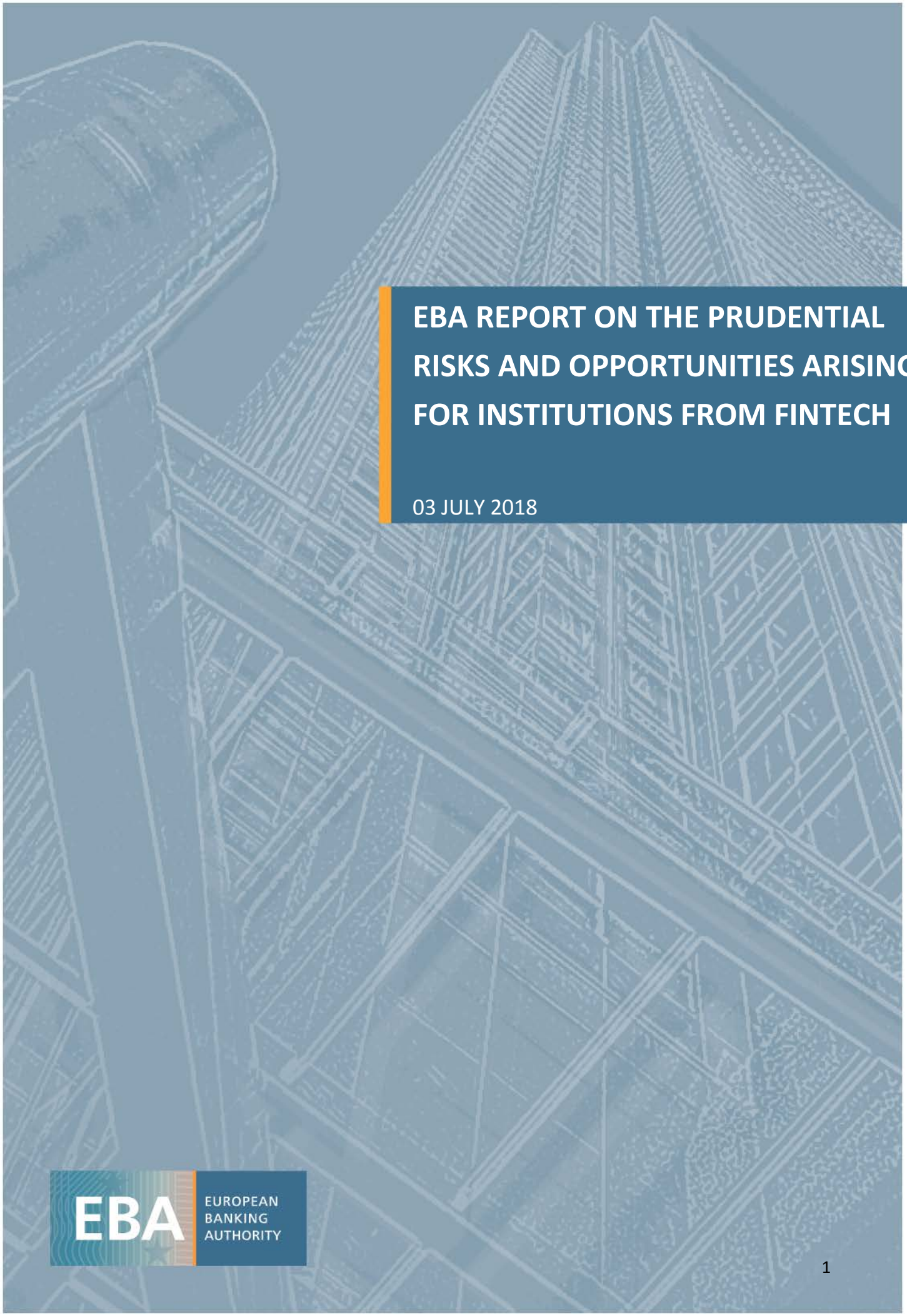


EBA REPORT ON THE PRUDENTIAL RISKS AND OPPORTUNITIES ARISING FOR INSTITUTIONS FROM FINTECH

03 JULY 2018

EBA EUROPEAN BANKING AUTHORITY

Contents

1. Abbreviations

AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
ATM	Automated Teller Machine
AuM	Assets under Management
BCBS	Basel Committee on Banking Supervision
CDD	Customer Due Diligence
CFPB	Consumer Financial Protection Bureau
CSP	Cloud Service Provider
DGSD	Deposit Guarantee Schemes Directive (Directive 2014/49/EU)
DLT	Distributed Ledger Technology
DP	Discussion Paper
EBA	European Banking Authority
EC	European Commission
eIDAS	Electronic Identification and Signature (Regulation (EU) No 910/2014)
EMD	Electronic Money Directive 2 (Directive 2009/110/EC)
ESAs	European Supervisory Authorities (the EBA, ESMA and EIOPA)
ESMA	European Securities and Markets Authority
ETF	Exchange-Traded Fund
FinTech	Financial Technology
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
HCE	Host Card Emulation
ICT	Information and Communication Technology
MCD	Mortgage Credit Directive (Directive 2014/17/EU)
MiFID	Markets in Financial Instruments Directive (Directive 2004/39/EC)
NFC	Near field Communication
OS	Operating System
PAN	Primary Account Number
PIN	Personal Identification Number
PoC	Proof of Concept
POS	Point of Sale
PSD	Payment Services Directive 1 (Directive 2007/64/EC)
PSD2	Payment Services Directive 2 (Directive 2015/2366/EU)
RTS	Regulatory technical standards
SME	Small and Medium-sized Enterprises

2. Executive summary

The rapid evolution of FinTech with its multiple applications and interactions within the financial services sector, ranging from front-end to back-end operations, may fundamentally change the risk profiles of institutions by creating new risks and/or amplifying some existing risks, prompting institutions to review their risk management frameworks and strategies. While at first sight ICT risks could be perceived to be the key risks associated with the emergence of FinTech, this report identifies and analyses the wider prudential risks and opportunities that may arise in institutions from the use of innovative technologies.

This report aims to raise awareness, within the supervisory community and the industry, of current and potential FinTech applications, striving to provide a balanced analysis of associated potential prudential risks and opportunities that may arise. The intention of this report is merely to inform and share information without making recommendations to competent authorities or institutions. It is focused on microprudential aspects and is envisaged to provide both the competent authorities and institutions with useful guidance on such applications. Specifically, the seven use cases selected for analysis in this report discuss the application of FinTech to existing financial processes, procedures and services.

While the analysis of potential prudential risks and opportunities focuses on the seven use cases, it may be applicable to other financial processes, procedures and services, where the same underlying technologies are used (also depending on the business case). It is also important to take into consideration the uneven activity level and pace of FinTech developments across Europe when discussing and analysing this report.

The use cases discussed in this report have also been informed by theoretical knowledge reflecting the development stage of each application having in mind the uncertainty and unfamiliarity about current FinTech applications. While the focus is mainly on the operational risk aspects, a number of other potential prudential risks have been noted, taking into consideration the forward-looking element of this analysis. As the development status of some use cases is still at the prototype or pilot stage, ongoing discussions and analyses are expected to continue to shape the approach and the implementation followed by institutions.

The analysis presented in this report assumes that technology will be implemented appropriately, adequately and sufficiently, as the impact on the risk profile of institutions will be highly dependent on the type of underlying technology and its implementation as well as the processes and business models adopted around it. Under no circumstances should this report be considered to favour or discourage the use or application of any technology or assumed to provide an exhaustive list of possible prudential risks and opportunities that may arise.

The use of **biometrics** in financial services is considered by the industry to hold significant potential for institutions, ranging from general security to mobile payment solutions, as is evident from the widespread use of biometrics in a number of financial applications. The use case focuses on the use of fingerprint recognition for customer authentication in mobile banking applications. This is a way to verify customers in addition to the use of one-time passwords, static passwords, security questions and other techniques. Improved customer experience is foreseen as the main opportunity in this case, as customers would not need to remember and enter passwords all of the time and it would be easier for them to perform authentication by a simple swipe of their finger. The potential streamlining of the authentication process and the promised security benefits compared with existing methods seem to support the increased adoption of biometrics by institutions. On the prudential risk side, the dependency on mobile device manufacturers and other providers could increase third-party risk and ICT-outsourcing risk as well as ICT security and data integrity risk, given the level of reliance on these providers.

In the context of the broader ongoing digital transformation across institutions' credit risk management functions, machine-learning techniques are being pursued by institutions and currently used (or piloted) in retail portfolios, probably because they have more extensive available data sources. A predominant area of machine-learning application, within the credit risk management area, has been in **credit scoring**. Institutions aim to use machine learning and big data techniques to improve their insights from existing data sources (e.g. transaction data), introduce further automation in credit decision processes and use new data sources (e.g. social media data). Through the extensive, wide and comprehensive credit analysis performed under these techniques, institutions may be possibly better placed to trust new customers at an early stage, resulting in quicker customer engagement through the provision of credit facilities (e.g. credit card applications or short-term credit in the e-commerce context). Improved credit portfolio quality and the provision of new insights in real time also appear to be important potential opportunities for enhancing the overall credit risk management for institutions.

On the potential prudential risk side, legal and conduct risk could be adversely affected, alongside reputation risk, in the event of unauthorised use of customer data (in the context of the GDPR[1]) or consumer protection issues such as unethical behaviour (e.g. discrimination). Once again, third-party risk could be higher if external providers are involved in such solutions than it is for services developed in house. ICT change and security risk may possibly increase, as ICT systems would need to develop to be more open to different data sources or technology providers and allow more agility in the use of data within the IT system.

The rise in the use of algorithms, in combination with the retail population with no previous easy access to financial advice, has led institutions to explore ways of providing **automated investment advice**. The provision of investment advice to a mass market through online advice sites/robo-advisors appears to offer fast and low-cost access. Customers are required to answer a series of questions, which then feed into a decision tree process that analyses and processes customers'

[1] Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

information in the context of suitability and appropriateness assessment, and subsequently provides automated investment advice to non-professional investors. While a number of new propositions on automated investment recommendations have been launched in the recent years, not many have been identified as offering automated investment advice in the context of MiFID/MiFID II.

Reliance on third-party providers, when applicable, legal uncertainty issues, reputation and conduct risk and overall increase in ICT risks could potentially be the most significant prudential risks when it comes to the provision of investment advice using robo-advisors. It is also unknown how retail customers will perceive this automated service, given that they are used to human contact and advice when it comes to investment decisions. This solution may possibly increase the accessibility of financial products to consumers, while on the other hand it is also possible that the extensive use of customer data could lead to financial exclusion (e.g. unjustified discrimination).

The convenience to customers in terms of speed and quality offered by such robo-advisors, as customers would no longer have to physically visit a branch or meet a financial advisor, and the ability to reach mass customers at less cost than the existing advisory offerings appear to be the most prominent opportunities in automated investment advisory services.

Two potential applications of DLT are discussed in this report, namely the use of DLT and smart contracts for trade finance and the use of DLT in the management of CDD documentation, data and information. In the area of **trade finance**, a number of developments are currently taking place with different DLT initiatives going through proof of concept (PoC) and pilot testing, with active interest and investment from institutions. Today, trade finance processes are considered to be very labour-intensive, involving large amounts of paperwork. In addition, the transfer of assets is perceived to lack transparency, with payments frequently delayed and prone to errors, having as a result high operating costs.

From a prudential risk point of view, legal and compliance risks appear to be potentially affected, mainly because of current legal and regulatory uncertainties as well as possible difficulties entailed in designing the governance of such a model. The immaturity of the technology could potentially pose other prudential risks in addition to the challenge currently faced regarding cooperation and participation by all the parties involved in the trade finance process (e.g. banks, shippers, carriers).

With the use of DLT and smart contracts, trade finance stakeholders aim to streamline the process, and reduce time and costs with punctual information for the parties of a transaction. This may potentially enable institutions to automate the financial process of trade transactions and reduce the risk for both the importer and the exporter.

Institutions could potentially use DLT in their AML/CFT compliance, particularly as part of their **customer identification and verification processes**. This application of DLT aims to facilitate the CDD process, which can be quite complex, expensive and burdensome to institutions. DLT seems to be offering decentralisation, immutability, security and visibility to all participants, resulting in a

number of institutions exploring its use for CDD processes. The use case is currently only theoretical and discusses a possible solution in which a number of institutions participate and have access to a distributed database of verification results of corporate customer data. This customer data is verified by one participant institution when the corporate customer initially approaches the institution. When the same corporate customer approaches another institution participating in the scheme and using the same distributed ledger application, that institution can access, with the customer's consent, the customer's already verified information. Each institution is responsible for ensuring that the customer's documentation, data and information is up to date and therefore the institution can accept, amend or reject the customer's verified data and complete its own CDD process. If information is updated, one of the participant institutions can upload or amend the customer's information as required. The contents of the DLT can then serve as the corporate customer's digital identity for transacting financial services with the members of the scheme.

On the potential prudential risk side, data privacy and other compliance concerns as well as legal aspects of liability (in the event of a fraudulent activity) could arise along with concerns about the governance of the distributed ledger. The standardisation of the identification and verification part of the CDD process could be challenging due to the jurisdictional nature of AML/CFT legislation and different policies and procedures applied by each institution when on-boarding customers on the basis of the institution's risk appetite and the customer's ML/TF risk profile. A third-party risk aspect could also appear if an institution places reliance on the efficacy of another institution's CDD process, an activity that could be considered critical or important under the EBA draft Guidelines on Outsourcing[2]. Moreover, this concentration of identity data may make the solution a target for hacking or cyber-attacks.

From the prospective opportunities perspective, this could potentially enhance customer experience and reduce operational costs and administrative burden for institutions as the updated CDD would be distributed in real-time between all participating institutions and increase transparency through a clear audit trail of customer records. However, to achieve this, participating institutions might need to align their customer on-boarding processes and ML/TF risk management systems, which could prove to be challenging if these institutions are located in different countries with different AML/CFT rules.

Another widely used application is **mobile wallets with the use of Near Field Communication (NFC)**. After the introduction of Apple Pay in 2014, similar offerings were launched, aiming to improve user experience. This is already a common payment method in some jurisdictions, where institutions have developed their own mobile wallets and/or collaborated with mobile device providers. It is generally based on a credit/debit card linked to a mobile device, which can be used for e-commerce and point-of-sale (POS) payments. Using mobile wallets, customers are able to

[2] EBA, Consultation Paper – Draft Guidelines on Outsourcing arrangements (22 June 2018): http://www.eba.europa.eu/documents/10180/2260326/Consultation+Paper+on+draft+Guidelines+on+outsourcing+arrangements+%28EBA-CP-2018-11%29.pdf

make contactless payments (below a pre-determined monetary threshold) enabled using NFC technology by holding their mobile device within a short distance from the POS terminal.

The predominant benefit of mobile wallets is the improved customer experience through a more convenient payment method and no need to memorise passwords or PINs or carry physical cards. In addition, it may be possible for mobile wallets to provide additional security for customer payments.

On the potential prudential risk side, the dependency on mobile device manufacturers and the overall use of mobile devices could raise concerns regarding third-party access to customers' bank accounts when customers use a third-party wallet, affecting aspects of ICT security risk and data protection. The use of mobile wallets using NFC technology could have repercussions for the availability and continuity of payment activities, such as technical failure, thus possibly affecting ICT availability risk. The institutions' ability to gain and maintain their customers' trust in using their or third parties' mobile banking applications for payments would also be important.

In recent years, there has been increasing interest from institutions in using the services of **cloud** service providers. Although the interest was initially focused on systems that may be deemed non-core, institutions are now also exploring the possibility of migrating core systems to public clouds.

Cloud outsourcing services are standardised, allowing services to be provided to a larger number of customers in a highly automated manner on a larger scale. The flexibility provided by cloud infrastructure along with the lower-cost environment, scalability and agility are considered the predominant benefits of public cloud.

Although cloud services could offer a number of advantages, a potential migration to the cloud could increase ICT change risk, in the event of reliance on complex legacy infrastructure, and other potential issues related to the multi-tenant environment of public cloud as well as the jurisdictional location of data. ICT outsourcing risk could be also considered important, not only from the point of view of individual institutions but also at an industry or systemic level, as large suppliers of cloud services could become a single point of failure should many institutions rely on them. Additionally, a possible impact on the wider operational risk could arise from issues with data security, systems and banking secrecy, especially when cloud services are hosted in jurisdictions subject to different laws and regulations from the institution.

3. Background

Article 1(5) of the Regulation establishing the EBA (Regulation (EU) No 1093/2010) requires the EBA to contribute to promoting a sound, effective and consistent level of regulation and supervision, ensuring the integrity, transparency, efficiency and orderly functioning of financial markets, preventing regulatory arbitrage and promoting equal competition. In addition, Article 9(2) requires the EBA to monitor new and existing financial activities.

These mandates are key motivations underpinning the EBA's interest in financial innovation in general and more specifically in FinTech, which is defined by the FSB[3] as 'technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services'.

Over the years, the financial landscape has started to look very different as a number of waves of financial and technological innovation have eroded the boundaries between financial products and services, and between those providing them or enabling their provision. The use of technologies by financial services firms is not new per se. Financial services firms have always implemented technological solutions to support the provision of services to their customers and to ensure that they comply with regulatory obligations. They have also long relied on outsourcing arrangements with external service providers for the provision of technological solutions and performance of operational activities, including aspects of ICT operations. However, the more recent phenomenon of FinTech appears to be raising this process to a new level, as a result of significant investments in innovative technologies by institutions and entities outside the financial services sector. It is argued that FinTech has the potential to transform the provision of financial products and services further, while this growth may also change institutions' risk appetite.

The EBA has decided to take forward work in relation to FinTech with initially publishing a Discussion Paper[4] on its approach to FinTech. Following the public consultation on that Discussion Paper, the EBA published its FinTech Roadmap[5] setting out its priorities for 2018/2019.

One of the priorities set out in the EBA FinTech Roadmap is the analysis of the prudential risks and opportunities for institutions arising from FinTech, including the development and sharing of knowledge among regulators and supervisors. This thematic report, as the first step towards this priority, aims to raise awareness, and focuses on the potential prudential risks and opportunities

[3] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf

[4] EBA, Discussion Paper on the EBA's approach to financial technology (FinTech) (4 August 2017): https://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf

[5] Available at: http://www.eba.europa.eu/-/eba-publishes-its-roadmap-on-fintech

that may arise for institutions from the use of emerging technologies. Given the wide application of innovative technologies in financial services, the approach followed for this report was the selection of a number of practical FinTech applications in traditional banking, payment and e-money activities, namely 'use cases', along with the analysis of the prudential risks and opportunities arising from each use case. These use cases are considered existing traditional banking or payment activities, processes and procedures to which institutions apply, or are considering applying, innovative financial technologies. For the selection of these use cases, the level of involvement and activity observed in each jurisdiction were taken into account in combination with the supervisory need to further explore specific applications as well as the interest expressed by EU institutions in investing further in exploring and developing such applications. In addition, this selection aimed to capture as many financial technologies as possible.

In the context of the EBA Risk Assessment Questionnaire (RAR), conducted on a semi-annual basis among banks and market analysts, 37 European banks were asked to indicate their level of involvement in the selected FinTech-related activities. The autumn 2017 RAQ was conducted in October-November 2017.

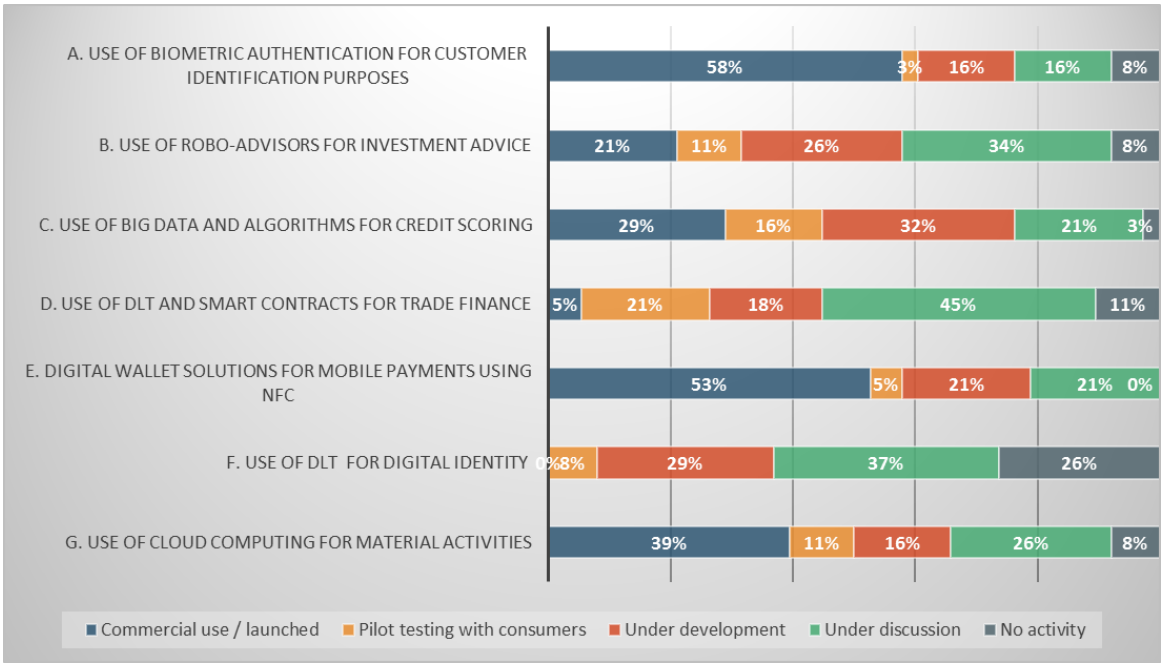


Figure 1: Level of involvement in the selected FinTech use cases (37 EU banks)

At that point of time, the use of biometrics and mobile wallets with the use of NFC were the most widespread applications, whereas the DLT-based applications appeared to be in their early stages. This evidences the different levels of development between financial technologies as well as the growing interest of institutions in exploring and leveraging the potential opportunities that may arise from financial technologies.

For the purposes of this report, the term 'institutions' encompasses credit institutions, investment firms, payment institutions and e-money institutions. While the concepts of most use cases could

be considered more applicable to the banking industry, they could be also applied to payment institutions and e-money institutions, as the same issues, risks and opportunities could be encountered. Nevertheless, use case 2, 'Use of robo-advisors for investment advice', is considered applicable only to credit institutions and investment firms, as payment and e-money services do not involve the provision of investment advice.

Having in mind the rapid development of FinTech, which is still in its early stages[6], this analysis is forward-looking and specific to the current level of development, understanding and knowledge.

During the development of this report, it became evident that the activity status (i.e. proof of concept, prototype, pilot, production) and pace of the selected use cases vary across the EU financial sector. Under no circumstances should this report be considered to favour or discourage the use or application of any technology or assumed to provide an exhaustive list of possible prudential risks and opportunities that may arise.

In line with the European Commission's guiding principle, the EBA fully supports the technological neutrality principle and maintains an open-minded approach when reviewing existing measures or developing new measures to ensure that regulation and supervisory practices do not prefer specific technologies.

For the purposes of this report, useful interactions with the industry were leveraged to inform the practical application of financial innovative technologies along with the potential changes to institutions' risk profiles, as FinTech extends beyond the usual boundaries of supervisory communication with regulated institutions.

At this stage, this work aims to support supervisors and institutions in understanding the prudential risks that could possibly arise from the use of innovative technologies along with the corresponding opportunities. This will contribute to building and sharing knowledge and experience among the supervisory community and responding to emerging technologies, one of the avenues for pursuing technological neutrality.

In line with the EBA FinTech Roadmap, the EBA will continue to observe and consider the pace of employment of technologies in financial services and, where appropriate, to accompany this work with an opinion and/or proposals for guidelines to enhance supervisory consistency and facilitate supervisory coordination.

[6] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf

4. Use cases

4.1 Use case 1: Biometric authentication using fingerprint recognition

4.1.1 Introduction

Current landscape

People use face and voice recognition to identify each other all the time. Through time and population growth, the need for more reliable identification methods arose. In the 1800s, the Bertillon system was developed, an anthropometric method of measuring body parts to identify individuals. As it soon turned out, such measurements were time-consuming and not stable, because of ageing, and there were difficulties with precision. By the end of the 19th century, the Henry fingerprint identification system was developed and used for criminal investigations. The Metropolitan Police Service started using fingerprint identification in 1901 and fingerprint identification systems rapidly evolved.

Automated biometric identification systems[7] became available over the last few decades thanks to significant advances in the field of computer processing, and widely adopted because of the spread of mobile devices. Such systems use electronic sensors to take digitalised biometric measurements, which are then processed by computers.

The shift in user behaviour and the introduction of digital channels facilitated the quick adoption of biometrics in the financial services sector. It is still in the early stages but is gaining popularity rapidly. A number of implementations for the use of biometrics to authenticate customers have been witnessed, such as (among others):

- Authentication based on customer's fingerprint. In practice, with the use of a fingerprint scanner, the details of the fingerprint are captured as a digital image, which is then analysed and turned into a code to authenticate the customer.

- Authentication through voice recognition. The customer has to contact the institution to record a voice sample for the use of voice recognition software. Consequently, the customer can be authenticated based on his or her voice and may request information or carry out financial transactions.

[7] For clarity, biometric identification answers the 'who are you?' question to identify an individual. Biometric authentication answers the 'prove who you are' request whereby the individual needs to prove his or her identity to be allowed access to a system or service.

- Authentication of customers and authorisation of transactions through biometric signature verification. Signature pads capture the signature image, the writing dynamics and the pressure applied, to increase the reliability of authentication. Applications may include signing documents for opening new accounts, credit and loan applications, and deposit and withdrawal slips.

- ATMs using facial recognition. ATMs may use facial recognition as an additional authentication factor (besides the customer's card and PIN or mobile device, for example) in high-value transactions. The customer is asked to perform a facial scan during the account setup. If the scan matches the customer's pre-recorded image, the ATM executes the high-value transaction.

While the safe authentication of customers and reduction of the risk of fraud is imperative, institutions are also assessing ways to satisfy customers' demand for quick and convenient authentication. Biometric authentication technologies rely on physical and behavioural features, so no passwords are required. The question may then be the reliability of such technologies.

Underlying technologies

Biometric authentication technologies are based on measuring a person's unique and stable biometric features and matching them with authorised biometric samples of that person.

Physiological biometrics rely on either external features of the individual, such as fingerprints, face, voice and iris patterns, or internal features, such as vein, pulse and electrocardiographic patterns. Behavioural identification can be based on, for example, signature dynamics, typing and gait patterns. Multi-factor biometric identification and authentication are achieved by a combination of the above, e.g. fingerprints plus iris scans.

Biometric features need to satisfy a set of requirements to be suitable for biometric authentication:

a) Universality ensures that the attribute is something each individual has.

b) Uniqueness ensures the patterns are different for every individual.

c) Permanence relates to the changing of a feature over time. Features with good permanence are reasonably invariant.

d) Collectability relates to how easily the pattern can be acquired or measured. The more difficult it is to access the pattern, the less effective the identification method is.

e) The ease of circumvention affects the security and reliability of the method.

f) Social acceptance, i.e. the customers' acceptance, or resistance critically affects the usage of the method.

Recent technological advancements, such as the increased computing power and spread of mobile devices, allow more and more of these aspects to be satisfied. The suitability of biometric

identification and authentication technologies depends on their accuracy, speed and robustness as well as on the goal and circumstances of their usage.

Biometric features in combination with the technologies used for authentication provide varying level of reliability. From the perspective of security, the risk of false acceptance, measured through the false acceptance rate (FAR), is the most important, whereas the risk of false rejection, measured through the false rejection rate (FRR), can ruin the user experience. Voice recognition and facial recognition seem to have relatively high false acceptance rates, whereas fingerprint identification may have a significantly lower FAR. Iris and retina scanning appear to be more reliable, with even lower FARs[8]. The error rates correlate with the accuracy of the identification. As accuracy is increasing, the risk of false acceptance decreases, but the risk of false rejection increases. Therefore, the target is a healthy balance between secure identification and user experience.

As biometric authentication is still at an early stage, its reliability is often increased by combining it with other authentication factors (something you know or something you have), for example combining fingerprint recognition with static or one-time passwords.

Fingerprint recognition is one of the most popular biometric techniques used in automatic personal identification and authentication. The reliability of fingerprint identification methods also varies greatly, based on the number of details identified in the fingerprint, the algorithm applied and the technologies used to take the patterns. Some of these technologies are as follows:

- Capacitive sensors: the map of the finger is created by using condensers; therefore, this method is not reliable with dirty or wet fingers.
- Thermal analysis: the sensor measures the temperature differences between the skin's ridges, so the analysis is reliable even in cases of fingerprints with small ridges. It can also be used in extreme circumstances with high temperature and humidity, but it is expensive.
- E-field technology: it measures the electronic field between the finger and sensor; therefore, it is not influenced by the quality of the fingerprint.
- Optical sensors: this method is the most common and uses a tiny scanner with LED illumination. Cleaning the surface of the scanner is crucial for reliability.

4.1.2 Use case

As fingerprint recognition is currently the most popular biometric authentication method, this case focuses primarily on fingerprint recognition.

[8] Dimopoulos V, Fletcher J and Furnell SM, 'Evaluating the reliability of commercially available biometric devices', *Proceedings of Euromedia 2003, Plymouth, England, 14-16 April*, 2003, pp. 166-174.

The use of fingerprint recognition technology in mobile banking as an alternative to passwords has already been implemented by a number of institutions because of the increasing use of mobile banking applications and the rapid changes in customer demand.

Customers need to register their smartphones, which must have fingerprint scanners, as trusted mobile devices to access the mobile application of the institution. Once the devices are registered and the mobile application is installed on the devices, the customers need to activate fingerprint authentication with their security information, whereby the smartphones record details of the customers' fingerprint patterns. Fingerprint-scanning devices often use basic technology, such as an optical camera that takes pictures of fingerprints, which are then read by the device to identify and record a certain number of details in the fingerprint. Thereafter, customers may use the smartphones' fingerprint readers to access the mobile banking application, as the recorded details are used to authenticate the customer instead of relying on passwords. This makes the process more convenient. Nevertheless, after a number of failed login attempts by using fingerprints, customers may have to re-enter their password.

Institutions usually limit the services that customers may access on their smartphones using only fingerprint authentication, e.g. customers may access their accounts and cards to query balances or transactions, may transfer funds between their own accounts or may transfer funds to trusted beneficiaries. For services with a higher level of risk, institutions may request additional confirmation (e.g. passwords) on top of the biometric authentication, e.g. to make transactions to accounts other than trusted beneficiaries, to make pre-paid phone top-up transfers to numbers other than trusted numbers or to make mobile transfers without using a card. Institutions may also impose limits on transactions using biometric authentication.

4.1.3 Prudential risks

The use of fingerprint authentication may have an impact on a number of prudential risks, with legal, reputation and ICT security risks possibly being the most prevalent.

ICT security risk could be affected because fingerprints are not secret and could be collected without the customers' consent from everyday objects they touch. Fingerprint impressions left behind on fingerprint sensors may also be captured (i.e. residual attacks), and fingerprints could not be changed if they are compromised or 'stolen' in some way.

Another possibility that could affect ICT security risk is when the owner of a mobile device registers the fingerprints of other persons on his or her device so that they can also access that device to make phone calls, etc. If the mobile banking application relies on the fingerprints registered for accessing the device, these persons may also make transactions from the bank account of the owner of the mobile device without his or her consent.

Reputation and legal risks could also possibly be affected if the fingerprint reader devices copy and store fingerprint data that is then compromised and stolen by hackers. Hackers may bypass

biometric reader devices and inject the stolen fingerprint data directly into fingerprint authentication systems to trick them into granting access on behalf of the customers.

Legal and ICT security risk could be also affected if fingerprints are falsely accepted. Nevertheless, the risk of false acceptance is relatively low compared with other biometric identification methods, e.g. voice recognition.

Legal, conduct and reputational risk could arise from a breach of the GDPR[9] and related national regulatory frameworks in terms of the protection, use and processing of sensitive personal data, as biometric data falls within the scope of the GDPR.

ICT-outsourcing risk could possibly be affected, as institutions would need to rely on software service providers developing the application installed on the mobile device. At the same time, third-party dependency on mobile device manufacturers and operating system developers could be raised, as biometric authentication is performed on mobile devices and, in addition, institutions would have no direct control over these companies and over the reliability of the fingerprint authentication technology.

In the scenario where fingerprint recognition becomes a common standard, it is possible for institutions with different risk appetites to implement different fingerprint authentication solutions, compromising security to provide a customer-friendly end-user experience and potentially reduce costs. While this could affect the overall business risk, it could also adversely affect ICT security and reputation risk. ICT availability risk could be affected where institutions face frequent service disruptions or choose not to offer biometric-based services.

The overall impact on ICT security risk would also depend on whether biometric authentication is used as complementary to existing authentication measures or as a replacement. In this context, the European Commission's Delegated Regulation on Strong Customer Authentication[10] (SCA) categorises biometric sensor as a possible security feature for the inherence element of SCA. The regulation will be effective from September 2019 for all electronic payments.

Given the proliferation of mobile banking and the market dominance of certain mobile operating systems, which include built-in biometric authentication mechanisms, a risk of concentration in a small number of market dominant mobile device manufacturers and mobile operating system developers could arise, reaching a systemic level, along with oligopoly and pricing power concerns.

[9] 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[10] Commission Delegated Regulation No 2018/389 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389

It is noted that most of the above could be applicable to other types of biometrics such as face recognition and iris recognition.

4.1.4 Opportunities

The predominant opportunity from the use of fingerprint authentication appears to be an improved customer experience. It could potentially offer customers easier, quicker and more convenient access to their mobile banking applications, and thus to their financial services, without the need to carry tokens and remember usernames or passwords. This could also be part of institutions' strategies for enlarging and/or maintaining their customer bases, depending on customer acceptance.

Even though there is a greater reliance on IT and the external service providers, it could be possible to improve security compared with traditional authentication methods. Fingerprints could also be less prone to theft and spoofing compared to passwords. In addition, fingerprint identification technology seems to be constantly improving; for example, some fingerprint scanners can detect the pulse of the user, thereby reducing the risk of spoofing. As also mentioned above, two-factor authentication could enhance security by combining fingerprint authentication with other authentication factors (e.g. passwords). Fingerprint authentication could possibly lead to a decrease in online phishing/hacking for passwords or embezzlement of funds.

Cost reduction and efficiency gains could also be potential opportunities, as, for example, biometric authentication methods may decrease call centre costs (e.g. for password resets) and customer visits to branches.

It could be possible for fingerprint authentication to be used in other banking/payment applications such as customer on-boarding and customer due diligence processes, given the prospective reduced risk of internal or external fraud through falsification of customer signatures.

4.2 Use case 2: Use of robo-advisors for investment advice

4.2.1 Introduction

Current landscape

The joint committee of the ESAs published a paper[11] in December 2016 describing the concept of automation in financial advice, whereby an institution provides advice or recommendations to consumers, through tools such as robo-advisors, without, or with very little, human intervention and relies instead on computer-based algorithms and/or decision trees.

While robo-advice could be employed in a number of financial services applications, this report focuses on its application to the provision of investment advice, as part of wealth management, to mass-market/retail investors.

Robo-advice can range from the provision of investment recommendations, which are not formally classified as advice and fall outside regulations such as MiFID, to services providing investment advice and automated monitoring and rebalancing of investment portfolios. The ESAs' paper noted that there are different automated aspects to robo-advice services including collection of information from consumers; generation of recommendations; execution of recommendations; and ongoing monitoring of investments. Hybrid robo-advice services also exist, combining automation with human advisors; some business models involve human advisors to provide additional customer services, while others involve human advisors to cater for more complex customer needs. The ESAs paper noted that 'hybrid' models are the most common manifestation of robo-advice.

While automated financial advice does not seem to be widespread in the banking sector, the institutions currently exploring such solutions appear to have adopted different approaches to robo-advice, with some launching their own in-house services and others partnering with, or acquiring, independent providers of robo-advice.

The ESAs in December 2015[12] identified that robo-advice was at that time being actively used in securities, banking and insurance across the EU. Nevertheless, the ESAs report concluded that, while the phenomenon of automated advice may occur across the banking, insurance and securities sectors, it appears that it is most prevalent in the securities sector and not equally widespread

[11] ESAs, Report on automation in financial advice (16 December 2016): https://esas-joint-committee.europa.eu/Publications/Reports/EBA%20BS%202016%20422%20(JC%20SC%20CPFI%20Final%20Report%20on%20automated%20advice%20tools).pdf

[12] European Securities and Markets Authority (ESMA), Joint Committee Discussion Paper on automation in financial advice (December 2015): https://eiopa.europa.eu/Publications/Consultations/JC%202015%20080%20Discussion%20Paper%20on%20automation%20in%20financial%20advice.pdf

across the EU. In its 2017 paper[13], the European Commission (EC) identified that robo-advice has the potential to disrupt the traditional wealth management sector.

Robo-advice wealth management services appear to target retail investors with also increasing offerings for institutional investors. Such services aim to be at low cost thanks to their reliance on automation and are typically available online, aiming to be highly scalable. Robo-advice seems to offer accessibility and affordability for customers who may previously have found wealth management services unaffordable, and poses a challenge to existing service providers, as it covers a rapidly increasing market share of assets under management (AuM).

In June 2017, the FSB reported[14] that the US is the leading market for robo-advice, with about USD 300 billion AuM. In Europe, the FSB reported that robo-advisors are reported to be entering asset management predominantly in the UK, Germany and Italy, although the proliferation of automated advice, brokerage and asset management still seems to be at a relatively early stage.

Researchers identified four trends that appear to fuel the growth of robo-advice firms:

- increased transparency of investment advice;
- increased accessibility through relatively low fees or the absence of a required minimum amount of capital;
- enhanced customer experience via internet- and mobile app-based services;
- use of exchange-traded funds (ETFs) to build diversified portfolios.

According to the ESAs' report on robo-advice[15], several existing EU directives and regulations apply to robo-advice, even if they do not make an explicit reference to it, and might, to some extent, mitigate some of the risks identified in relation to automated financial advice. The report cites MiFID I, MiFID II, the Mortgage Credit Directive (MCD), the Insurance Distribution Directive (IDD), the Payment Services Directive (PSD) and the Packaged Retail and Insurance-based Investment Products (PRIIPs) Regulation. The ESAs decided at that time not to develop requirements specific to robo-advice but to continue monitoring its evolution.

Underlying technologies

In 2017, the FSB[16] reported that FinTech, including services such as robo-advice, could use innovations such as machine learning and artificial intelligence to improve decision-making. However, at the time of the present report, robo-advisors appear to be generally based on

[13] European Commission, Consultation Document – Fintech: A More Competitive and Innovative European Financial Sector (June 2017): https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf
[14] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf
[15] ESAs, Report on automation in financial advice (16 December 2016): https://esas-joint-committee.europa.eu/Publications/Reports/EBA%20BS%202016%20422%20(JC%20SC%20CPFI%20Final%20Report%20on%20automated%20advice%20tools).pdf
[16] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf

automated structured questionnaires to gather and analyse customer responses, determine the investor's risk profile and arrive at an investment proposal. Investment platforms also use algorithms to automatically monitor and invest into a broad universe of funds, including rebalancing investments to remain in line with investor risk profiles as determined by the questionnaires. There is a potential that in the future robo-advice will harness more sophisticated AI-related technology, but the time horizon for this may be in the longer term. Given the specialist nature of robo-advice, institutions seem to have generally partnered with external providers in developing their robo-advice solutions.

4.2.2 Use case

At the moment, robo-advisors take the form of automated structured questionnaires for assessing individual customer risk appetite and knowledge level, then allocating a risk profile based on the assessment and making investment proposals in accordance with that risk profile. In particular, the customer starts by responding to a questionnaire, which gathers basic details on the customer's knowledge, experience, financial situation and investment objectives. The risk tolerance and investment profile preference of the customer are also collected through this questionnaire, possibly in the context of the suitability and appropriateness assessment requirements. All these inputs are then translated into a proposed investment portfolio for the customer. Following the investment, the portfolio is periodically rebalanced to bring the asset allocation to the initial investment recommendation/advice.

It is unclear if the costs of robo-advice services will be affected by the ICT investment required to launch such services and the investment required to demonstrate regulatory compliance.

4.2.3 Prudential risks

As with all the FinTech use cases discussed in this report, the implementation of each technology will play a significant role in its impact on the institutions' risk profile as will the processes and business models adopted around them. Having that in mind, robo-advice could possibly raise conduct-related risks, potentially leading to consequences such as regulator fines and customer redress.

Given the intention for robo-advice to be provided to customers on a large scale, in the event of issues with the quality of the advice provided or its compliance with relevant regulations, conduct issues could have a prudential impact on the institutions' operational risk profile, affecting the safety and soundness of institutions. A range of conduct risks could be conceivable such as the possibility that algorithms will recommend unsuitable products and could also facilitate inadvertent or deliberate market manipulation. This is in addition to the potential fines or redress costs given the potential scale of the service.

The ESAs' paper reported that robo-advice was not equally widespread in all EU Member States, and any risks posed by this innovation were therefore unlikely to have a widespread impact

across the EU. However, at the same time the paper also predicted that the demand and supply of robo-advice would increase dramatically and so this picture could change rapidly.

The possibility of the provision of poor advice could harm both the institution's and the technology provider's reputation. Dependence on external technology providers and other third parties may lead to increased reliance on unregulated third parties, which again calls for attention and could challenge institutions' operational risk management frameworks. This could also potentially contribute to the creation of systemically important unregulated technology suppliers. Furthermore, a possible lack of clarity over how legal responsibility would be attributed between the providers of robo-advice, customers and third-party providers could result in legal risk implications for the institutions.

If robo-advice services were provided across jurisdictional boundaries, compliance with the regulatory and legal requirements of multiple jurisdictions could be another challenging area for institutions that could affect legal and compliance risks.

Robo-advice would be reliant on effective ICT controls to mitigate ICT risks, including change risk, arising from more complex software, testing of which could become more complicated; availability and continuity risk, to ensure the continuity of the service in the event of, inter alia, hardware or software failure; and security risk, arising from the online nature of the service, which could increase vulnerability to cyber-threats such as denial of service attacks or fraud attempts. Highly automated ICT systems could present difficulties in determining the reliability of advice generated, because they may lack transparency or auditability, and this could be exacerbated if such systems utilise AI-based technologies such as unsupervised learning. This could increase compliance risk and also poses a challenge for regulators and supervisors.

If customers are unwilling or unable to answer extensive online questions, and institutions yield to this customer pressure by, for example, limiting the numbers of questions, then the customer suitability assessment could be ineffective, with a chain of possible consequences.

Indirect transmission channels, for example from multiple institutions developing robo-advisors using common development tools or services from the same third parties, could introduce macroprudential concerns in the scenario where (i) a supplier fails, (ii) there is a design flaw in a shared development tool or (iii) similar investment advice is provided by the robo-advisors, potentially exacerbating, for example, procyclicality in markets.

Competition from new, relatively low-cost and highly scalable robo-advice services could possibly affect the profitability of incumbents in the event that they are not able to adapt and compete. While potential competitive pricing might enhance the efficiency of the financial system, it could place competitive demands on established traditional asset managers to consider more competitive pricing and thus lower fees (business risk).

This could have a more significant impact in jurisdictions where financial services are concentrated into a small number of institutions. The potential elimination of human financial advisors could also reduce cross-selling opportunities or increase customer churn if robo-advice services are perceived as readily interchangeable, and possibly undermine the return on investments in the robo-advice services.

There could also be different rates of uptake of robo-advice in different population segments, with some segments of the population potentially unwilling or unable to access robo-advice services where access to the internet is limited. Robo-advisors could possibly have an impact on the mix of investments held by customers, which may potentially affect the liquidity and funding positions of institutions or increase market volatility by increasing the frequency of transactions.

4.2.4 Opportunities

The use of robo-advice promises to provide services without, or with reduced, human intervention, possibly reducing headcount, therefore resulting in offering services at a lower cost than traditional services. A corresponding improvement in customer service may be achieved, including better availability during weekends, evenings etc., given the highly automated nature of the services, reduced potential for conflicts of interest, and recommendations that are tailored to each customer.

Lower prices could possibly increase affordability and accessibility to demographic sectors previously priced out of using wealth management services, thereby widening customer bases and further reducing the marginal costs of the service. Additionally, robo-advice may potentially reduce the need for geographical proximity, promoting access in areas unserved by branch networks while promoting cross-border services and investment.

Robo-advice could possibly create economies of scale for incumbents and new market entrants, although incumbents may be burdened by legacy IT system costs and inefficiencies, while new entrants may be able to enjoy lower costs and higher efficiency. A potential high dependence on IT systems, data and online delivery channels, with a reduced dependence on humans, could reduce the risk of error or fraud and biased advice for customers, with products better aligned to customer needs.

In the scenario where robo-advice becomes established, with multiple providers, it may become fungible, with customers being able to change easily between advisors, reducing concentration risk and increasing competition, thus maintaining low fees. Moreover, robo-advice could possibly enhance transparency, as it could increase visibility to customers of how their funds are invested, and reduce information asymmetry.

4.3 Use case 3: Use of big data and machine learning for credit scoring

4.3.1 Introduction

Current landscape

Credit scoring is a process that aims to assess a customer's creditworthiness and to guide institutions in taking credit decisions. The score may be used solely for acceptance or rejection of a credit application but may also feed into other aspects of the credit offer such as the types of credit available or the interest rate charged to the customer.

Traditional credit scoring methods often focus primarily on data provided by the applicant in the credit application, such as payslips, as well as information the institution itself may request from central credit registers (typically public) or purchase from credit bureaus (typically private). The various data points collected are then used to develop a model through a traditional process that can involve varying degrees of statistical analysis, which is steered, to a large extent, by the developer of the model. Through these means, institutions try to establish the probability of default and the loss given default.

The growing importance of e-commerce, the Internet of Things, big data and increased computational power have prompted the emergence of alternative credit scoring models to assess creditworthiness. These models may use customer data from a variety of sources, such as social media data, data from other lenders, enterprise customer data, publicly available data, location data, mobile data, web data and behavioural data. These data sources may be used to assess qualitative concepts such as behaviour, willingness to pay, responsibility, etc. in order to predict a borrower's probability of default. Technological innovations, which have increased computational power and improved its distribution and availability, are driving the improvement and adoption of machine learning techniques, allowing users to mine large amounts of data to produce models that could perform better and faster than traditional statistical methods.

In a recent report[17], the FSB concluded that machine learning applications can be promising if their specific risks are properly managed. Institutions and relevant service providers have already started using machine learning for a variety of purposes, among which is credit scoring. A number of FinTech start-ups are capitalising on this opportunity by leveraging on large amounts of data to produce challenger credit scoring models, which assess creditworthiness faster and supposedly more accurately, and possibly in cases where conventional data is not available. It remains to be seen if machine learning models will indeed be more accurate, and if institutions that use them will revise their rate of credit acceptance.

[17] FSB, Artificial intelligence and machine learning in financial services (November 2017): http://www.fsb.org/wp-content/uploads/P011117.pdf

Underlying technologies

Machine learning appears to provide the financial sector with novel methods of performing statistical analysis and performing tasks and provides potential advantages over traditional statistics when leveraging another important technological development: big data. The use case discussed in this section will focus on machine learning, regardless of whether or not big data is used; however, it will indicate the risks that may be exacerbated when big data is used.

Machine learning is a sub-category of artificial intelligence, whereby a certain function is developed or improved by computer systems rather than directly by human intelligence. We can distinguish between unsupervised learning, which is a form of machine learning that can be used to analyse datasets when no dependent variable has been defined, and supervised learning, in which case the output (dependent) variable has been defined. While the former can provide insight into patterns that exist within a dataset and reveal these to the user, the latter can be applied with a more specific goal in mind, such as calculating a credit score that represents creditworthiness.

A key concept of machine learning is 'training' the algorithm. During this stage, the algorithm will, through a large amount of iterations, self-optimise to provide the best possible output data from the available input data. While these iterations are in essence similar to what a statistician could do, the algorithm will have no prejudice towards certain variables or functional forms, which a human could have. Complex patterns could also potentially be identified through machine learning, which possibly would not be identified through traditional statistical analysis. In the same way, traditional statistics may steer clear of certain patterns because there is (seemingly) too much noise in the data, or because the data is too complex to transform into a usable form, or because certain patterns are dismissed by prejudice – certain patterns may seem unlikely and are therefore never investigated through traditional statistics.

A promising feature of machine learning is that, after an algorithm has been 'trained', it can continue learning with each new item of information entering the dataset. Some datasets may be static, and grow only when new datasets are added manually, while others may grow or change rapidly, for example when consisting of a list of transactions. While it is technically possible in such cases, and sometimes desirable, to allow the algorithm to learn on a continuous basis, and hence continuously improve itself, there may be good reasons to maintain a stable model for a certain period of time before deploying a new iteration of the model. Such reasons may be model validation, back testing or simply managing computing costs.

While not the focus of this use case, big data may be an attractive source of data for the purposes of machine learning. 'Big data' refers to situations where high volumes of different types of data produced at high speed from a high number of various types of sources are processed, often in real time, by IT tools (powerful processors, software and algorithms). This includes processing of datasets so large and complex that they cannot be handled by traditional data-processing software. Examples of such data are a person's internet searches and browsing history, purchasing history at

different shops and GPS location history, but also 'likes' on social media, etc. Big data may be proprietary data belonging to the institution or third-party public or private data.

4.3.2 Use case

Traditional credit scoring models often rely on a limited set of variables, which applicants may not always be able to provide. Applicants who lack a sufficient credit history, for example because they recently immigrated from another country, may be rejected because no credit score can be calculated for their specific case. In general, institutions may struggle to determine the driver of their credit risk and wish to identify the common factors of defaulting customers.

To this end, institutions may consider the use of alternative credit scoring models, through the use of machine learning techniques, to assess more accurately and faster the creditworthiness of their retail customers. The first significant process of an alternative credit scoring model is the collection and transformation of data points. According to the article 'Credit scoring in the era of big data' from the *Yale Journal of Law & Technology*[18], data points used by credit scoring tools usually fall into the following categories:

a) Borrower's data: information provided directly by the applicant during the application process as well as other information arising from online activities, such as web browser activity, or time spent on reading terms and conditions of the loan to determine if the borrower reads them carefully.

b) Proprietary data: information obtained from privately or governmentally owned data stores (data brokers). It includes the individual's online and offline purchase history.

c) Public data: information obtained from searches of the internet and techniques such as web crawling.

d) Social network data: information aggregated from the borrower's social media posts and any other useful information from the borrower's social network(s).

After collecting raw data points, the data is translated into a usable format to be processed by a computer. Then the machine learning process follows, in which all the data points collected are used as training data for the algorithm. However, only some of them will ultimately be used for calculating the final credit score. The machine learning algorithm, through an iterative process, can specify the most significant input variables, assigning the appropriate weights to them, and then discard all other irrelevant data inputs (i.e. those not used to calculate the credit score). As the learning process advances and becomes more mature, the most significant features are assigned greater weights, as these features are considered crucial for the calculation of the credit score. To

[18] Hurley, M. and J. Adebayo, 'Credit scoring in the era of big data', *Yale Journal of Law & Technology*, Vol. 18, No 1, 2017, Article 5: http://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5/?utm_source=digitalcommons.law.yale.edu%2Fyjolt%2Fvol18%2Fiss1%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages

derive the final credit score, other financial and statistical algorithms may be used in addition to the machine learning process.

Currently, few EU institutions are leveraging credit scoring tools that rely on big data and machine learning algorithms. It is understood that these institutions prefer to use data that has been properly verified and originates from trusted sources. For this reason, it appears that social network data is currently not being used on a large scale. Nevertheless, the limited information about these tools, along with the concern that they may rely on inaccurate data points, has already drawn the attention of regulators and consumer advocacy groups[19].

4.3.3 Prudential risks

The use of machine learning, and possibly big data, for credit scoring comes with certain risks that are not present, or are present to a lesser extent, with more traditional modelling techniques.

A major assumption of any model calibration is that the sample data used is representative of the wider population, or, in the case of credit scoring, the population of possible applicants. For machine learning in particular, there could be an increased risk of retaining false or reverse causal relations that would otherwise be easily detected and removed by human intelligence.

The instability of the credit model that may result from machine learning, due to continuous learning, could make it difficult to assess, challenge, validate and supervise the models or the algorithms used to calibrate them.

The supervision or auditing of machine learning models may be difficult or even impossible, as it could be unclear which model is currently in use, how it was calibrated, how it may change over time when new data is added, or exactly how certain variables are used by the model, increasing operational and model risk. Machine learning algorithms and models have varying degrees of transparency; in some cases, the way variables are used, or even what variables are used, can be particularly opaque.

The use of machine learning algorithms in credit scoring tools may lead to financial exclusion from access to financial services. While this exclusion could be unintentional, it could negatively affect conduct risk, if the algorithm is based on factors not directly related to creditworthiness. Furthermore, as mentioned in the EBA Report on innovative use of consumer data[20], this could also arise if the algorithms discriminate against those who are less willing to share their data online.

[19] Consumer Financial Protection Bureau (CFPB), Requests for information: Use of alternative data and modelling techniques in credit process: https://www.regulations.gov/document?D=CFPB_FRDOC_0001-0521

[20] EBA, Report on innovative uses of consumer data by financial institutions (28.06.2017): https://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf

The analysis of data points through an automated process and without human judgement may indirectly lead to discrimination by considering sensitive characteristics (race, sex, ethnicity, etc.).

Machine learning implementations for credit scoring may steer institutions away from their credit strategy and policy, through a vicious circle whereby certain types of customers could unintentionally be excluded from the provision of new credits, as a result of which no new learning data on these customers would be obtained and hence the mistake could potentially not be corrected over time.

The development, implementation and (back-)testing of these models could be more complicated, and may be more resource-intensive, than maintaining more stable models over time. As a result, the operational risk, including in particular ICT change risk, could increase.

The scalability of data and new technologies may give rise to third-party dependencies, also increasing the ICT outsourcing risk. This could in turn lead to the emergence of new systemically important players. Having regard to the activities of, and services provided by, these entities, it may become appropriate to review the regulatory treatment of such entities. Such a review may involve a range of authorities taking account of the potential issues (e.g. prudential treatment, consumer protection and data privacy).

There may be an increase in ICT data integrity risk, as some types of alternative data may be non-proprietary and inconsistent, incomplete or inaccurate.

ICT security risk may be increased, as personal data stored in credit scoring systems could be highly attractive targets for hackers.

4.3.4 Opportunities

The use of machine learning could possibly mine large amounts of data efficiently, including poorly structured or unstructured datasets, thereby finding patterns and relations that may be difficult to find with more traditional statistical modelling techniques. In addition, machine learning algorithms could dynamically adapt to new data, and thereby quickly detect changing patterns or allow the use of previously unavailable data. This could potentially improve institutions' resilience against such new negative trends or make them aware of existing bias in their credit portfolio.

Unlike traditional modelling techniques, machine learning would not avoid complex calculations or outcomes unless it is programmed to do so. More specifically, certain complex patterns may never have been tested through traditional modelling, as they were deemed too complex, while machine learning could reveal that they perform significantly better than their simpler alternatives.

Institutions often own large amounts of data that is verified, trusted and audited. Through machine learning, they could possibly exploit this data efficiently to produce more accurate credit scoring results for their customers.

Machine learning appears to allow its users to integrate qualitative factors into their credit scoring more easily while still applying statistical testing and calibration methods. As the accuracy of credit scoring could potentially grow, institutions could also exploit the same credit score to determine the interest rates to be paid by different customers. A more risk-based rate could be in the interest of the institution.

A potential fully automatic and trusted credit scoring model could be used to automate the credit acceptance process, potentially improving the speed for customers and further digitalising the process. Such an opportunity could be valid for any automated credit scoring model.

The large amount of variables that could potentially be exploited using big data and machine learning may lead to better customer screening and financial inclusion, by increasing the accessibility of financial products to consumers, especially for borrowers who do not generally have access to credit because of limited credit information data, although this remains speculative in the absence of evidence (as also mentioned in the EBA Report on innovative use of consumer data[21]).

[21] EBA, Report on innovative uses of consumer data by financial institutions (28.06.2017): https://www.eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf

4.4 Use case 4: Use of DLT and smart contracts for trade finance

4.4.1 Introduction

Current landscape

Trade finance is a complex process in which disparate actors are involved, especially in the case of international trade, where it is challenging to reconcile the divergent necessities. While the exporter would prefer to be paid up front, the importer runs the risk that the shipment will not take place. Conversely, if the exporter ships the goods, the importer may refuse to pay.

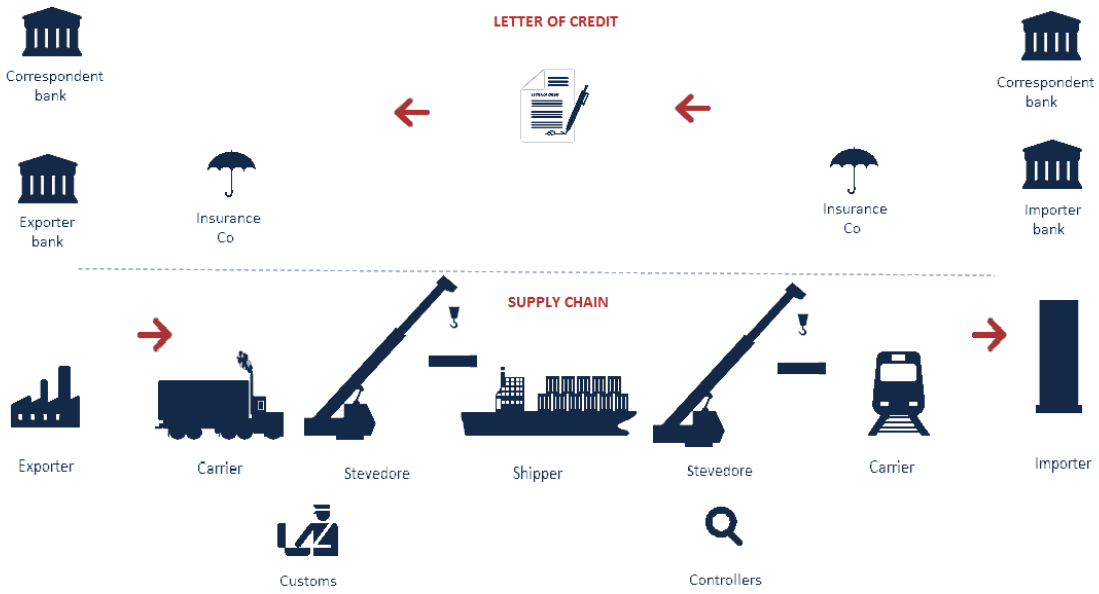


Figure 2: Supply-chain and letter-of-credit flows

Banks have played a key role in mitigating the risks that trade finance and supply chains pose, in both domestic and international trade, such as, inter alia, compliance with laws and regulations currently in force in each and every jurisdiction, counterparty risk, risk of goods being lost or damaged in transit, and foreign exchange risk. In order to mitigate these risks, banks offer various products to their customers, such as bank guarantees, to ensure payment when the other party does not fulfil its contractual obligations, or letters of credit, aiming to guarantee the payment to the exporter upon receiving proof that goods have been shipped.

The execution of a letter of credit starts with the agreement upon the sales terms between the exporter and the importer and consists of a number of steps:

a) The importer applies to the issuing bank for a letter of credit in favour of the exporter. Once checked and approved, the letter of credit is forwarded to the exporter's bank. If the importer's bank and the exporter's bank are located in different countries, they can interact through correspondent banks.

b) The exporter's bank forwards the letter of credit to the exporter, which reviews it. If there is no discrepancy, the exporter ships the goods and sends to its bank all the documents to be used as proof of shipment.

c) The exporter's bank examines the aforementioned documents and whether they comply with the letter of credit or not.

d) If the exporter's bank considers that the criteria of the letter of credit are met, it claims the funds and posts the proof of shipment to the importer's bank.

e) The importer's bank examines the documents and, if they are in order, debits to the importer and forwards the documents to the importer. The importer uses the documents to clear the goods from the customs.

In this context, many stakeholders may participate in a trade transaction, such as the exporter, the importer, banks, insurance companies, carriers, stevedores, custom offices, shippers and controllers, each one having its own ledger, with the consequent need to reconcile their registries. In addition, tracking the status of each transaction may require querying a number of stakeholders.

Underlying technologies

Distributed ledger technology (DLT) is the term used to refer to those technologies that allow a common ledger to be shared across networks of computers. In particular, this report focuses on blockchain, which is a particular type of DLT. Although some implementations within the banking sector are diverging from the original conception of blockchain, many of the characteristics described below are also applicable to other types of DLT.

Blockchain is based on previously existing technologies, combined in an innovative way to implement a decentralised and distributed ledger in a peer-to-peer network. Transactions are signed by the issuer, validated by consensus among a group of nodes and stored in blocks that are chained cryptographically (each block includes a hash [22] of the previous block), making the blockchain more difficult to tamper with.

As regards other features of blockchain, the chronological order of transactions in different blocks is ensured and the inclusion of digital signatures aims to guarantee authentication, non-repudiation and integrity of transactions in the ledger.

Taking into account all the above, the need for a central counterparty would disappear, as participants could rely on the platform itself.

[22] A hash is a function that converts an input string of any length into an encrypted output of a fixed length; a hash is created using an algorithm.

There are different types of distributed ledger depending on who is able to read, create or include transactions permanently on the ledger:

- Public versus private: in public ledgers, anyone has access to read the ledger while, in private ledgers, they need to be granted access. In some private ledgers, only those involved in a transaction are allowed to read it.

- Unrestricted versus restricted: in unrestricted ledgers, anyone is able to create transactions while, in restricted ledgers, authorisation is needed in order to create transactions.

- Permissionless versus permissioned: in permissionless ledgers, anyone can validate transactions and include them permanently in the ledger while, in permissioned ledgers, only some members are able to do it.

Bitcoin was the first application of blockchain. This is an unrestricted, public and permissionless implementation of a distributed ledger for digital exchanges that stands as proof of every transaction on the network.

Nevertheless, as privacy of information is a key requirement for numerous services, attention is currently being diverted towards restricted ledgers, where an institution or consortium administers the ledger, with authorised and recognisable members and a limited group of trusted validators.

Smart contracts are not a new concept per se either. There have been a number of definitions for them since the 1990s. However, only very recently have smart contracts generated great expectations, especially in conjunction with DLT, although other technologies could also make use of them.

For the purposes of this report, 'smart contracts enabled by DLT' refers to pieces of computer code stored in a DLT, which are executed automatically on multiple distributed nodes upon fulfilment of pre-defined conditions, to enforce the terms of an agreement between parties. Therefore, agreements are automatically enforceable. Smart contracts may store the status of a transaction, to avoid having to go through the list of records in the DLT, and their execution can be triggered by another contract, by an individual or by a group of individuals if multiple parties are involved in the approval process for the execution of the contract.

Smart contracts may be:

- Pieces of computer code designed to be executed when pre-defined conditions are met, without an underlying legal contract.
- Extensions to a legal contract written in computer code.
- Legal contracts or parts of legal contracts set down in writing, transposed into software code and executed by computers that participate in the DLT network. Not all parts of a contract are susceptible to be automated, and sometimes that automation might not even be desirable.

4.4.2 Use case

As described above, nowadays trade finance is grounded on paper-based contracts travelling around the world with settlements that may take weeks, resulting in a rather inefficient process. Additionally, stakeholders are not provided with end-to-end visibility of the entire process and disputes may arise around the interpretation of contract terms.

For these and other reasons, a number of companies engaged in trade transactions have been analysing whether or not DLT, and more specifically smart contracts running within a permissioned DLT, could be used to streamline the process. DLT enables a common and almost real-time view of a trade transaction stored in a shared ledger for all participants involved, creating a level playing field for all parties and eliminating their reliance on paper instruments exchanged among them. A shared view could rationalise the manual effort and reconciliation processes, with consequent savings in time, money and resources.

From the moment the importer applies for a letter of credit, the application could be registered in the ledger. Once the importer's bank approves the letter of credit, the seller could receive a notification triggered by a smart contract, being able to initiate the shipment of goods immediately, saving days or even weeks compared with the previous procedure. Every step along the supply chain could also be registered in the ledger, as well as any event or data related to the process, including invoices, shipment data, payment status, photos or any other useful information.

In some cases, only a number of the participants in a trade transaction are directly involved in the distributed ledger while others could access it through intermediaries providing the service or using traditional procedures, such as paper-based contracts.

Smart contracts stored in the DLT could trigger other actions when pre-defined events occur in a trade transaction. For example, funds could be released to the seller when the custom office registers that the good have been cleared. Additionally, embargo and sanction lists could be queried by means of smart contracts to guarantee that funds will not be transferred to banned parties or countries.

At the time of writing this report, the use of DLT and smart contracts for trade finance was still a prospective use case, as a number of entities had developed proofs of concept to verify its feasibility and potential, but DLT had not replaced the traditional processes.

4.4.3 Prudential risks

The use of DLT and smart contracts for trade finance poses several risks from a prudential point of view. Some are due to the immaturity of these technologies, while others relate to the legal and regulatory uncertainties or the difficulties entailed in designing the governance of such a model.

Currently, potential legal and compliance risks could arise from a number of factors such as the uncertainties around the applicable law, the unclear and uncertain legal value of smart contracts and the lack of a clear applicable jurisdiction, as the DLT nodes could be located in different jurisdictions whose laws may even conflict with each other. For example, a digitally signed contract might not be enforceable in all the jurisdictions. It is essential to establish the applicable jurisdiction, in case of conflict, and the dispute mechanisms, when a dispute arises. Furthermore, the possible absence of a central party to govern the platform and assume liability could pose additional challenges to the overall governance and management of the model.

Despite the use of DLT, the risk of forged papers could arise again if not all the participants accept the use of digital documents.

Potential compliance issues with the relevant regulations could arise, for example on personal data protection if sensitive personal information is revealed; on competition laws, especially when joining consortia; or on AML/CFT. With specific regard to the AML/CFT regulation, as this technology potentially allows less physical analysis of documentation, DLT could lead to abuses for money-laundering and terrorism-financing purposes. Non-compliance with these regulations could carry large fines, with a material financial impact and possible reputation consequences.

The overall governance of the distributed ledger, such as who is allowed to participate in the ledger and each participant's role, how to proceed if one member loses its private key or whether or a member could be expelled from the platform on the grounds of non-compliance with the governing rules, could raise significant challenges for all the participant institutions. A lack of adequate governance could have a negative impact leading to operational and reputation risks.

The dependence on third parties could be increased, as DLT and other systems around the platform would generally be provided by ICT service providers.

A concentration risk may also arise if multiple institutions rely on the same provider, implementation or consortium, leading to macroprudential concerns, i.e. a possible single point of failure.

Possible impact on ICT security risk could arise because, although data is replicated in different computers, undermining the possibility of altering the ledger, it could also entail more nodes to protect, each one with a different security level. Furthermore, the sums involved in trade transactions could incentivise internal or external fraud, including at the level of organised crime.

An attacker could exploit a vulnerability in the weakest node to steal its private key, to forge a node or to access sensitive data of persons or companies, especially when data is stored in clear text. Even in those cases where encrypted data is stored, it could be possible to correlate transactions when they are made using the same public key. Additionally, when smart contracts need to send or retrieve external data, they rely on external services, the so-called oracles, which could also be attacked or unavailable.

Computer code is distributed throughout the DLT, and correcting a mistake in every node becomes challenging, affecting the ICT change risk. Keeping all nodes updated to the last version of the software and testing the changes could also be more complicated than in a centralised system.

While DLT is generally perceived as more resilient than traditional systems thanks to its distributed nature, it could also pose ICT availability and continuity risks, caused by nodes or networks being maliciously collapsed, that could prevent it from validating and sharing transactions.

In addition, operational errors may be exacerbated by the fact that errors in the data or computer code could be quickly propagated throughout the DLT.

In the scenario where trade finance transactions are streamlined through the use of DLT, institutions could be pressured to reduce fees and commissions on foreign exchange, with therefore a possible impact on business risk.

Lastly, a potential poor service, poor user experience and fines for non-compliance could negatively affect the overall reputation.

4.4.4 Opportunities

A number of opportunities emerge from the use of DLT and smart contracts for trade finance. The most promising are the potential efficiency gains, cost reduction, and lower risk of duplicate financing and loss or manipulation of documents.

DLT technology appears to be able to provide efficiency gains by reducing administrative burden and unnecessary waiting times. Events could be automatically triggered by smart contracts, and processes could be streamlined by eliminating reconciliation needs, possibly leading to quicker execution of transactions. Nevertheless, gains could be reduced when not all the parties of a transaction are directly connected to the ledger, as paper instruments or reconciliation processes may be still needed at some stage.

Institutions could benefit from the use of smart contracts and DLT through the potential opportunity of reducing processing costs by the elimination of manual processes and reduction of the number of physical paper instruments. This could depend on the adoption of such applications and whether parties would use a common platform or two interoperable platforms.

Institutions could leverage this application to enlarge their customer base by offering a more convenient, efficient and transparent solution to their customers.

Furthermore, as the proof of the documents involved in a transaction would be stored in the ledger, their existence and integrity could be verified, possibly preventing duplicate financing and potentially reducing the amount of loss and number of manipulated documents while keeping audit trails. This could potentially encourage institutions to boost their trade finance business, with the possibility of enlarging their customer bases.

DLT technology could potentially make the trade finance platform more resilient, as transactions would be distributed and replicated in multiple nodes, thus providing high availability, as the platform would continue working even with a limited number of nodes not working properly, offline or controlled by malicious parties.

The time exposed to counterparty credit risk could be reduced, as smart contracts could trigger the claim of funds when certain criteria of the letter of credit are met.

As cash flows could be automated by the use of smart contracts, the time of disbursement could be potentially easier to predict, thus reducing liquidity risk.

With DLT, all participants could share a common view of the ledger, the same source of authoritative information, instead of multiple databases spread across all stakeholders. That would avoid the consequent reconciliation needs and potentially reducing disputes.

The participants in a trade transaction could be able to enter and read the information related to the transaction in the ledger. This could potentially create a level playing field for all participants and provide transparency, with almost real-time visibility of each step along the process, improving coordination between participants.

End-to-end visibility granted by the existence of a distributed ledger could make it easier for participants to spot transactions or patterns that may give rise to suspicions of money laundering or terrorist financing or warrant the application of enhanced due diligence measures in line with applicable AML/CFT obligations, such as unit pricing that appears unusual or goods that are shipped through another jurisdiction for no apparent commercial reason.

Smart contracts could allow the possibility of including dispute resolution mechanisms in their code.

Lastly, the overall automation could make the process less prone to errors by significantly reducing the possibility of human mistakes. However, this could also have a disadvantageous effect, with low-frequency and high-impact operational losses.

4.5 Use case 5: Use of DLT to streamline CDD processes

4.5.1 Introduction

Current landscape

'Digital identity' refers to the information used to represent an entity in an information system. The purpose of the information system determines which of the attributes describing an entity are used for an identity[23]. In this regard, it is important to consider that an entity encompasses persons (physical or legal), objects (information, systems or devices) or a group of these individual entities. Besides, attributes could be heterogeneous in nature, for example name, phone number and educational background for natural persons or, as regards a legal entity, a statement attesting its financial situation or the result of the verifications of its data in a customer due diligence (CDD) process.

When it comes to CDD, institutions must comply with Directive (EU) 2018/843 on the prevention of money laundering and the financing of terrorism as transposed in their national legislation. The Directive requires that institutions should assess money laundering and terrorist financing risks associated with their business and customers and put in place group-wide policies and procedures to mitigate these risks. To achieve this, institutions are required to exchange information with their branches and wholly owned subsidiaries within the EU and third countries to the extent permitted by local laws.

The ESAs published an Opinion[24] on the use of innovation solutions in the CDD process in an effort to support the appropriate use of innovative solutions where these improve the effectiveness and efficiency of AML/CFT compliance. One of the measures applied by the institutions to mitigate ML/TF risks is the identification and verification of customers on the basis of documents, data and information obtained from reliable and independent sources. In this context, digital identity and attribute sharing becomes relevant, as the customer identification and verification is carried out by each institution as part of their customer on-boarding and the heavy burden of this task could potentially be shared between the institutions.

Recently, a number of initiatives have emerged on digital identity and attribute sharing across institutions[25] as well as on CDD management simplification. The use of digital identity in the EU has evolved considerably because of a number of factors, which range from new legislation to support

[23] Information technology: Security techniques – a framework for identity management. Part 1: Terminology and concepts: ISO/IEC 24760-1:2011, https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:24760:-1:ed-1:v1:en

[24] ESAs, Opinion on the uses of innovative solutions in the CDD process, 23 January 2018: https://www.eba.europa.eu/-/esas-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process

[25] In Canada, the Canada Revenue Agency has set up a digital identity and credential-sharing network with financial institutions to facilitate the login process for users; Brazil's Ministry of Planning, Budget and Management is conducting a pilot run of a blockchain-based identity application to verify the legitimacy of personal documents; and in Spain, Alastria, a multi-sector consortium, is establishing a semi-public blockchain/DLT infrastructure with an initial focus on digital identity.

interoperability and mutual recognition of digital certificates like eIDAS Regulation[26] to concrete steps taken by some Member States[27] towards a digital society. The intensive use of the internet, social networks and portable devices to interact with each other or to consume products and services has also played an important role in the evolution of digital identity as much more information about a person is now collected and available online. Currently, entities share their digital identity with many institutions and service providers with which they have a business relationship. This is a challenging process for both institutions and entities as the information required by different institutions is often repetitive and needs to be kept up to date.

Underlying technologies

Currently, a number of digital identity solutions enabled by DLT are under discussion in the market. In general, these solutions are based on (i) a DLT that stores proof of public keys of the identities and proof of data and attestations; (ii) external data storage where data and documents are located; (iii) an end-user application to control the identity; and (iv) smart contracts orchestrating the process. The elements involved are described in more detail below:

- End-user application: this holds the user's private key[28], which controls the digital identity. The private key is stored in a secure part of the device and associated with a unique identifier generated during the registration process. The unique identifier will be permanently linked to the person. Users can identify themselves in online services, and share attributes and attestations of their identity through this application.

- External data storage: users' attributes can be stored on an external data store (InterPlanetary File System, Dropbox, bank's database, etc.). Cryptographic proofs of this external data could be stored in the DLT as evidence. External data may also reference the proofs stored in the DLT network.

- Distributed ledger: this acts as a decentralised public key infrastructure (DPKI) that maintains the link between public keys and identities. The ledger stores the smart contracts and the proofs or hashes of the public keys of the identities. Additionally, the ledger could store metadata, claims and attestations, or cryptographic proofs or hashes of all the above.

- Smart contracts: these form the core of the identity. They cryptographically bind the unique identifier to the identity and its attributes and allow identity recovery in the case of device loss or theft. In order to recover an identity, it is necessary to achieve consensus among members in a previously defined recovery network that could be formed by individuals, such as chosen friends and family members, or institutions, such as financial institutions and government agencies. When reaching consensus, a new key pair is generated for the

[26] Regulation (EU) No 910/2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014R0910

[27] Initiatives in some jurisdictions, such as Estonia, involve a unique digital identity issued by government authorities.

[28] Private key is a cryptographic key, a variable that is used with an algorithm to encrypt and decrypt code.

same unique identifier. The new private key is installed on the device while a proof of the public key is stored in the DLT, and they become the new valid key pair for that entity.

Each digital identity may have an associated list of attributes. These attributes can be signed by the owner or by a third party who certifies their veracity, giving rise to attestations. By the use of cryptography, other entities are able to challenge the authenticity and integrity of these attestations. The following are examples of potential attestations in a digital identity:

- customer's data verified in a CDD process and attested by an institution to be used in subsequent CDD processes;
- customer's financial situation attested by an institution;
- others, such as educational background attested by a university, medical data certified by a hospital.

4.5.2 Use case

Some institutions are currently exploring the possibility of sharing verified customer data with other institution through the use of DLT in order to avoid the duplication of efforts and enhance their customer experience by making the on-boarding process more convenient for them in comparison with the traditional processes, for example, where the customer is required to be physically present at the time of the identity verification. Due to potential compliance issues stemming from the use of personal data, institutions are narrowing the scope to share only CDD data and verification results of corporate customers. This is the use case described in this report.

Initially, when the platform contains only limited or no information about the customer, the institution performs the identification and verification of the customer in a way that is commensurate to the ML/TF risk associated with the customer. Upon verifying the information received from customers, the institution would store the digital version of relevant documents and information received on its internal database. The hashes of the documents and proofs of the result of the verification process (verified or rejected) could be stored in the DLT.

As the verification result is linked to the digital identity of the customer, the customer can disclose it together with the digital version of the documents in subsequent on-boarding processes. Institutions may trust the documents if their hashes are the same as those in the distributed ledger.

In this context, the receiver of an attestation may verify its integrity on a basis of who issued it and whether or not it is reliable for its purposes (e.g. depending on who is the issuer or if the attestation is recent). This could allow simplification of the process of verifying the authenticity of the documents and consequently reduce the associated costs and time.

In addition, this technology has the potential to change profoundly how customers are accessing financial services online, as it would enable the use of a single digital identity, making it more convenient. It would also allow clients to present digital documents and attestations instead of

physically carrying documents to a branch. On top of that, customers' information could be kept up to date in a single place and the institution could receive a notification when it changes, triggered by a smart contract stored in the DLT. However, there might be times that the digital identity stored on the ledger might not be sufficient to meet the participating institutions' CDD requirements and additional documentation or information might be required to mitigate the risk associated with the customer e.g. personal data and information related to a beneficial owner (natural person) of the corporate customer.

While there are several major technology companies which have announced new alliances with start-ups, specialising in digital identity and attribute-sharing solutions based on DLT, all these initiatives appear to be at early stages and have not produced any tangible results so it has not been possible to assess their effectiveness when used in AML/CFT compliance.

4.5.3 Prudential risks

While this specific use case has not been seen to be implemented yet, there are a number of prudential risks that could arise, possibly related to potential compliance issues, lack of an adequate governance, dependence and concentration on third parties, legal uncertainty, unclear liability and ICT risks. Some of these risks are already described in use case 4: 'Use of DLT and smart contracts for trade finance'.

A possible impact on compliance risk could arise if institutions rely on previous CDD processes performed by others, as there is the risk of trusting invalid or incomplete CDD verifications and therefore facing compliance issues for not fulfilling their AML/CFT duties, which remain obligatory for institutions. An invalid, incorrect or incomplete verification made by one institution could affect the other participant institutions, if they trust the previous CDD measures. Compliance risk is further increased where DLT is used in the CDD process by institutions based in different member states due to the jurisdictional nature of the AML/CFT legislation.

The potential legal and regulatory uncertainties relating to digital identity could have an impact on the corresponding prudential risks, as in some jurisdictions a digital identity may have a different legal status than in others (as happens with digital signatures). Furthermore, the legal status of smart contracts is also uncertain and unclear. In general, because of the distributed nature of this technology, it could be difficult to assign liability when a risk materialises.

In addition to the provisions of competition law, which should be respected when forming consortia or other forms of cooperation, potential legal issues could arise if personal data is collected within the digital identification process, in the context of the GDPR.

The overall governance of the distributed ledger, such as who is allowed to participate in the ledger and its role, who could be part of a recovery network, how to proceed if one member loses its private key or whether or not a member could be expelled from the platform on the grounds of non-compliance with the governing rules, could raise significant challenges for all the participant

institutions. A lack of adequate governance could have a negative impact leading to operational and reputation risks.

The dependence on third parties is expected to increase, as DLT, external data storage, end-user applications, oracles and other external systems would generally be provided by ICT service providers. A concentration risk may also arise if multiple institutions rely on the same provider, implementation or consortium, leading to macroprudential concerns, i.e. a possible single point of failure.

ICT security risk could potentially rise due to inadequate protection of sensitive data in transit and in storage. In particular, sensitive information on external data stores could be leaked or inappropriately accessed, especially if not encrypted. Recovery networks may not be adequately managed or may be deceived or attacked to get others' identities. Once an identity is compromised, it could be used to impersonate an entity or its attestations, and the legitimate owner might possibly face difficulties in proving its real identity. In an extreme scenario, if an attacker could impersonate enough members in the recovery network to reach consensus, the whole system would be compromised.

Digital identities or attestations could possibly be manipulated by generating documents producing the same hashes as those stored in the ledger. End users' devices could also be attacked to obtain identities, constituting another attack vector that could give rise to fraudulent impersonation of customers. This risk would not be fully controlled by institutions, as their security would depend on the manufacturer and also on users' precautions. Moreover, as the network is formed by a number of nodes, a node with a lower security level could be used to gain illegitimate access to the DLT.

Computer code is distributed throughout the DLT and correcting a mistake in every node could become challenging, with a possible impact on ICT change risk. Keeping all nodes updated to the latest version of the software and testing the changes could also be more complicated than in a centralised system.

While DLT is generally perceived as more resilient than traditional systems thanks to its distributed nature, it could also pose ICT availability and continuity risks caused by nodes or the whole network being collapsed maliciously, which could prevent the validation and sharing of transactions.

As data, information and documentation obtained as part of the CDD process could be accessed from internal systems or stored in internal databases, inadequate integration with them would lead to operational risks, which could be exacerbated by the fact that errors in the data or computer code are quickly propagated throughout the DLT.

An improperly managed recovery mechanism could potentially damage the reputation of the institution, for example by locking customers out.

4.5.4 Opportunities

In addition to the potential benefits of the DLT, such as decentralisation, resilience and reduction of data integrity risk, a number of potential opportunities could possibly stem from its use as part of the CDD process by institutions. The most relevant appear to relate to cost reduction and improved customer experience resulting from a possible simplification of the process and access to updated information.

When it comes to the on-boarding of new customers, institutions could potentially leverage their CDD measures previously applied by other institutions (subject to the respective risks mentioned above), thus reducing costs generally associated with AML/CFT compliance.

To share data through this technology, institutions would need to integrate their systems with the network instead of deploying solutions for each participant's software, eliminating the costs and effort needed to deploy different solutions.

As the data and information on corporate customers could be stored in a single place which can be accessed by all participants in the DLT, such data and information is continuously updated by all participating institutions. This means that additional information required by the institution to meet the enhanced CDD requirements where the customer is considered high risk, may already be saved on the platform by other participating institution.

New business models could potentially appear, as institutions could be also seen as data service providers, offering services such as certifying the solvency or financial situation of their customers by generating attestations for third parties, offering identity recovery services or even validating digital identities.

Lastly, the automation could make the overall process less prone to errors by significantly reducing the possibility of human mistakes.

4.6 Use case 6: Mobile wallet with the use of NFC

4.6.1 Introduction

Current landscape

In the last few years, a number of innovations have influenced payments, leveraging mobile devices and connectivity, with examples ranging from digital wallets to automated machine-to-machine payments. The majority of these innovations are modifying banking front-end processes to improve customer experience while leaving the underlying operating infrastructure unchanged. Nowadays, digital wallets for mobile payments are becoming a promising FinTech service provided mostly by non-bank institutions.

According to Visa's 2016 Digital Payments Study[29], the number of consumers regularly using a mobile device – whether a smartphone, tablet or smartwatch – to make payments had tripled in 2015. In 2016, in the EU, 54% of consumers surveyed used a mobile device regularly to make payments for everyday goods and services, compared with 18% in the previous year. The increase in mobile payments coincides with the greater adoption of contactless technology, such as NFC, Bluetooth and quick response (QR) code. The research indicates that, across all age groups, contactless payments are now becoming the norm.

In the EU, the same study also highlights the correlation between the usage of contactless payments and new payment solutions, revealing that contactless users are more interested in using solutions based on a mobile device with a debit card digitalised and loaded on the device.

A mobile wallet is a digital wallet that allows customers to have, in a single application on a portable device, one or more payment instruments stored in a digital form, such as NFC contactless card payment, virtual cards, direct debit and other types of payment instruments. Digital wallets are electronic applications that offer customers easy access to their funds, through cards or other payment instruments, and other data in order to make payments for goods or services, in stores or online over the internet; the wallet can be linked to payment accounts to fund payments and reduce the need to carry cash or plastic payment cards, and allow internet payments.

The rise of NFC mobile payments started in 2014, when Apple launched the Apple Pay solution and many other companies followed, offering similar solutions. Other examples of mobile wallets are Google Pay, Samsung Pay, Alipay, PayPal Mobile App and Swish[30]. Other potential actors will enter the market in the near future, and a number of institutions are also offering their own solutions.

Today, the mobile wallet market appears fragmented and in its early developmental stage. The frontier of the competition seems to be defined by the large commerce ecosystems managed by

[29] Visa Europe 2016, https://www.visaeurope.com/media/pdf/40172.pdf

[30] In Sweden, a mobile wallet with the use of NFC is available, but the dominant solution for payments is Swish, a non-NFC payment app for mobile phones. The situation of Alipay is similar for Chinese customers.

BigTech[31] firms. Moreover, since January 2018, the application of PSD2[32] and the related set of guidelines and technical standards for the security of payment services[33] are expected to facilitate innovation, competition and efficiency as well as ensuring the security and protection of customers.

Underlying technologies

A mobile wallet is a digital wallet installed on a mobile device. Digital wallets can be grouped into two broad categories: client-side and server-side.

- Client-side wallets are generally maintained by the customer, who downloads and installs a program and then enters all pertinent payment data on a mobile device.
- Server-side wallets are those maintained by the company supporting the digital wallet account and data on its systems.

Payments initiated via a mobile wallet and processed through card networks do not change the fundamental design of the system that is already set up for card payments[34]. The process is replicated, with the significant difference that card and payment data are replaced with token[35] and cryptogram[36] to prevent real card data from being sent over the network and stored somewhere.

How tokens and cryptograms are handled by the mobile wallet, how the security of them in storage and in transit is managed, and the design of the mobile wallet are essential for the security of mobile payments and depend on the underlying technologies[37].

[31] 'Big tech' refers to large globally active technology firms with a relative advantage in digital technology (BCBS, February 2018, https://www.bis.org/bcbs/publ/d431.pdf).

[32] **Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.**

[33] **EBA, EBA mandates in PSD2 and their timelines:** https://www.eba.europa.eu/documents/10180/87703/EBA+Mandates+PSD2.pdf/5c2493a4-ef26-4434-8338-736895bd423f

[34] For a traditional card-based payment, the cardholder initiates the transaction by transmitting payment authorisation data, including the primary account number (PAN), to the merchant, such as by swiping the magnetic card or by inserting the chip card at the POS. The merchant then relays the data to the acquirer and then the card network relays this to the issuer for authorisation.

[35] Instead of the card number (PAN) and the verification code (CVC).

[36] A one-time encrypted string representing transaction and merchant information.

[37] ENISA, Security of mobile payments and digital wallets (December 2016), https://www.enisa.europa.eu/publications/mobile-payments-security.

Mobile wallets can use different communication technologies to exchange data between the portable device and the merchant (POS or online), such as magnetic secure transmission (MST[38]), NFC[39], QR[40] codes, Bluetooth[41] and short message services (SMSs), as well as the internet.

One of the promising technologies, NFC, is an international standard for two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 2-10 cm of each other. Major solutions currently available for NFC payments range from SIM-based solutions[42] to software that emulates NFC cards[43]. However, the most common solutions are based on the device or on the operating system (OS). Basically, device-based solutions (provided by mobile device manufacturers) manage secure payment elements directly on the device whereas those based on the OS use specific functions embedded in the OS of the smartphone[44].

4.6.2 Use case

A number of institutions in the EU have already launched mobile wallets, and their diffusion depends largely on consumer habits in individual jurisdictions. Institutions can develop mobile wallets in-house, adopting for instance a host card emulation (HCE) solution, or outsource to (or partner with) a third-party provider.

Mobile wallets, like any other digital wallets[45], provide a method for making payments electronically, allowing users to make transfers between traditional bank accounts and payment accounts at non-bank payment service providers (often the digital wallet provider itself). Payments can have several purposes, including bilateral money transfers between consumers, and those from customers to businesses to buy goods and services. Mobile wallets can also store other information, such as driving licence details, health cards, loyalty cards and other documents that can be passed to the merchant using NFC technology.

The customer should follow a number of steps for using its mobile wallet for NFC payments:

a) the enrolment, through which the customer registers with the wallet service and identifies itself to the provider, defining its digital credentials;

[38] Samsung, 'What is MST (Magnetic Secure Transmission)?': http://www.samsung.com/us/support/answer/ANS00043865/

[39] Want, R., 'Near field communication', *IEEE Pervasive Computing*, Vol. 10, No 3, 2011, pp. 4-7.

[40] Walsh, A., 'Quick response codes and libraries', *Library Hi Tech News*, Vol. 26, No 5/6, 2009, pp. 7-9.

[41] Haartsen, J.C., 'The Bluetooth radio system', *IEEE Personal Communications*, Vol. 7, No 1, 2000, pp. 28-36.

[42] This was the first solution provided for NFC contactless payments on telephone devices and has been available since 2007. It is similar to those used in credit cards and electronic ticket smartcards.

[43] Host card emulation (HCE) allows mobile applications to provide NFC contactless payments independently of the phone operators, smartphones or pre-defined payment solutions, enabling providers to offer their own solution more easily and without changes to the provider payment infrastructure.

[44] Although Apple Pay encrypts and protects card secure elements in the device.

[45] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf

b) the card digitalisation, which is the virtualisation of one or more of the customer's cards (payment or of other type) on the mobile device and the transformation of the PAN into a secure token, stored in a secure mode depending on the type of NFC solution used[46];

c) the NFC payment itself, which could be a single or multiple transactions initialised by the customer to purchase goods or services in a physical store provided with a contactless point of sale (NFC-POS), or to send money to another customer, face to face.

A specific characteristic of mobile wallets is the adoption of many innovative technologies, such as mobile banking, digital wallets, biometric authentication and NFC, to enable a new business model for the retail payments market. This new business model appears to be aiming to create value from (i) a customer-centric service, leveraging the needs of targeted segments of the public and opportunities of multiple distribution channels; (ii) an inter-organisation, or cross-company, network in which transactions are facilitated through coordination and collaboration among parties; (iii) an innovative technological architecture that identifies the required ICT solution and organisational arrangements for the efficient and effective management of payments.

4.6.3 Prudential risks

The development of a mobile wallet could potentially have different impacts on institutions' risk profiles depending on whether or not a third-party provider is involved. Nevertheless, a number of prudential risks could possibly arise on both scenarios, such as legal risk and ICT security risk as well as the wider operational risk. Possible implications for business risk should also be considered in addressing potential business model changes.

Legal concerns could possibly arise from a fragmented payment market and a complex operating environment in which the institution manages several providers of different parts of the payment service.

A fragmented payment market together with the proliferation of innovative products and services could bring about changes in operational processes and therefore new challenges for the governance, management and control of the overall operational risk. However, it is difficult to foresee whether or not the level of operational risk would be significantly affected by the development of mobile wallets. Underlying management processes for the delivery of payments through mobile technologies (whether using NFC or not) could be root causes of a potential increase in operational risk.

An institution could resort to outsourcing to offer a mobile wallet service, in which case it could be forced to use a number of third parties because it lacks internal expertise or is under competitive pressure. The management of possibly complex legal and regulatory aspects of outsourcing could

[46] Card secure elements can be stored in the mobile device, hardware or software secure solutions, as well as in the issuer systems, using payment network functions for tokenisation.

have an impact on legal and ICT-outsourcing risks, also taking into account the data protection aspects of outsourcing or processing mobile payments.

In the scenario where the third-party provider manages the customer relationship and the customer data directly, business risk could be adversely affected by a possibly weaker, less stable customer relationship with the institution. In addition, in such a case the customer activity-flow could be less visible to the institution, while this could provide the opportunity for the third party to tailor and enhance its offers to customers.

A fragmented and complex operating environment for payments could increase the ICT security risk to institutions, including cyber-risk, which could be increased if institutions' internal control systems do not reflect the business model changes, operating environment and security threats. Security incidents could possibly increase as a result of the multitude of available solutions for mobile payments and the strong focus on customer convenience.

The proliferation of viruses and malware affecting mobile devices and the danger of lost or stolen devices could increase the risk of unauthorised payments through mobile wallets, raising once again the primary importance of security concerns.

Moreover, the proliferation of mobile devices in a market dominated by a limited number of operating systems that support NFC services could further increase the dependency and concentration on mobile phone manufacturers and mobile OS developers (please refer to the FSB case study on retail payments and digital wallets[47]).

4.6.4 Opportunities

Mobile wallets with the use of NFC appear to have the potential to deliver significant benefits to both institutions and customers, widening access to financial services. They could provide enhanced customer experience, as customers could better manage and monitor their funds through these technologies, which promise faster service, greater choice and keener pricing. Mobile wallets could possibly enable institutions and merchants to use data-driven customer engagement platforms.

Depending on the implementation choices, it may be possible for mobile wallets to provide enhanced security to protect personal and payment data through the application of encryption and strong customer authentication.

The use of mobile wallets could be possibly considered as another common payment method that institutions could offer in an effort to retain their customers, and it could also provide an additional customer touchpoint to expand market and cross-sell services. The potential elimination of the need to carry physical cards, easy payment on the internet and the availability of solutions

[47] FSB, Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention (27 June 2017): http://www.fsb.org/wp-content/uploads/R270617.pdf

supporting payment decision could enable the proliferation of niches and merchant-issued cards or e-money services, allowing mobile wallets to host many payment instruments. Therefore, product value could possibly be enhanced by integrating other services in the mobile wallet (e.g. loyalty cards, coupons, public transport payments).

Mobile wallets could possibly result in reduced transaction costs in the financial system, while NFC mobile payments may increase efficiencies by allowing merchants or customers to rely on a simple payment rather than providing full card details. In general, the development and use of mobile wallets appear to provide institutions with the possibility to offer a better user experience, focused on customer needs and enriched with contactless communication.

4.7 Use case 7: Outsourcing core banking/payment system to the public cloud

4.7.1 Introduction

Current landscape

Over the last few years, the benefits offered through the use of cloud computing have attracted the interest of the financial services industry, with the adoption of cloud computing growing at a fast pace. Many business functions across financial services are moving to the cloud with the aim of leveraging greater scale, cost-effectiveness, more efficient use of IT resources and standardisation enabled through cloud.

The USA's National Institute of Standards and Technology[48] has defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A number of institutions have already been using cloud computing for non-core activities, such as customer relationship management, while some other smaller institutions are exploring the possibility of transferring entire core services to the cloud.

It is important to note that, for any use of core banking services in the public cloud, an institution is not relieved from its responsibilities with respect to confidentiality, integrity and availability of data. These requirements are expected to be ensured through proper contracts, monitoring and auditing as prescribed in the EBA Recommendations on outsourcing to cloud service providers[49].

The public cloud is one of the deployment models of the cloud; in it, essentially, the cloud infrastructure is available for open use by the public. It is the practice of using a network of remote servers hosted on the internet to run applications and manage data. With a pricing model of 'pay-per-use' and the ability to scale computing resources up or down as needed, such services are making it appealing for institutions to host and run their applications in the cloud instead of hosting and running them in their own data centres.

Another deployment model of the cloud is the private cloud, where the cloud infrastructure is made available for the exclusive use of a single institution. There are two types of private cloud, the first one operated by the institution itself, and the second one where the private cloud is operated by a

[48] Mell, P. and T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg, MD, 2011: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[49] Available at: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

cloud service provider (CSP). Using the first type, institutions run the operation in-house on their own hosting infrastructure, with staff managing and running the infrastructure, while in the second case the CSP provides all the technical infrastructure, including running the infrastructure, and the institutions manage and monitor the CSP's operations. In the second outsourcing setup, the technical infrastructure of the systems is dedicated only to one institution albeit some areas are still shared, such as the data centres and networks.

When it comes to public cloud computing options, a diverse market of CSPs exists with a wide range of different offerings. In general, the CSP controls or owns the network that connects the data centres and regions. All regions are connected together and can be used as alternatives to the region set as primary by the institution. This setup is said to provide a fault-tolerant[50] solution.

A number of CSPs across Europe offer public cloud services. The CSPs are often country specific, with the technical infrastructure often set up on two or three data centres from which the services run. In this setup, used in several European countries, one CSP provides core banking/payment/e-money services to more than one institution, using the same core system and storing the different institutions' data in the same technical infrastructure.

Underlying technologies

Cloud computing provides internet-based shared or dedicated processing resources and data storage on demand. One of the components of the cloud model is its service model[51]. At this point, the following are offered:

a) **Infrastructure as a service (IaaS):**

The capability provided to the consumer is to use processing, storage, networks and other fundamental computing resources on which the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

Currently, this appears to be the most basic cloud-service model, and the cost of this service reflects the amount of resources allocated and consumed.

b) **Platform as a service (PaaS)**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and

[50] Fault tolerant is defined as 'Of a system, having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault' (https://csrc.nist.gov/Glossary/?term=4318).
[51] Mell, P. and T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg, MD, 2011: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

tools supported by the provider[52]. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems and storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

This service can be usually delivered as a public cloud service from a cloud provider or as software deployed on public infrastructure as a service.

c) **Software as a service (SaaS)**

The capability provided to the consumer is to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems and storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

This is sometimes referred to as 'on-demand software'. It has become a common delivery model for many business applications such as office software and payroll-processing software.

For applications for which security is of prime concern, a private cloud could be considered preferable, as it allows the most flexibility in data processing and security. On the other hand, private clouds are typically less scalable and more expensive than public clouds. As a result, some institutions may prefer a hybrid model, where some activities could be performed in the public cloud while more sensitive activities (including hosting of sensitive data) could be performed in a private cloud.

The basis for the majority of high-performing clouds is virtualised infrastructure. Virtualisation has been in data centres for several years as a successful IT strategy for consolidating infrastructure and servers. Virtualisation in the cloud environment is often divided into the following categories: hardware virtualisation, operating system virtualisation, server virtualisation and storage virtualisation. Virtualisation software allows one physical server to run several individual computing environments. In practice, there are multiple virtual servers for each physical server. This can allow the separation of processing power, storage and memory among environments, independently from the physical installations of the hardware.

4.7.2 Use case

In the area of banking, payments and e-money, where more standardised services are offered across each sector, with diverse technical resource requirements, the use of a standardised core system in the public cloud is seemingly becoming increasingly attractive for institutions. As a

[52] This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources.

number of financial services are moving towards greater standardisation across the industry (and are becoming less of a differentiating factor between different institutions), institutions regard developing and maintaining their own core applications as inefficient. Cloud providers of core banking, payment and e-money solutions are now offering their solutions to be run from the public cloud and some institutions appear to already be exploring leveraging this opportunity.

In this use case, we will focus on such a scenario where a core system is running on a public cloud. In banking, a core banking system is defined as 'a back-end system that processes daily banking transactions and posts updates to accounts and other financial records'[53]. Core banking systems typically include deposit, loan and credit-processing capabilities, with interfaces to general ledger systems and reporting tools.

Technical implementation in this case can be challenging, taking into account the importance of such a move to the public cloud as well as the underlying security requirements. Retail banking/payment at its core deals with customer data, for which there are strict data protection requirements to be taken into account (e.g. the GDPR). Furthermore, the use of public cloud core banking/payment would need to be integrated with the institution's specific systems and services, which typically run not in a public cloud but rather in a private cloud within the institution.

Another challenge in using the public cloud for core banking/payment lies in its migration. New entrants may choose to start providing their services directly through the cloud. In the case of an existing institution, a potential move to the cloud will involve a technical migration of its offered services into the cloud. This involves the translation of databases into the core banking/payment provider's format and copying them into the cloud as well as significant modifications to a variety of business applications that remain in the institution's data centres.

The role of IT staff in institutions could possibly undergo a significant transformation in this case, with increased cloud outsourcing services, and could possibly convert into support and consultation for cloud service selection, engagement and management.

4.7.3 Prudential risks

Regardless of whether a local or a global CSP is contracted, an increase in ICT outsourcing risk could be expected for a number of potential reasons such as governance, compliance, adequacy of resources, business continuity plan, information security including cyber-security, access management, data management and contract management.

When an institution starts to offer services processed in the public cloud, the implementation of information security management (including access management), encryption key control, encryption, authentication (including multi-factor), cyber-security and configuration of technical infrastructure are of vital importance. The institution will always remain responsible for its

[53] https://www.gartner.com/it-glossary/core-banking-systems

operations, regardless of the use of outsourcing. Operational risk could be high if the institution trusts and relies solely on the CSP to implement all the right security controls.

A possible area that could affect legal and compliance risk as well as the wider operational risk profile is the final contract to be discussed and agreed between an institution and a CSP, which should comply with the relevant regulatory requirements (e.g. EBA Recommendations on outsourcing to cloud service providers). An adequate and appropriate contract management process would be important to address possibly challenging areas such as the right to audit, for both the institution and the supervisory authority.

At the global level, risk of concentration on a limited number of CSPs could be elevated if a significant number of institutions use the same CSP's infrastructure. Nevertheless, this scenario could also raise macroprudential implications that should not be evaluated only at country level (e.g. cross-jurisdictional interest).

In an outsourcing environment, such as the provision of public cloud services by a global CSP, the issue of transparency on chain outsourcing is another area to be taken into consideration. For example, the use of subcontractors from a high-risk area/country could negatively affect the wider operational risk and reputation risk of the institution. Moreover, the institution's competence in sufficiently controlling the technological infrastructure used by a CSP could affect the ICT outsourcing risk of the institution. Therefore, the necessary skills and resources to adequately monitor these outsourced activities would become even more important.

Another possible risk that could arise through the use of core banking/payment systems in the public cloud is vendor lock-in, whereby institutions, be they incumbents or new entrants, may find it difficult to exit and migrate to a new CSP or re-initialise a service. In addition, potential concerns about moving to alternative CSPs (e.g. possible substandard performance or interruption of supplier service) may deter institutions from adequately addressing this risk. In line with the EBA Recommendations on outsourcing to CSPs, appropriate contingency plans and exit strategies are important to increasing trust and resilience, and therefore to the adoption of cloud outsourcing.

Another possible risk could arise from users' lack of trust in data security and privacy, loss of governance, and uncertainty regarding a CSP's compliance with data security regulations. Trust is important for institutions, and a possible reason for being cautious towards cloud computing, as concerns could arise when sensitive data and critical applications move to a cloud computing setup where CSPs may not be able to guarantee the effectiveness of security and privacy controls, because services are delivered from multiple jurisdictions or there may be uncertainty over the jurisdiction where the data is held, given that many large CSPs operate in multiple jurisdictions with potentially fungible data centres.

Moreover, the pricing of CSP services could have implications for institutions' business risk where sufficient knowledge is important to determine the complete cost of the service. The maintenance

and follow-up of such an outsourced service could also affect the pricing, along with the institutions' internal costs around the area of governance, compliance and information security.

4.7.4 Opportunities

Small and new institutions appear to be attracted by the potential benefits of cloud services for core and non-core functions. The potential economies of scale, which may result in lower costs, and CSPs' optimised IT operations appear to attract institutions' interest along with the potential opportunity to avoid capital costs and incur predictable expenses, which scale up and down according to the business needs.

The institutions with occasional usage could possibly be more keen on such potential benefits, as they pay for resources only when they are using them. Institutions with more stable usage patterns could potentially benefit from the possibly lower cost of outsourcing services than in-house development.

The potentially lower cost of using cloud computing appears to be a key driver of its wide acceptance by institutions, probably because the traditional IT model requires institutions to make a front-loaded investment in software and hardware as well as a life-cycle investment in professional staff to maintain servers and upgrade software. IT services in the cloud appear to promise a shift of these expenses to a pay-as-you-go model and therefore offer potential cost advantages. In addition, outsourcing to a CSP might lead to a higher overall quality of the cloud, compared with the quality level of institutions that have their own cloud.

The cloud computing approach could potentially speed up deployment while maintaining flexibility. This capability may mean that, as demand changes, it will not require adjustments in infrastructures to accommodate the changes.

5. Conclusions

5.1 Outcomes

At this stage, a few financial technologies appear to be widely spread across the financial services sector, while interest, in terms of number of initiatives and amount of investments, is growing rapidly. In general, **no significant implementation of sophisticated technologies** as such was noted, possibly because institutions are very cautious and do not seem to trust such technologies, probably owing to security concerns. Regulatory and supervisory uncertainties around emerging technologies also appear to play a key role in the progression, application and implementation of such technologies. This could also be a result of institutions filtering the marketing and hype around FinTech.

The use of biometrics for identification and authentication purposes and the launch of mobile wallets with the use of NFC technology seem to be some of the FinTech applications already implemented by institutions. This is probably because of their non-complex setup and the immediate improved customer experience driven by the competitive pressure. Both FinTech applications require the use of mobile devices, which is essentially out of the control of the institutions, and **create dependencies on third-party providers** such as device manufacturers and operating system developers.

A growing shift towards operational risk has been witnessed in the last few years following the overall increase in change. Operational risk is becoming important in all change processes. This starting phase of FinTech could contribute to increased operational risk, especially when a new technology is developed and used for the first time in the market and also when a technology is used by another institution whose staff are at the beginning of the learning curve. The lack of technical skills, shortage of expert staff and the inadequacy of technology infrastructures could be possible reasons contributing to this potential shift in operational risk.

The uncertainty about the scale of adoption and extent of issues that can go in the wrong direction could negatively affect conduct risk along with **accentuation of ICT risks** as institutions move towards more technology-based solutions. In particular, this could bring about increased ICT security risk (cyber-security issues and digital fraud issues) and amplified ICT outsourcing risk while at the same time legal and compliance risks as well as reputation risk, stemming for example from the risk of mismanagement of personal data or lack of data privacy, could also be affected.

While the engagement with FinTech may come with potential risks, which should be thoroughly and comprehensively assessed and managed, **a number of prospective opportunities could materialise in return**. This prospect is essentially the key driver of the active interest observed

around FinTech. The potential efficiency gains and the improved customer experience, both connected with the wider competitive pressure within the financial services sector, appear to be the predominant key drivers when it comes to potential opportunities. In addition, **changing customer behaviour is a key factor** triggering institutions' interest in FinTech.

As this analysis does not necessarily encompass every possible outcome stemming from the application of each technology, both competent authorities and institutions should note that the **actual impact on the risk profile of institutions would significantly depend on the type of underlying technology and its implementation as well as the processes and business models adopted around them.** Furthermore, the risk assessment would partially depend on the context of each specific institution. The different levels of FinTech activity and engagement observed across the EU should be taken into account when considering this report.

While **this report has focused on the microprudential risks** that may arise from each use case, consumer protection and macroprudential aspects could also arise and should be identified separately and appropriately.

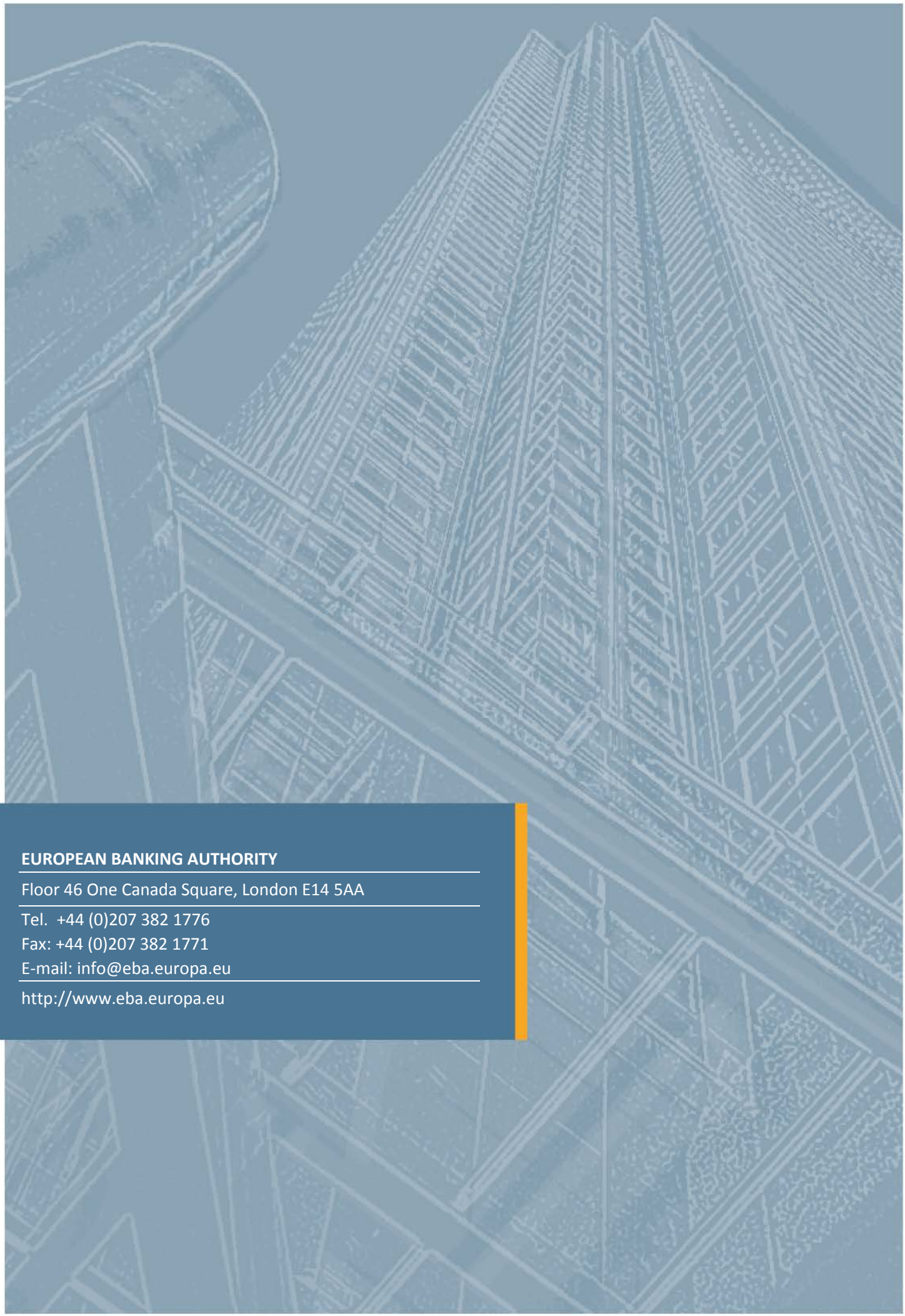
In conclusion, this report aims to **support sharing of supervisory knowledge and experience** in assessing, and responding to, new technologies. Such sharing is critical in promoting technological neutrality. In addition, **the use of technologies could bring new opportunities to institutions**, which could potentially outweigh the risks, provided that it is accompanied by the establishment of effective governance structures as well as appropriate implementation and risk management processes.

5.2 Next steps

In line with the EBA FinTech Roadmap, the EBA will continue to monitor FinTech developments and, as appropriate, carry out additional tasks with a view to policing effectively the regulatory perimeter and fostering neutrality in regulatory and supervisory approaches to new technologies.

In the meantime, it should be noted that, while this report focuses on the potential prudential risks and opportunities that may arise from the selected use cases, the analysis may be applicable to other business cases and financial processes, procedures or services where the same underlying technologies are used.

Moreover, both the supervisors and the institutions should carefully assess the potential impact of the aforementioned use cases on risk profiles and appropriately balance the prospective benefits.



EUROPEAN BANKING AUTHORITY

Floor 46 One Canada Square, London E14 5AA

Tel. +44 (0)207 382 1776
Fax: +44 (0)207 382 1771
E-mail: info@eba.europa.eu

http://www.eba.europa.eu