaction with the customer is based on the user experience in digital products, rather than the interactions with people in real life. To give their customers a user experience that elicits trust, banks need to funnel customer control, security, data usage and openness into consistent, convenient, and fit-for-purpose user interactions in line with their overall branding. Balancing those four aspects is key to promoting trust. For instance, in a digital process that has been optimised for convenience, customers may feel more secure, if the bank adds an additional checkpoint to confirm whether they want to execute a certain action. Further, trust-enhancing features like two-factor-authentication can be designed in a highly user-friendly manner using, for instance, mobile technology, biometry, and app-binding.

One key aspect in user experience should be **design for purpose**. It can be assumed that customers interact with financial institutions for a specific reason and with a goal in mind. Therefore, a clear start and end of each interaction is required to let the customers know the status of their request and the nature and purpose of the data processed. Financial institutions should be extremely clear about the purpose of each interaction and model the user experience in a way that supports the interaction's purpose and the customer's expectation.

Last, the user experience should be as **uniform and consistent** as possible throughout all products and channels of the financial institution. Trust in the institution is based on its brand and how it is viewed, as well as the way customers interact with the brand. Having a consistent experience makes sure that customers can identify themselves with the same trustworthy organisation at all times.

EXAMPLE: MONEYOU CONSENT DASHBOARD

Within the context of PSD2, financial institutions for the first time were obliged to provide appropriate online-banking access to third party-services which their customers wanted to use. In order to facilitate and ensure the above-mentioned principles, Moneyou chose to embed a "Consent Dashboard" within their primary banking app.

The dashboard entails an overview of all current/active confirmations of consent for data sharing, which the customer has explicitly given to (external) third parties. It also includes the date of consent provision and the specific data types shared. A consent history is also available. A detailed view shows further in-depth information such as end date or scope of sub-accounts.

Most importantly, the dashboard also includes the option of revoking consent, allowing the customers to be in full control of their consent confirmations without needing to leave the banking app. The technical implementation allows for audit-proof traceability in case of disputes.

While not required by PSD2 (and subject to scrutiny of the NCA in some jurisdictions – see 5.2.4), Moneyou prioritised the dashboard functionality to give full control over their data to customers in a convenient manner.

Source: MoneYou

5.2.6 Collaborative implications

GDPR and PSD2 have introduced and further pushed various aspects of customer control and data privacy from a regulatory perspective. Each financial institution can individually choose to go beyond these minimum requirements to establish trust around data to a degree that lets it stand out of the crowd. At the same time, there is a case for banks collectively engaging in setting and practicing technical data standards that set the bar for the whole industry, broadly reinforcing trust in banks and setting banks apart from other players.

The English banking community, for instance, has issued a whitepaper on the ethical use of customer data in 2019, putting forward five principles of data ethics.[19] A step beyond a set of principles would be to establish protocols and breaking down principles into concrete measures - dos and don'ts to which individual banks can subscribe. Whether at a level of principles or protocols, banks could establish common ground in the financial sector.

Concrete sector-level technical standards for data usage can provide a basis to actively strengthen reputation and trust in the banking sector.

5.3 TRUSTED ADVISOR: CREATING VALUE BASED ON TRUST

Creating trust around data by following the principles outlined in section 5.2 provides a foundation upon which financial institutions can build a trusting relationship with their customers. It also enables them to collect the intimate

19 See UK Finance, "Ethical Use of Customer Data in a Digital Economy", March 2019, https://www.ukfinance.org.uk/system/files/Data-Ethics-White-Paper-FINAL-ONLINE.pdf. Principles put forward relate to respecting human agency, safeguarding equality and fairness, delivering transparency, sponsoring organisation-wide approach, and establishing accountability.

understanding of their customers needed to provide valuable advice and propositions that will keep them in the position as their customers' premier and most trusted financial advisor throughout their different life stages. In turn, providing consistent value is also a major propellant for further trust. To do this, based on their trust position as "benevolent protector", financial institutions should focus on three major areas: use data to gain an intimate understanding of their customer and create personalised offerings; leverage Open Banking to provide propositions that cater to customers' core needs; and provide a superior experience across channels.

5.3.1 Intimate customer understanding based on data

Only with the use of customer data will financial institutions be able to understand their customers to the degree needed for providing truly relevant offerings. The inherent trust placed in banks, enhanced by digital trust measures detailed in the previous section, provides banks with the basis for using data in the best interest of customers. Focused, scientific research as well as broad, international surveys support this notion.[20]

An important first step is proper customer segmentation based on personas. Customers not only differ in their needs, but also in their attitudes towards sharing their data. Generally, younger people with a higher digital affinity tend to be more open to sharing data in return for benefits than older customers. But even in the latter group, according to the 2019 Global Financial Services Consumer Study, a majority of consumers are open for certain value exchanges based on data. Benefits that find most support include advice more relevant to personal circumstances, more competitive prices and faster, better services.

Examples for data-driven value for customers can range from proposing personalised next-best products to encouraging saving habits based on spending patterns or suggesting investment opportunities based on risk profiles – to name but a few. The use of predictive analytics can help to create more granular personas as a basis for personalisation.

5.3.2 Propositions addressing core needs with Open Banking

Previous reports of the Open Banking Working Group have explored how Open Banking enables financial institutions to enrich their own customer proposition by integrating product, features or data from third party providers (banking as a platform), as well as by exposing APIs (banking as a service) to embed their own products in customer journeys outside their own environment.[21]

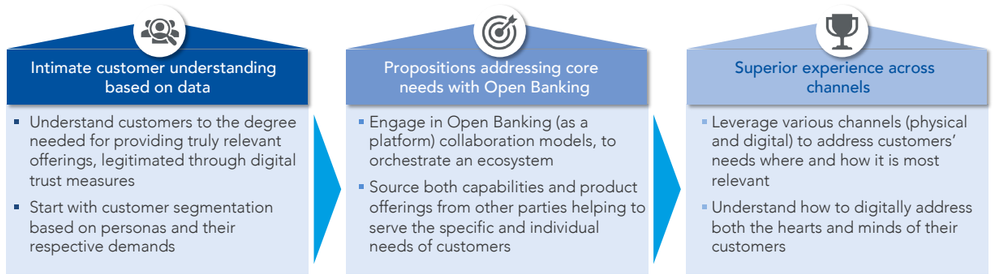
Customers expect propositions that address their needs in a relevant way – beyond basic financial services. Living up to these expectations will be aided by engaging in Open Banking (as a platform) collaboration models and sourcing both capabilities and product offerings from other parties which help serve the specific and individual needs of their customers. For example, banks might be offering flexible insurance products in line with specific life situations or circumstances of the customer, or external investment or savings products. They could also go "beyond banking" to mobility, energy, or housing, for instance.

20 Biljlsma, van der Cruijsen, Jonker, "Consumer propensity." ;Accenture, "Discover the Patterns in Personality," Global Financial Services Consumer Study, 2019, https://www.accenture.com/_acnmedia/pdf-95/accenture-2019-global-financial-services-consumer-study.pdf.

21 See in particular the EBA Open Banking Working Group reports on "Understanding the business relevance of Open APIs and Open Banking for banks," May 2016, and "Open Banking: advancing customer-centricity", March 2017.

Figure 10 – Elements of becoming a trusted advisor

Building on their trust position as benevolent protector, banks should strive to become trusted advisors for their customers also in a digital environment.



Source: EBA and INNOPAY analysis

Assuming the role of benevolent protector as laid out in section 5.2 will enable financial institutions to assume the role of trusted advisor by orchestrating an ecosystem of services meeting specific client needs. As they do this, it is essential that the banks set the level of trustworthiness and impose the same standards on the ecosystem – expressed in consistent user experience, standards of authentication and transparency rules, for instance. Likewise, the trusted advisor role implies that outcomes are optimised for the customer in a transparent way without any compromise, and that neutrality is applied towards banks' own versus external products.

5.3.3 Superior experience across channels

Banks should leverage the various channels they possess – both physical and digital – to address their customers' needs where and how it is most relevant. That said, not all channels are similarly important for all customers. A persona-based approach helps identify and decide which types of customer to optimise the channel experience for. The importance of face-to-face contact, however, does not only depend on the type of customer but also on the complexity of the product or service. For example, a global retail banking customer loyalty report cites one bank where customer satisfaction was significantly higher for fully digital customer journeys than for those that start digital and end human when it came to activities such as opening a bank account or applying for a credit card. In contrast, when applying for a mortgage or opening a general investment account, customers appreciated a human interaction within the

process.[22]

According to the above-cited report, in countries such as the Netherlands, Germany and Sweden, a sizeable share of customers trying to digitally buy a banking product still failed to do so. Likewise, major reasons to go through human channels related to the assumption that this was easier than digital, next to a preference for human advice.[23] A 2018 study among American retail banking customers suggests that there is room for improvement: according to the study, mobile-only and online-only banks had the least satisfied customers among all.[24] Shortcomings on communication and advice were found to be major factors.

Banks need to understand how to digitally address both the hearts and the minds of their customers. Creating digital proximity to their clients – in other words, put the human touch in a digital transaction – is a key challenge for banks as they build relational trust through the digital channel: in order to overcome this, the digital channel experience should incorporate empathy in its design, thus creating an emotional connection to customers. Also, interactions should be designed to provide value to customers quickly. Finally, it should empower customers to make informed and meaningful decisions. This can be achieved by framing financial decisions around actual goals of customers, rather than presenting them at face value.

Physical channels, nonetheless, can provide additional value and, for some customer groups, continue to be vital. Also, they may prove to be a differentiator for higher-impact and more trust-intensive products such as mortgages. To leverage their physical channels for the trusted advisor role, banks should raise the value of personal advice by moving more transactional activities to the digital channel, while enabling personal advisors to provide the best advice possible based on data-generated insights about their customers.

N26 AND FINANZGURU

For some months in 2019, N26 integrated with Lime, a sharing service for electrical scooters, for a common promotional campaign, knowing that the customer profiles served are likely to overlap: N26 customers automatically saved 50% off the rental fee for a scooter when using the N26 card to pay. That way, N26 was able to create additional benefit and digital proximity with their customers. At the same time, Lime integrated with Google Maps so it could be chosen as mode of transportation right out of the Maps application, massively increasing its reach.

The personal finance app Finanzguru creates empathy with customers through its engaging design as well as a feedback option on every page it displays. It displays financial information with a focus on the most relevant issues, such as how much money a user can spend until the end of the month. Finally, it focuses on immediate value: its contract termination feature automatically points out contracts and subscriptions which may not be needed and allows terminating them with a few clicks and without leaving the app.

Source: N26 and Finanzguru apps

22 Bain, "As Banks Pursue Digital Transformation, Many Struggle to Profit from It", 2019.
23 Bain (2019). Failure of the digital purchase process was perceived by 15-18% of respondents in these countries. The figure in other countries was slightly lower.
24 J.D. Power, "Retail Bank Customer Satisfaction Strained by Growth of Digital-Only Segment", press release, April 26, 2018, https://www.jdpower.com/business/press-releases/jd-power-2018-us-retail-banking-satisfaction-study.

Finally, optimising customer experience across channels also includes the use of Open Banking: with the use of APIs, financial institutions can embed their functionalities and products into customer journeys outside the realm of the bank. Appropriately designed for the prevalent customer personas, this can strongly support the creation of relational trust through digital proximity.

5.3.4 Collaborative implications

While achieving the role of trusted advisor in the digital domain is up to the individual institution, the banking community as a whole can make a collaborative effort toward technical standardisation in several areas conducive to the development of propositions as mentioned earlier in this section.

Specifically, the banking community should promote a level playing field for access and usability of relevant data as a basis for differentiating propositions. As stated in the OBWG's previous paper on "Artificial Intelligence in the Era of Open Banking", efforts could focus on:

- reducing the fragmentation created by various Open Banking standards in Europe to prevent weakening cross-border collaboration in the financial sector and beyond
- expanding the scope of API functionalities beyond the requirements of PSD2 to align with the developing standardisation schemes outside of Europe
- improving the quality of accessible data through enhanced standardisation of syntax (data structures), semantics and processes for an increasingly interoperable exchanges across all stakeholders in the financial sector

5.4 DIGITAL ADVOCATE: ENABLING TRUST SERVICES FOR THE DIGITAL ECONOMY

In the digital economy at large, as also stated in the European Commission's data strategy (see box in this section), trusted and secure ways of interacting, transacting, and storing and sharing data are needed. Trusted digital identities provide the basis for achieving these requirements. Banks, building on a trust foundation of regulation, secure infrastructure and clear principles of digital / data trust are optimally positioned to take a leading role in providing this trust to the broader digital economy, assuming the role of a "digital advocate". They can even go beyond to take an active position in strengthening and defending the digital rights of their customers in transactions with other service providers. By doing so, banks can become their customers' trusted linchpin for identity, financial and data transactions going forward.

5.4.1 Banks as digital identity and attribute providers

The market for digital identity verification is estimated to grow by over 200% in the next ten years, from USD 5.5 billion in 2018 to 18.1 billion by 2027.[25] Financial institutions can monetise this projected growth by leveraging current Anti Money Laundering (AML)-compliant Know-Your-Customer (KYC) processes and customer due diligence, through which institutions control digital identity data for their customers at a

25 Statista, "Identity verification market revenue worldwide from 2917 to 2027," published July 2019, https://www.statista.com/statistics/1036470/worldwide-identity-verification-market-revenue/.

high level of assurance.[26] Underpinning these identified attributes with further data stemming from frequent customer interactions and more intimate customer knowledge through the bank's role as trusted advisor, may result in even more solid, and therefore more valuable digital identities and additional attributes. On a strong trust basis with the customer, banks can provide strong attestations of customer identity and additional attributes for third party service providers. Identity attributes may include verified name, age, and address, whereas additional attributes could, for instance, relate to credit rating, payment preferences or investment interests.

Sharing data can be done in ways that are both privacy-preserving and leave the customer in control: customers decide which identity attributes to share and can be given the option to review, or modify, the data before sharing. Data minimisation can increase privacy by only sharing data that is strictly necessary. An example for that would be to share the attribute "is older than 18" rather than a birth date. Finally, sharing of identity can be instilled with "blindness", i.e. technically ensuring that parties in the data exchange only see what they need to see. For example, banks could be prevented from knowing which party the attestation or data is shared with, and vice versa.

The benefits for banks of positioning themselves as identity or attribute provider include creating additional customer touchpoints, further enhancing relational trust by providing highly relevant services and reinforcing their brand. For the economy, providing trusted digital identities reduces cost, mitigates risk, and enables innovation. At the same time, identity provisioning also allows banks to monetise trust, for example by charging a fee for identity transactions, potentially varying by attribute shared and level of assurance provided. Any such effort should be embedded in a broader scheme as any individual financial services player will lack the market required for success (see collaborative implications in section 5.4.4).

5.4.2 Beyond bank data: data account and digital key box approaches

Acting as an identity and attribute provider rests on the principle of sharing bank-controlled customer data with third parties. However, banks can also use their trust position to go a step further and enable the sharing of customers' data that does not stem from its own interaction with the customer.

The concept of **data accounts**, or data vaults, proposes that customer data should be held in accounts similar to money, which are held and protected by institutions that are trusted by customers. In the scenario, banks could use the trust customers put in them to position themselves as the providers of choice for such accounts, thus offering two types of accounts, one for money and one for data. This type of "personal data banking" implies the use of the banks' secure infrastructure and trusted authentication and consent mechanisms to share the non-banking data with other parties under the customer's control. Drawbacks of this approach include heavy infrastructure investments and, more importantly, additional efforts to convince customers that the data is held, but never used by the bank.

An alternative is presented by the **digital key box** approach. Instead of attempting to centralise consumers' data, the digital key box principle leaves the data at their source and focuses on providing aggregated access and consent management of that data. In practical terms, it will provide consumers with a simple and effective means to manage consent and allow data sharing across organisations. The key box is a hub to control and manage data, where a separate digital key is associated with each personal data attribute irrespective of its provenance. Upon the data request of a third party, the customer gives consent with bespoke conditions to use the relevant keys to unlock access. If at any future time, the customer wishes to revoke the third party's data access, the customer withdraws the digital key through the dashboard of the key box. If implemented properly and adopted widely, this approach can create significant commercial opportunities for businesses in the ecosystem, whilst simultaneously ensuring their GDPR compliance.

5.4.3 Enforcing customers' digital rights

Finally, in addition to providing identity data and attributes as well as enabling broader data sharing, financial institutions can take a proactive role in protecting their customers' digital rights within

26 One example from the Nordics is Invidem, a KYC platform founded by leading Nordic banks. The service makes KYC information available in a common standard and AML-compliant data process. The platform is operated independently and is accessible for all parties requiring compliant KYC data.

A EUROPEAN STRATEGY FOR DATA

On February 19, 2020, the European Commission published a European data strategy with the aim of making the EU a role model for a data-empowered society. Given the value potential of data for the economy and society, it aims to frame a European way for sharing and using data while preserving privacy, security, safety and ethical standards. The strategy is built on a vision "to create a single European data space […] where personal as well as non-personal data, including sensitive business data are secure, and businesses have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint".

Furthermore, individuals should be **empowered** to exercise their rights: GDPR and ePrivacy regulations have granted high levels of protection for personal data, yet they do not give people the tools and standards to exercise these rights in a practicable and uniform way. The data strategy therefore aims to provide a supportive environment for the development of tools for consent management and personal information management, for instance, as well as novel, neutral intermediaries in a personal data economy (such as personal data cooperatives).

The empowerment of individuals is consequently one of the four pillars of the EU data strategy – next to developing a cross-sectoral governance framework for data access and use, strengthening Europe's data capabilities and infrastructures, and creating common European data spaces in strategic sectors. A potential Data Act to be drafted by 2021 is expected to underpin the efforts around individual empowerment around data.

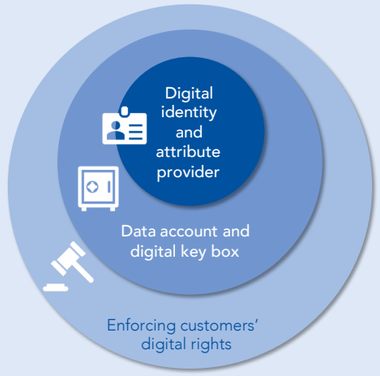
A positioning of banks as trusted protectors of data and providers of data services is very much in line with the EU's strategy – and banks have an important role to play in shaping Europe's digital economy if they act now.

Source: European Commission, "A European Strategy for Data", 2020, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

Figure 11 – Elements of the digital advisor role and the requirement of soft data infrastructure

As digital advocates, banks enable trust services for the digital economy beyond banking. This should be accompanied by collaborative development of "soft infrastructure" for data.

ENABLEMENT OF DIGITAL ECONOMY



REQUIRED (COLLABORATIVE) SOFT INFRASTRUCTURE

Structural approach to digital identity and data sharing requires "soft infrastructure", providing the rails for efficient, secure and user-friendly exchange of (identity) data.

Such infrastructure or framework:

- is established in a sector-wide (or cross-sector) collaborative effort
- ensures through its setup that the participating parties can trust each other
- includes agreements across various domains, such as technical, functional, operational, legal and business
- leaves sufficient room for competitive areas in which individual participants can differentiate their offers
- has been proven to be successful in various European markets and domains, in particular also as digital identity schemes

Source: EBA and INNOPAY analysis

the sphere of control they exercise in an (Open Banking) ecosystem. For example, banks could monitor unauthorised use of their customers' data by third parties. This would include scanning transactions, providing visibility on personal data collection or transfers in the ecosystem, informing the customer and facilitating the correction or deletion of personal data at other providers.

In summary, a bank acting as digital advocate optimally supports their customers' ability to navigate the digital ecosystem and control their data within it. The bank provides the user experience, for instance in the form of dashboards and consent interfaces, to make this as simple as possible.

5.4.4 Collaborative implications

Offering identity data and attestations unilaterally through APIs is possible and frequently observed as part of API programmes of banks opening up. However, a structural approach to digital identity and data sharing requires a sector-wide (or cross-sector) collaborative effort in the non-competitive space to establish a "soft infrastructure" connecting identity or attribute providers, relying parties (receiving data), and customers. This infrastructure needs to provide the rails for efficient, secure and user-friendly exchange of (identity) data and, most of all, ensure through its setup that the participating parties can trust each other.

A prerequisite for such a **soft infrastructure** is the collaborative development of a framework of agreements across technical, functional, operational, legal and business domains. Stakeholders will need to align on common principles and technical standards, including common elements of user experience, as well as a model of roles and a governance framework. At the same time, the solution will need to ensure sufficient room for competition whereby individual participants (such as banks) can market their competitive offers and service providers who offer, for instance, integration services can compete freely. With broad support among financial institutions and other market stakeholders, clearly defined collaborative and competitive domains, properly set incentives for stakeholders and a framework designed with customer value and benefit in mind, there is a high likelihood of success. Examples exist in several European countries for successfully deployed digital identity schemes based on bank identities, which can serve es example for other markets (see box).

Of course, other players are working to access the opportunities that come with managing digital identity and consent. BigTechs may lack the trust factor of banks but have unsurpassed reach and experience in creating seamless, ecosystem-embedded user experience. Nevertheless, as this report shows, financial institutions are well positioned to act as both guardians of their customers' identities and managers of consent. It is now time for banks to collectively leverage their advantages and not let this opportunity pass. [27]

27 A similar point is argued by the Mobey Forum (2020) in their report on digital ID. See Mobey Forum's Digital ID Expert Group, "How to make digital identity a success: insights and learnings from seven digital ID schemes," February 2020, https://mobeyreport.com/digital-id-report20200213/.

SUCCESSFUL BANK-BASED TRUST INFRASTRUCTURES FOR IDENTITY AND DATA

BankID in Sweden, Norway, and Finland, as well as iDIN in the Netherlands are examples of operational and successful digital identity schemes built by banks. All these schemes leverage verified customer identities held by those banks. Elements they have in common include full support and involvement of the respective banking communities, clear standards and rules around technical and non-technical elements, well-defined roles (such as identity issuers), central governance, a decentralised approach to data, free choice of provider for consumers and open competition in roles such as relying party (merchant) acquiring. In the case of iDIN, the pre-existing payments infrastructure of the online payment scheme iDEAL has been repurposed to securely share identity data instead of digital money.

Itsme in Belgium is an identity solution with broad bank involvement which centralises the user interface in one consumer app and centrally stores identity data. Banks act as "registrars" responsible for verification of the identity but not for its storage.

The market success of bank-based identity systems can be impressive, as for example BankID shows: in November 2019, 98.7% of the Swedish population had a BankID. In January 2020 alone, close to 400 million BankID transaction were carried out in Sweden.

Source: See BankID, "Statistik BankID – användning och innehav", January 2020, https://www.bankid.com/assets/bankid/stats/2020/statistik-2020-01.pdf.

6 CONCLUSION AND WAY FORWARD

Trust is fundamental to the success of financial institutions. The digital transformation that both society and economy are undergoing, requires banks more than ever to think about how to protect, reinforce and leverage the trust put in them to serve their customers in a relevant way. New technology and channels of communication, changing consumer attitudes and expectations, the unbundling of the financial value chain and the pivotal role of data are all new parameters that imply an active and structured approach to building trust in a digital way.

Banks are in a good position to build digital trust, but they need a clear plan going forward that involves, in part, a coordinated industry effort. On the way to building a digital trust advantage, this report proposes three steps for banks to take:

1. **Build digital trust based on the bank-inherent trust advantage to differentiate themselves from other market players**. To do so banks should, as a basis, implement additional highly robust measures around data security. Pursuing and putting in place principles of consistent customer control and the responsible use of data are further required to build trust. When engaging in Open Banking, banks should develop a stance on how to ensure standards of security, privacy and control of their ecosystem partners. Finally, all this should be reflected in a consistent and designed-for-purpose user experience.

2. **Become a trusted advisor to their customers by leveraging digital trust.** With the digital trust foundation in place, banks can leverage that trust to use customer data with the goal of becoming the prime destination for handling their customers' financial well-being. This includes building relevant customer propositions, engaging in Open Banking to include third-party propositions and capabilities in their offering, as well as ensuring superior overall customer experience.

3. **Become a digital advocate who provides trust-based services and leverages trust as a direct value driver.** This includes roles as digital identity or attributes providers using verified customer data controlled by the bank, as well as going beyond to take care of non-bank data of behalf of the customer or provide consent management and data access services to customers, supporting transactions in the digital economy beyond the bank's realm.

Collaborative measures by the banking sector should support these steps: At the level of data protocols, finding ground for and aligning on common principles could help strengthen trust in the sector as a whole. Reducing the fragmentation around Open Banking standards, API functionalities and data syntax and semantic of shared data may increase the overall competitiveness of services provided. And finally, the development of the "soft infrastructure" that is needed to achieve the necessary reach and interoperability of new types of trust-based services, such as digital identity, requires a collaborative effort.

Going forward, individual financial institutions may find the framework, steps and measures outlined in this report helpful when defining their own approach to systematically building digital trust, uncovering areas of attention in existing strategies and implementing roadmaps and, more generally, continuing to adopt a digital trust-focused mindset.

On a sector level, focus should be on how to drive existing initiatives, for example around data conduct, forward to their adoption. In the area of trust-based services, successful identity schemes, for examples in the Nordics, can serve as inspiration to build bank-driven schemes in other countries while being aware of the different market conditions and settings. In a next phase, the focus for the financial sector will have to turn to 'Open Finance'.

Now is the time for financial institutions to solidify their role in the new economy. Building on the strong trust they already enjoy, they now have the opportunity to successfully transition into the digital economy, maintain their role as their customers' prime partner for financial well-being and claim a new role beyond that in a digital transaction ecosystem.

IMPRINT

Euro Banking Association
40 rue de Courcelles
F-75008 Paris

CONTACT

association@abe-eba.eu

GRAPHIC DESIGN

Bosse und Meinhard, Bonn

IMAGES

istockphoto/maxkabakov