Efma

REPORT

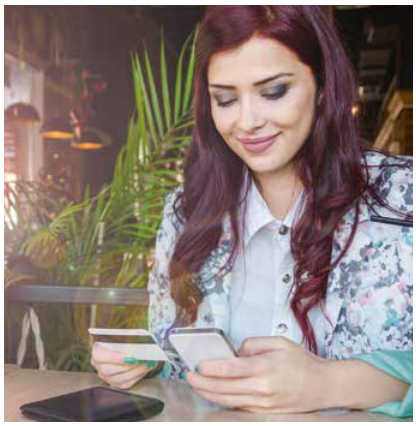
# Building the future of mobile banking

## Part III: Security and regulatory issues

In collaboration with:

WAVESTONE

CONTENTS



# Introduction

For several years now, the growing use of mobile devices to surf the web and make online payments has caused a steady rise in the number of targeted attacks. Every year, fraud-related incidents are generating increasingly heavy costs for banking establishments and the techniques employed are becoming more sophisticated.

In addition, while users are becoming more vigilant when carrying out digital operations, they seek reassurance when it comes to their personal data. According to a recent report published by HSBC[1], key consumer concerns include 'personal data leaks' (56% of respondents), 'bank account hacking' (55%) and 'bank card cloning' (54%). Furthermore, 87% of respondents consider the security of their personal data as important as the security of their money.

In a bid to contain these trends, legislation has been tightened in recent years and is posing several major operational challenges. Rather than being a constraint, these new regulatory requirements offer mobile banks the opportunity to optimise customer knowledge, personalise customer experience and services, reinforce operational security and, as such, boost trust in mobile banking services.

In addition to respecting regulatory requirements, mobile banks must obviously provide the necessary guarantees to win and retain client trust in digital services: ensuring authentication and personal-data confidentiality and implementing measures to combat fraud.

This level of security must be maintained at all times, notably for:

- Customer onboarding, in order to validate their identity
- Accessing banking services even if not authenticated
- Payments services, to identify and block any doubtful transactions.

In this, the third and final part of our *Building the future of mobile banking* study, realised in collaboration with Efma, we take another look at these key moments of exchange between the bank and its clients from the point of view of introducing the security and compliance principles to be implemented.

Our report, which covers the individual and professional markets worldwide, is based on numerous inputs such as our security and compliance materials, our digital banking services benchmark, our digital banks and fintech observatory, our benchmark of process performance within the retail banking industry, banking case studies and a selection of interviews. These resources are shared throughout the report, alongside analysis of more than 30 digital banks, including new challenger banks, digital banks, traditional banks, and approximately 180 fintechs.

This will be followed in due course by a global report that summarises all our findings into the future of mobile banking by looking at the pillars that address the bank's key areas of operation:

- Part I: Customer targets, acquisition strategy and customer experience
- Part II: Organisation and processes
- Part III: Security and regulatory issues.

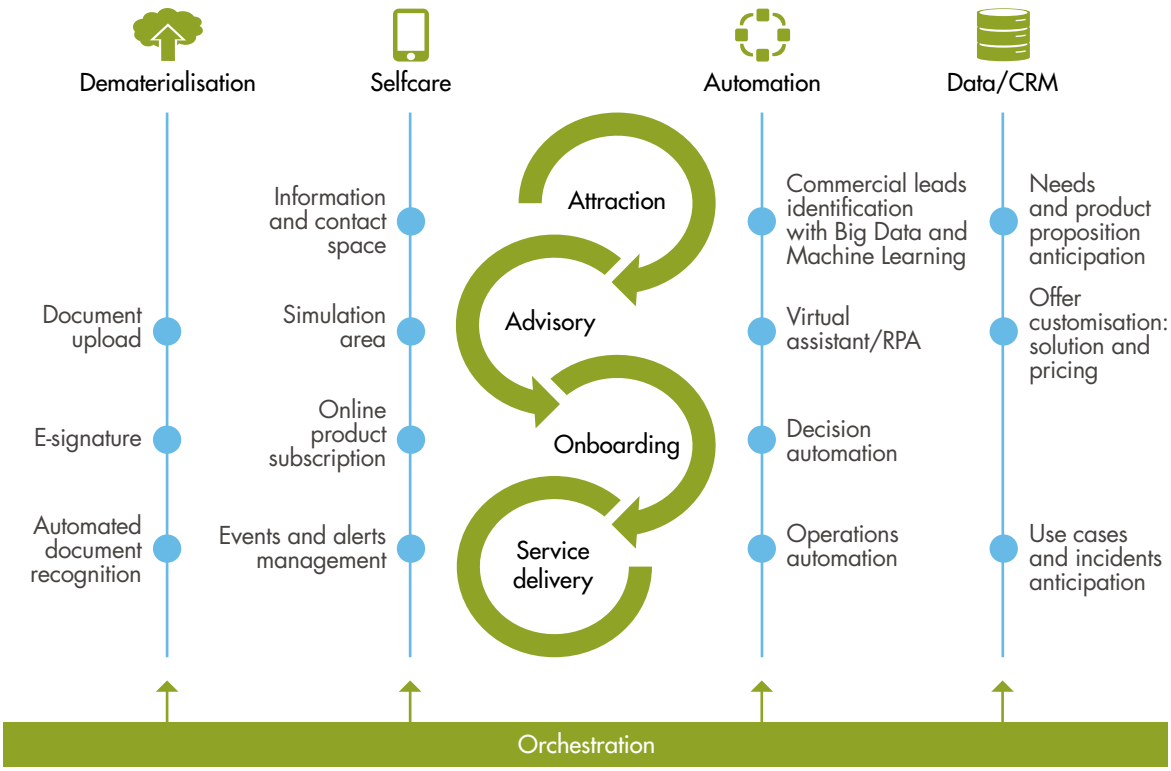
[1] HSBC, Trust in Technology, November 2017: https://iatranshumanisme.com/wp-content/uploads/2017/06/170524-hsbc-trust-in-technology.pdf

# Onboarding as the cornerstone of mobile compliance

Onboarding, designed with a view to winning new clients, is decisive in fostering lasting and profitable customer relationships in the banking sector. For mobile banks, this is the first stage in the customer journey which determines whether or not they will be able to achieve their ambitious customer acquisition objectives, which systematically target portfolios of over one million clients.

As such, this is a key moment which enables banks to establish contact with clients, determine their identity accurately (and by doing so respect legislation in force) and identify those who could be at risk. This traditionally long and complex process must now be fully digitalised to enhance fluidity and appeal.

Figure 1: Onboarding end-to-end digitalisation around four pillars: dematerialisation, selfcare, automation and client-data value extraction



## Validate the identity of future mobile bank customers

The identification and verification processes enable banks to forge customer relationships on the basis of correct information and constitute the bedrock of security. The revision of the fourth European Union Anti-Money Laundering (AML) directive stipulates that the means used to identify clients electronically must be equivalent to those used in a one-on-one context, in accordance with European eIDAS[2] legislation requiring the digital read-out of passport and ID card data.

For example, N26, a German mobile bank which operates in all countries throughout the Eurozone, has developed a 100% mobile account-opening process that can be completed in eight minutes.

After completing the first automatic email address verification stage and inputting the standard subscription information (surname, first name, address, password, etc.), new clients are required to make a video call to a bank agent. During this conversation they will be asked to answer several questions and present the two forms of ID needed to open an account in an online bank.

This video authentication stage is ensured by IDNow, which partners with several European banks and whose Automatic Identification and Data Capture (AIDC) technologies notably make it possible to:

- Identify the type of ID document presented (ID card, passport, etc.) by comparing it with a set of models
- Verify document integrity: validation of image quality, verification of control keys and the Machine-Readable Zone (MRZ)[3]
- Extract data: once extracted by means of Optical Character Recognition (OCR)[4], data is compared to the information entered by the user.

AIDC technologies can also be used in conjunction with a document uploading module to automate the verification of all types of document (pay slips, income tax returns, proof of address, etc.). This stage is also proposed by companies such as ResoCom[5] in France, which delivers a certificate of compliance upon document verification and, in the event of any anomaly, contacts the administrative body that issued the document in question.

Furthermore, in the not too distant future it may be possible to delegate prospective-client identification to an entrusted third party such as the State. In 2002, Estonia[6] implemented, and has since been developing, a digital identity system for its citizens which can be accessed by private companies via an Application Programming Interface (API). Similarly, in France, FranceConnect is a service that enables all administrative authorities and certain private players that contribute to public action to validate an individual's identity by giving them access to data of trusted third-party bodies such as the French Tax Authority or French Health Insurance. In India, Digibank, a 100% mobile bank launched in 2016 by DBS, offers a 90-second account-opening service based on the state biometric authentication repository.

---

[2] eIDAS: Electronic Identification and Trust Services – an EU ruling implemented in 2014 to harmonise the minimum standards to ensure trust and digital identification, such as the electronic signature.

[3] The MRZ is a zone reserved for document identification and validation purposes that can be read automatically.

[4] OCR covers IT processes that make it possible to transform images and printed text into digital text files.

[5] http://www.resocom.com/solutions/

[6] http://www.gemalto.com/france/gouv/inspiration/digital-estonia

## Digitalise scoring and respect the MiFID 2 directive

Scoring, or profiling, consists of rating clients according to the degree of risk they present for the bank (solvency, criminality, etc.).

Scoring is based on controlling the relevance of data communicated according to external information sources, such as:

- Central banks' files (such as FCC, FICP and FNCI[7] in France)
- Local authorities' lists
- In-house and inter-bank lists
- Politically Exposed Person (PEP)[8] lists
- Declarative information (employment, revenues, assets, etc.)
- Smartphone data (geo-localisation, data entry time, etc.).

Scoring should not be used too early in the subscription process to avoid making excessive demands that could discourage potential clients. If there is any suspicion of terrorist financing, the operation may be blocked before the process has run its course. However, in other cases, such as for people whose bank account has been suspended or who are politically exposed, it is advisable to wait until the process has been completed. The mobile bank even offers consumers the possibility of opening an account with a very low payment ceiling pending the last level of control, such as proof of residence.

The scoring process must also satisfy MiFID 2 directive requirements stipulating that financial product distributors ensure their products meet customers' loss-bearing capacity and risk tolerance as well as investment needs and objectives.

Given the absence of direct one-on-one contact, the mobile bank has to use an interactive questionnaire which, together with situation simulations and practical questions, is designed to develop customised offers that best suit the client's profile. Information obtained can serve to enrich the client profile for the purposes of identifying future commercial leads or detecting account functioning anomalies. The gathering of this information offers a marketing advantage if the questions asked are meaningful for the client, or express his/her needs and expectations with regard to the service in question. This process can also be designed in an instructive and amusing way to reassure clients that their remote relationship can be as personalised as the one they would have in direct one-on-one contact with a bank manager.

To validate client identity and digitalise scoring, the process must interface with complex internal and external systems traditionally used by branch counsellors. To this end, mobile banks use APIs which separate front-office procedures from the complexity of the underlying business while maintaining the ability to calculate the level of risk in real time, for example.

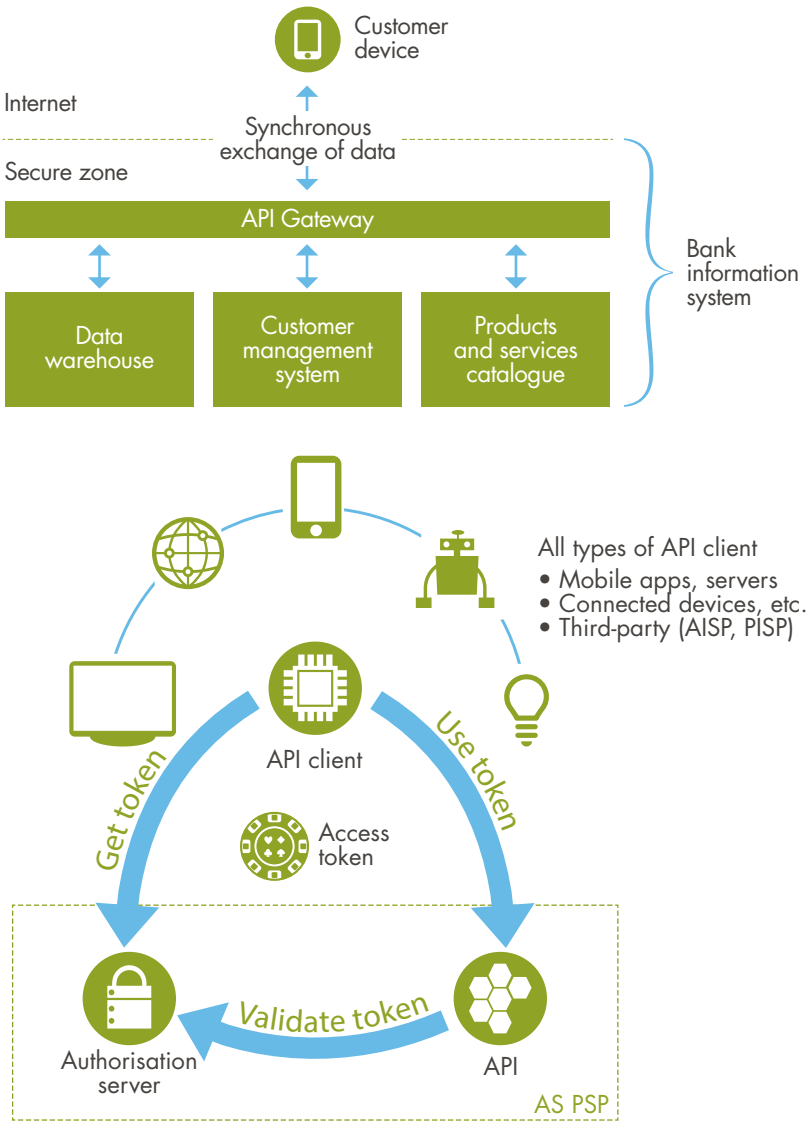
[7] Files issued by the FCC and FNCI identify bank clients with ongoing incidents involving payments by check, while those of the FICP concern individual indebtedness or default on credit repayment. Listing in any of these files implies a five-year interdiction from the services in question. https://particuliers.banque-france.fr/fichiers-dincidents/les-trois-fichiers-dincidents-fcc-ficp-fnci

[8] Politically Exposed Persons are individuals who, because they hold or have held high-level public offices, are under heavy surveillance to prevent corruption and money laundering.

## Application Programming Interfaces (APIs)

APIs enable the sharing of services with other applications. API developers determine the mandatory information required for user registration so they can exploit the data and the results obtained. FranceConnect's API, for example, gives access to personal data such as surname, first name, date of birth, gender, place and country of birth, once the user's login and password have been verified by FranceConnect (Pivot ID).Recognised, mature technical standards include HTTP, REST, JSON, OAuth and OpenID Connect.

Figure 2: Simplified IS map and API security fundamentals



## Respect customers' rights and protect their data to reinforce trust

During the onboarding process, numerous personal data are collected (surname, first name, date of birth, etc.). According to a worldwide report published by ING[9], the subsequent processing of these data is key to establishing relationships of trust and ensuring client satisfaction.

This report highlights the fact that customers have greater confidence in the security of mobile banking services once they have used them (46% answered 'very secure' or 'somewhat secure') compared to non-mobile users (35% answered 'very risky' or 'somewhat risky'[10]).

In addition, asking for consumer consent during data collection significantly enhances client trust. Indeed, the European Union's General Data Protection Regulation (GDPR) requires firms to obtain the explicit and informed consent of their clients to process their personal data. Clients must be able to understand, in plain language, what elements of their personal data are being processed and to what end (service security, risk management, marketing proposals, etc.). The inclusion of any form of inferred consent, such as pre-ticked boxes, is now prohibited.

GDPR also provides a governing framework for the numerous automated algorithm-based decisions made during onboarding. The client may contest certain automated decisions, which means the bank must be able to retrace and therefore justify every decision it makes. Furthermore, GDPR stipulates that all personal data be associated to a specific client, and recommends data encryption to limit the consequences of any possible leaks.

Data-management transparency is a differentiating factor to reinforce customers' trust. Banks are the best placed actors to win this trust: at European level, 56%[11] of banking customers do not use the mobile channel because of security concerns. However, banks are preferred by 60%[12] of consumers to subscribe to financial products, before other actors like telecom operators or start-ups. Consequently, banks need to concentrate their efforts in reassuring customers in the transition to a fully secure mobile interaction.

### GDPR

GDPR will become the first unified data protection regime for all 27 EU Member States, binding for both EU and non-EU companies that operate in the EU.

GDPR requires companies to develop a tailored strategy for consumer data protection within the organisation. Violations could result in fines of up to 4% of annual turnover or €20 million.

Firms will now need to collect explicit consent for each specific purpose of data processing, and customers must be immediately informed of any data breach potentially concerning them. They also have the right to contest automatic decisions and can demand that their data be deleted or transmitted to a third company (i.e. when changing mobile phone operator).

Regulators have already announced that assessing banks' compliance with these new standards is their priority.

[9] ING International Survey, *Mobile banking – the next generation*, May 2017 https://www.ezonomics.com/ing_international_surveys/mobile-banking-2017-newer-technologies/

[10] Percentages indicate the differential between answers by mobile bank users and non-users when asked about mobile banking security perception.

[11] ING International Survey, *Mobile banking – the next generation*, May 2017 https://www.ezonomics.com/ing_international_surveys/mobile-banking-2017-newer-technologies/

[12] Ibid.

# End-to-end digitalisation of banking relations to secure access at every connection

## Adapt security measures to smartphones

In order to secure access to mobile banking services, additional measures must be deployed. Indeed, smartphones are a preferred target for hackers since their use is quickly spreading, representing as many gateways to the bank's information system. Nevertheless, the most common typologies of identity fraud have not drastically changed in recent years:

- Malware installation on customers' smartphones to capture user identification and passwords
- Phishing[13] to steal authentication data, by usurping a financial institution's identity with a fraudulent email that asks customers to provide their authentication keys
- User identification and password interception in an unsecured connection, for example when using a public WiFi network.

Mobile banks can build a first line of defence against the most common threats along three simultaneous dimensions, which are discussed below:

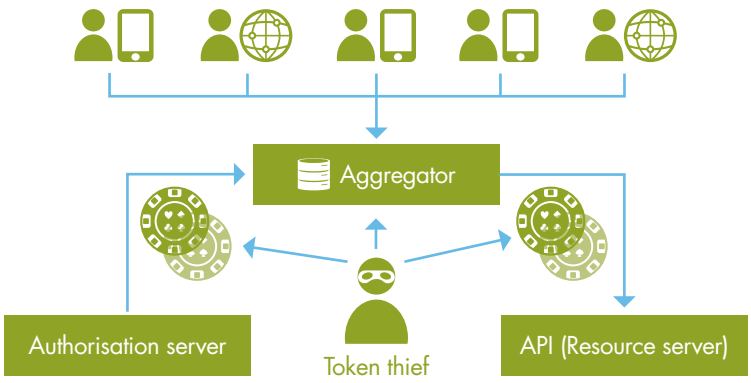
- Secure mobile banking applications to avoid identity fraud through security breaches
- Raise awareness among clients concerning phishing risks. In particular, banks should advise customers on how to identify a phishing campaign and how to alert about fake emails to enable immediate reaction and limit the number of impacted clients
- Increase the required authentication level to perform a payment, in order to avoid fraudulent access to client accounts.

### First dimension: Implement a token binding solution to avoid client token theft

Generally, when authentication tokens expire after a fixed time limit, they become useless and the impacts of token theft are limited. However, in the current context where the second Payment Services Directive (PSD2) requires banks to open their services via APIs, third parties such as account aggregators or payment initiators may possess a large number of tokens. Given that the third party may be a start-up, more focused on innovation than on security, the bank must anticipate a compromise of the third-party's security.

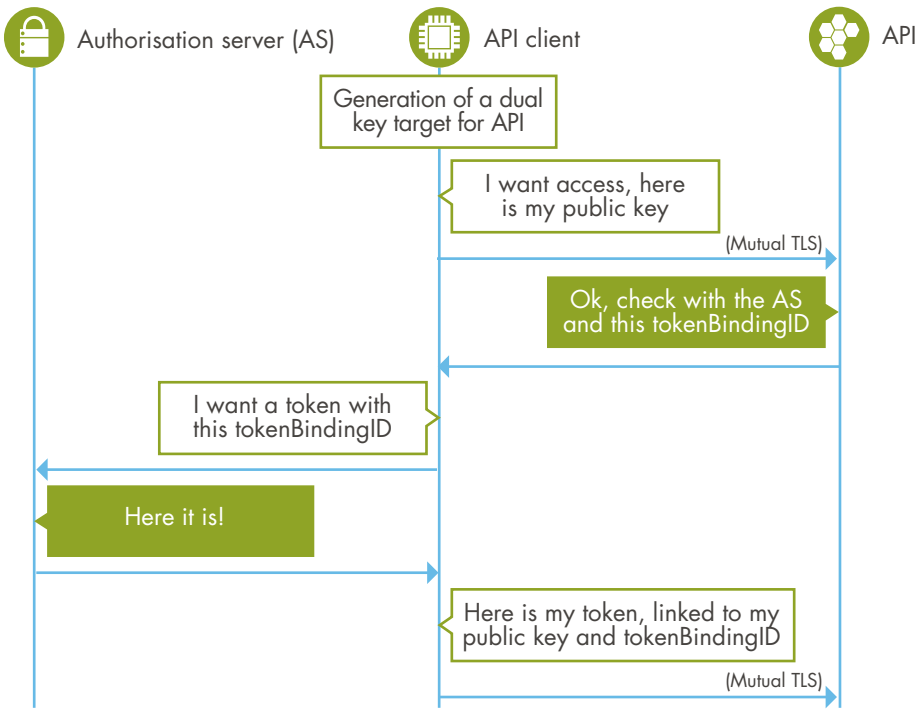
[13] Phishing is a technique for stealing authentication data that consists of the usurpation of identity of a trusted third party, e.g. a financial institution.

Figure 3: Location of token theft risks




The technique of token binding addresses this need for enhanced security by linking a token or a cookie to a cryptographic key. The third party must prove that it possesses the corresponding private key by establishing a mutual Transport Layer Security (TLS) secured connection, in order for the token to be usable. In the event of a token being intercepted by an intruding third party who does not possess the cryptographic key, the token is refused by the bank's API server.

Figure 4: Illustration of flows in the token binding solution



## Second dimension: Raise awareness among customers concerning phishing risks

In order to alert customers about the risks of having their connection IDs and passwords stolen, it is highly recommended to send out regularly – e.g. once a year – an official communication to remind users about security best practices. In addition, the bank should display security advice in a prominent space on its website or mobile application. This will increase clients' maturity and awareness and will help in reducing the risks and impacts of future frauds.

Moreover, an online contact space should be operated, where customers can alert about potential frauds or phishing campaigns. If the attack is confirmed, a special communication could be sent out to the targeted customer group during a certain period of time to avoid contagion.

### Best practices to build customer awareness

**Protect your mobile device**
Customers must be aware that it is essential to regularly update their mobile device as the updates include security patches that correct recently-discovered weaknesses. Using an obsolete version of an operating system enables hackers to take advantage of known security breaches and to obtain fraudulent access to customers' accounts.

**Use a secure connection**
The choice of a private and secure connection is paramount, since many public WiFi networks have not deployed essential security measures. Any transferred data is accessible via the network and an intruder can easily intercept data packages in transit and obtain non-encrypted client IDs and passwords. This scenario is known as 'man in the middle.'

**Identify and detect fraudulent emails**
Customers must be aware that their bank will never request personal and confidential information by email. Before clicking on a hyperlink received by email, they should position their mouse on it to verify that it is the authentic bank website. Generally, customers must pay attention to checking that URLs are secured with an SSL certificate. This is displayed with a small 'lock' symbol on the web browser and a URL starting with 'https://'.

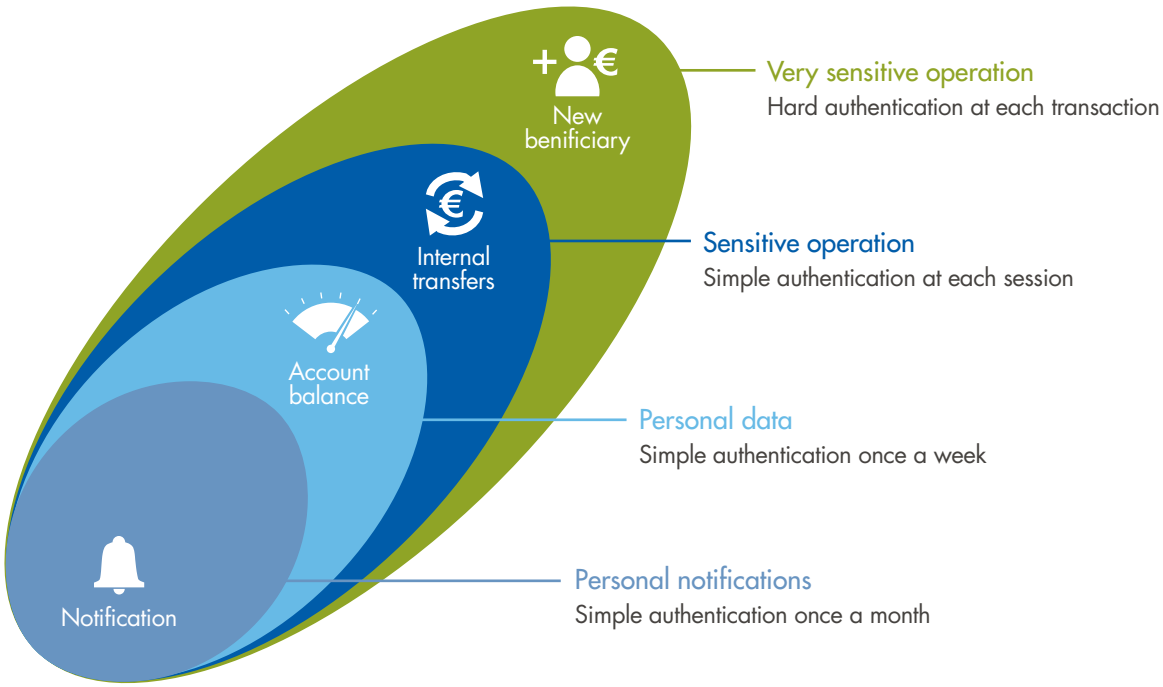
**Use a unique and complex password**
Clients must be especially alerted about the importance of using a different password for the mobile application. It is highly recommended to regularly change this password and to make it sufficiently long, secure and difficult to guess. It should not contain any personal information like the holder's date of birth.

## Third dimension: Adapt the authentication level for sensitive actions to reduce fraudulent access

The level of authentication required for payment services has been historically low in Europe. Indeed, for many years, only the client's login and password were requested to connect to the service and order a payment.

It is essential to increase the authentication level required to access banking services. However, this level should be adapted according to the nature of the service that is being accessed. Other factors such as the operation's features (amount, beneficiary account, etc.) or the user's context and habits are helpful in determining an acceptable authentication level.

Figure 5: Operation types and related authentication levels




Authentication factors can be classified into four different categories:

- 'What I know' – i.e. a password or the answer to a secret question
- 'What I possess' – i.e. a material device such as a magnetic card, USB pen drive, smartphone, chip card or token[14]
- 'What I do' – i.e. the speed of typing on the phone's keyboard or the signature
- 'Who I am' – i.e. a fingerprint, an eye-print or a voiceprint.

To address the contextual need for authentication, it is paramount to distinguish basic from sensitive services or operations. For the most critical operations, a hard authentication will combine at least two independent factors among 'What I know', 'Who I am' and 'What I possess', of which at least one should not be reusable. For less risky services, like checking an account balance without money transfer, authentication may be limited to 'What I know'.

When accessing more risky services, an additional authentication level such as 'What I possess' should be added. The use of physical or behavioural biometrics ('Who I am' and 'What I do') should allow the identification of high-risk access attempts. If there is any doubt about the person's identity, an additional level of authentication must be imposed. Such biometrical authentication methods are currently not robust enough to identify users with a small margin of error.

[14] Single-use password

Practically, if the customer wants to order a payment, and behavioural biometrics confirm that he or she is the right person, it is not necessary to request a second authentication factor to simplify user experience. On the contrary, if the analysis of the person's behaviour does not match their past habits, it cannot be ensured that they are not an intruder. Thus, a second authentication factor must be requested to confirm and verify their identity. Furthermore, other complementary criteria such as the usual location of the connection or the number of failed login attempts may be taken into account.

All these different mechanisms make it possible to ensure a first security level by limiting the risk of intrusion of a fraudulent user into another person's account. However, in certain cases such measures are not sufficient to prevent fraudulent access. Therefore, risky transactions must be detected to enable a real-time reaction on payments to limit impacts of identity fraud.

## Advantages and disadvantages of second-factor authentication

**Software certificates**
Generally used by corporate clients to access online banking portals or to sign operations online, software certificates are not adapted to smartphone or tablet. They provide an insufficient level of security since they do not ensure the identity of the person that commands the operation. Indeed, once enrolled on the device, anyone can use the certificate.

**Material certificates**
Installed into the mobile phone, material certificates serve to access and confirm sensitive operations. However, they may cause friction in the customer experience.

**Physical tokens**
Such authentication factors are frequently used to operate on mobile devices, even if weakly ergonomic. Many banks provide such a solution to millions of customers despite its low ergonomy and high costs for device manufacturing and logistics. The security level depends on the end use of the device.

**Soft tokens**
Soft tokens are a proper alternative to physical tokens, although security is limited if the token is sent to the device where authentication is attempted. Many banks deploy this solution to millions of customers via the mobile banking application, which is much cheaper than physical tokens.

**Soft tokens with out of band (OOB) authentication**
These authentication factors improve the user experience delivered by soft tokens. They manage integrated push notifications, context pages prior to validation and the native integration of this context in generating a one-time password (OTP), without any action needed from the user. They may also be introduced to validate operations initiated on other channels, which reinforces the security level. We thus generally recommend implementing this second factor of authentication.

**Other authentication methods**
Other less mature authentication methods like fingerprints, voice recognition or facial recognition may also be considered. However, the targeted customers are more limited since not all devices are compatible. OTPs sent via SMS are not advised for web and mobile usage due to numerous security breaches.

## Digitalise fraud management to enhance security and reactivity

On the mobile channel, in addition to the identification and authentication of the customer, mobile banks face the challenge of complying with transaction-monitoring regulations. Native mobile banks can capitalise on new technological capacities devoted to client authentication and payment security to build a transaction analysis system. This second level of security of the mobile banking relationship addresses the client's interactions with all the different services offered.

Indeed, mobile banks can leverage their native digital platform to create an autonomous and digitalised anti-fraud policy. Built on behavioural and contextual analytics, this policy can be constantly improved thanks to Machine Learning. Interactions with customers, naturally digital in a mobile bank, are constantly generating useful data that may be employed in client profiling and transaction security. To this purpose, they could exploit not only hard transaction data (amounts, beneficiaries, frequency, etc.) but also metadata associated to each operation (e.g. location of a credit card payment, smartphone location).

This reinforced security policy should, however, be limited to delicate operations so as to guarantee the necessary security level while not being too restrictive or permissive. Finally, it should also fully respect regulatory requirements regarding personal data protection.

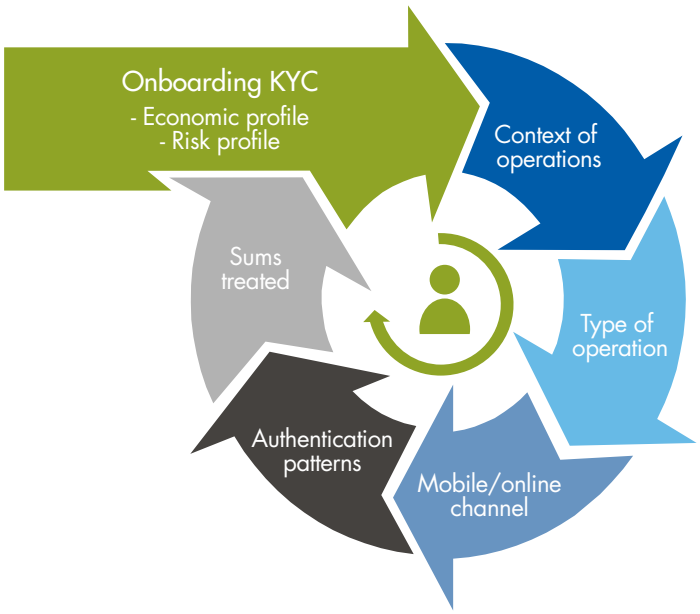
### Use bank-customer interactions to secure operations

Until now, traditional banks have relied on Know Your Customer (KYC) efforts to understand and classify clients' behaviour. This encompasses face-to-face contact, client profiling according to revenues and financial activity, financial needs, and a traditional threshold-based approach to analyse operations on an ex-post basis, mainly by taking into account the amounts of operations.

However, digital banks can constantly gather much richer client data to feed a system for ex-ante or even real-time transaction security. Dynamic and transparent data management enables financial institutions to enhance the knowledge of their customers' habits, needs and service expectations.

Data gathered throughout banking relations opens a new dimension for the analysis of clients' identity. In addition to traditional KYC, representing a rather static picture of the client, a 'digital identity' can dynamically assess client behaviour by analysing transaction data (amount, beneficiary, issuer) and its associated metadata. The level of client knowledge and security is then enhanced through the combination 'who the client is' and 'what the client does.'

Figure 6: Client knowledge evolution via Big Data and Machine Learning analysis




The combination of transaction analysis and instant geolocation ought to be considered as a data treatment in the sense of GDPR. Thus, the client's explicit consent is necessary to deploy this functionality. Mobile banks can leave clients the choice to enable or disable such functions needing personal data processing, as is already the case with various social networks that operate privacy dashboards. This privacy set-up management is fully aligned with the principle of opt-in[15], mandated by GDPR. Indeed, transparency in client data management should be regarded as a lever to reinforce the client's trust in financial institutions as major actors in the new digital environment.

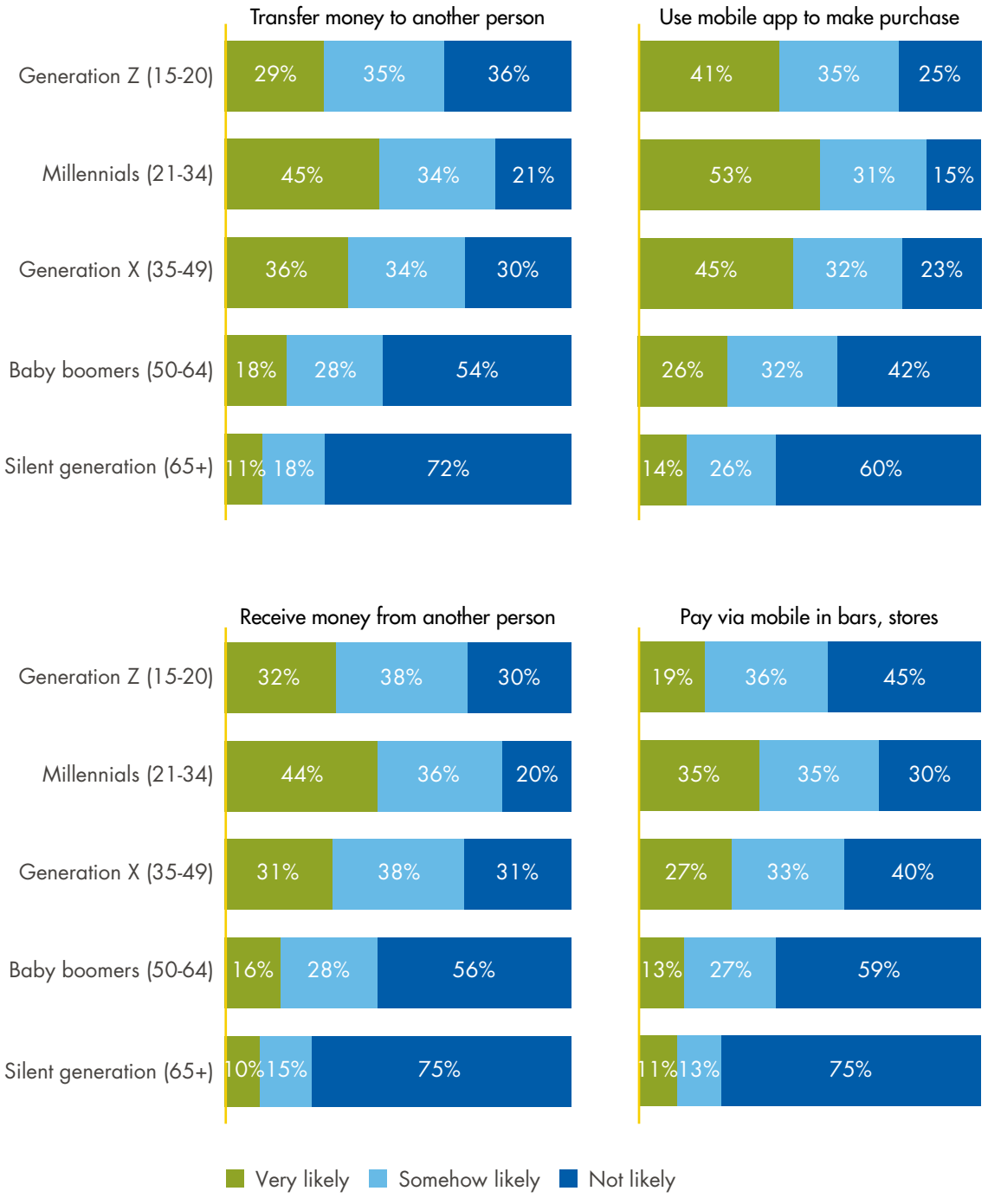
A risk-based process should be conceived to enhance reactivity and user experience of regulatory compliance. This risk-based approach needs a reliable and up-to-date client knowledge, as well as a fair representation of the risk that the client presents for the bank. Only then can the bank apply the most appropriate controls and checks.

Starting at onboarding, a first client data analysis should establish a risk profile and eliminate major risks. The client's risk profile may then be updated thanks to the discipline of Machine Learning, which will take into account any evolutions in the client's behaviour. The analysis of customers' patterns of normal behaviour may take into account their preferred service and transaction types and the size of amounts normally exchanged, among other factors. This process aims at triggering a tailored real-time reaction as soon as an anomaly in customer's behaviour is identified.

[15] The opt-in principle lays down the right for consumers to accept or refuse the precise purpose(s) for which their personal data is processed.

## Figure 7: Usage of four major services per age group

*Answers to: How likely is it for you to [...] within the next six months?*




Source: The Nielson Mobile Shopping, Banking and Payment Survey Q1, 2016

## Modulate security policy depending on the context of each operation

Since consumers spend increasingly more time on internet and mobile every day (A daily average use time across European countries ranging between 4:09h and 3:26h on laptop and desktop, between 2:08h and 1:08h on mobile phone)[16], the smartphone constitutes an immediate reliable channel between the bank and its customers. Mobile banks should capitalise on their efforts to deploy a 100% digital customer experience to enhance their reactivity whenever they have suspicions about a transaction's legitimacy. Additional options for verification can be deployed in real time to the customer's smartphone to clarify any doubt, e.g. security questions, passwords or location.

For instance, MasterCard already operates a security system for credit card payments made abroad. Before authorising a transaction, the customer's smartphone location is used to confirm that he or she is in the country where the payment is ordered. Should this not be the case, an alert is triggered and the payment is not authorised[17].

In addition to identity checks upon client onboarding, banks must also comply with AML and Anti-Terror Financing regulations, by ensuring that clients are not blacklisted in any official sanctions or surveillance lists. This requirement also applies to every single transaction, which must be properly identified with fully transparent information. The purpose is to detect any officially sanctioned counterparties, or any prohibited dealings such as arms exports to countries under embargo, oil exports from sanctioned regions, etc. Real-time filtering systems are capable of ensuring the compliance of such transactions; however, they generate vast amounts of false blocking alerts[18] that need to be handled by a human operator. Should a customer transaction be blocked during this process, the mobile phone could be a reactive method to collect the missing information needed to confirm the transaction's compliance. For example, a client could receive a notification asking him to input his date of birth to dismiss a homonymy with a sanctioned person, to indicate the economic purpose of the transaction, or to provide information on a transaction's counterparty or beneficial owner.

The challenge lies in orchestrating a multi-layer verification system in case any anomaly or behavioural deviation is detected. An interaction with the client should then clarify the doubt via a private question, additional identity check, etc.

The use of biometric data like fingerprints, although supported on numerous modern smartphones, is more sensitive given its unique and inherent character as personal data. The French data privacy regulator (CNIL) advises prudent usage and reinforced security for this type of data, since it may not be replaced in the event of a usurpation.

---

[16] *Digital in 2017: A global overview*, We Are Social , https://wearesocial.com/special-reports/digital-in-2017-global-overview

[17] https://newsroom.mastercard.com/2016/03/15/mobile-opens-new-age-of-innovation-for-payment-card-services/

[18] False alerts may arise for example from homonymies between an officially sanctioned person and the issuer or beneficiary of a transaction.

# Conclusion

To sum up, our report underscores the fact that the issues of cybersecurity and banking compliance are closely related to the security of mobile banking. The steady rise in the number of cyber threats and incidents has led to increasingly onerous costs for companies and prompted the adoption of increasingly stringent regulations[19].

Mobile banking security must be ensured at all levels, namely:

- During onboarding, when the basic minimum requires the formal validation of the future client's identity. Additional verification is needed to fine-tune customer scoring and thus ensure the client presents no significant risk for the bank. This should, however, be carried out in an intelligent manner so as not to lose the future client.
- Every time clients access their banking services: a progressive authentication mechanism should be implemented to match the level of transaction risk. This mechanism may be supplemented with basic techniques such as token binding. Transparent user-ID authentication technologies, such as behavioural biometrics, can also be used to streamline the user experience.
- During sensitive transactions, for which Machine Learning can be used to automatically identify suspicious data flows requiring in-depth verification. The optimisation and automation of these mechanisms considerably reduces the level of fraud criticality.

Security is not, however, the responsibility of the bank alone. Numerous cases of reckless client behaviour can trigger data theft and significant financial losses that the bank has to reimburse. To combat these phenomena, while enhancing brand image and boosting client trust, the bank must communicate with and raise the awareness of consumers. Best practices must be presented in a simple and intuitive manner to prompt a change in behaviour of clients at risk.

While banks are under pressure from PSD2 to open their client database to outside players, digitalisation should not be viewed as the loss of a privileged contact with clients. It should rather be seen as an opportunity for banks to develop their distribution channels and gain access to a larger client base while improving the level of service, security and satisfaction. In the same way, GDPR, which has imposed tighter personal-data processing regulations, offers players the opportunity to personalise bank services and enhance client trust.

[19] http://www.itforbusiness.fr/thematiques/securite/item/9570-les-cyberattaques-coutent-11-7-m-par-entreprise

# About us


A global non-profit organisation, established in 1971 by banks and insurance companies, Efma facilitates networking between decision-makers. It provides quality insights to help banks and insurance companies make the right decisions to foster innovation and drive their transformation. Over 3,300 brands in 130 countries are Efma members.

Headquarters in Paris. Offices in London, Brussels, Barcelona, Stockholm, Bratislava, Dubai, Mumbai and Singapore.

www.efma.com


Wavestone is a consulting firm, created out of the merger of Solucom and Kurt Salmon's European activities (excluding retail and consumer goods consulting outside of France). Wavestone's mission is to enlighten and guide its clients in their most critical decisions, by drawing on its functional, sectoral and technological expertise. With 2,500 employees across four continents, the firm ranks amongst the leading players in European independent consulting, and number one in France.

*Wavestone's key financial-services contacts:*

**Joël Nadjar**, Practice Leader
joel.nadjar@wavestone.com

**Pierre de Brabois**, Partner
pierre.debrabois@wavestone.com

**Pierre-Louis Durel**, Manager
pierre-louis.durel@wavestone.com

**Maxime Meneboo**, Senior Consultant
maxime.meneboo@wavestone.com

**Quentin Pallotta**, Consultant
quentin.pallotta@wavestone.com

For more information: www.wavestone.com

Efma

# Building the future of mobile banking

## Part III: Security and regulatory issues

January 2018

www.efma.com

In collaboration with:

WAVESTONE