Deloitte.

The retail customer digital journey – navigating the regulatory hotspots

Brought to you by the Centre's FinTech team

CENTRE *for*
REGULATORY
STRATEGY
EMEA

Content

Click on the item to access the relevant slide

Foreword

From human relationships to digital channels: Assessing the risks of digital customer journeys

Customer interactions with financial services (FS) are increasingly digital. Inspired by other interactions, customers expect faster, easier and more tailored access to financial products. Customers now have a whole ecosystem at their disposal which they can navigate to "pick and choose" their FS products and providers.

FS firms need to respond to those heightened customer expectations so as to preserve or enhance their business. New entrants ("digital natives") as well as incumbent firms are using, or experimenting with, Artificial Intelligence, Cloud Computing and Open Banking APIs to leverage the power of Big Data, and provide a better experience to customers, including by offering products digitally rather than through more traditional channels.

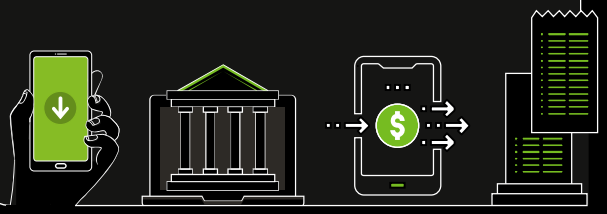
The shift in focus from "product" to "people", and from human-enabled to digitally-enabled, is taking hold, and takes firms into some nuanced regulatory and technological "hotspots" which require careful consideration and navigation.

- The use of digital channels, rather than, or in conjunction with, human interactions, raises new technology risks as well as challenges associated with the governance and controls around these technologies;
- The ease and speed of access to FS products mean that customers may be less vigilant when buying through digital channels, or assume that the products suggested to them online are knowledge-based and tailored to their personal needs. In this regard, they may be less attentive to the risks. Moreover, in a digital world, the human link to test and check the customer's understanding of the risks is less present than in a traditional interaction. Therefore, the risk of customers buying FS products rapidly and easily, but without understanding the related risks, is heightened; and
- In a more complex ecosystem, the relationship between the various participants may be less immediately clear, and their respective regulatory responsibilities more difficult to identify and communicate clearly to customers.

Here we seek to highlight some of those regulatory hotspots around conduct risks, digital risks, financial crime and data protection. These arise from a customer journey facilitated primarily through digital channels incorporating new technologies, and replacing substantively the need for a human interaction. The technological considerations are also key, as operational resilience and data quality directly affect the quality of the customer experience.

The journey illustrates some of the key regulatory issues that are likely to arise during a customer's digital journey. It is not a comprehensive analysis and cannot be relied on for regulatory compliance purposes.

Let's start the journey...



Overview of the journey

Introducing our customer

Click on the step to learn more

Sarah Jones

Age: 30

Place: Lives in Liverpool

Status: Married

Profession: Mechanical engineer

Introduction to the actors/technology used in this journey

Legacy relationship: Bank A and Bank B

Sarah's current banks – current account and credit cards. Sarah receives her monthly salary into her Bank A account

New App: CleverBudget

New budget management and account aggregation App

New banking relationship: MyNewBank

Recommended by *CleverBudget* – digital bank offering a marketplace for other FS providers

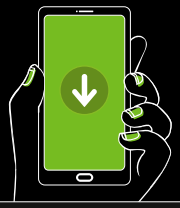
New MyNewBank platform product provider: InsurHome

App providing tailored home insurance products – connected to *MyNewBank*'s marketplace

Credit scoring agency : AICScore

External agency calculating credit scores for financial institutions. Used by *MyNewBank* to calculate customers' credit score

Sarah's four-step journey



Downloads a financial management aggregator App, CleverBudget. The App recommends a new digital banking account with MyNewBank and Sarah opens an account with it

Sarah applies for a mortgage through MyNewBank to buy a flat

Sarah applies to InsurHome for home insurance through MyNewBank's marketplace

Sarah's income becomes variable. She needs to review her entire financial portfolio

Key risks

Click on a risk to learn more

Conduct risks

Click here to learn more

Financial crime risks

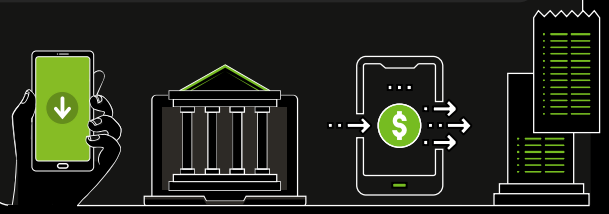
Click here to learn more

Data privacy risks

Click here to learn more

Digital risks

Click here to learn more



Conduct risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms

- When sending nudges*, firms will need to ensure that they clarify explicitly whether the nudge is a financial promotion, guidance (i.e. non-personal, generic information), or a personal recommendation. Accordingly, the firm will have to clarify its degree of regulatory responsibility and liability with regard to the customer's decision, based on whether the nudge is a financial promotion, or constitutes guidance or advice.
- If the nudge is a promotional offer, the firm will need to clarify the offer's deadline. If the nudge is a personal recommendation, the firm will need to explain why it thinks the recommended product is the best option for the customer, and highlight the size and scope of the market scanned to generate the given recommendation.
- Operators of marketplaces/shared platforms should be transparent to customers on the existence of any commission they receive in relation to the sale of a product/service.

*Nudges can be defined as prompts or actions that aim to inform customers and change the way they feel and behave. In a customer journey context, such nudges usually take the form of prompt notifications on customers' devices to inform them of a product or service that could be better tailored and suited to them.

Conduct risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms

- Firms using analytics to nudge customers towards specific products or providers based on the customer's data may be providing advised sales, as this may constitute a personal recommendation. Characteristics of an advised sale include: (i) explaining why the particular product or provider meets the customer's demands and needs; and (ii) giving a recommendation tailored to the customer's needs. In such cases, firms will need authorisation from their regulators to conduct advised sales.
- If the firm's business model is based on non-advised sales, firms will need to ensure they have controls in place to ensure that they do not stray into providing advice. Non-advised sales should avoid giving personal recommendations and leave the customer to decide how to proceed. For example, by providing generic information without mentioning any specific product(s) or provider(s).
- The use of analytics and customers' data should not result in customers being encouraged to buy products which are not appropriate for them or which offer poor value for money. Customer data should not be shared within the firm/group with the sole purpose of conducting cross-selling of financial products.

*Nudges can be defined as prompts or actions that aim to inform customers and change the way they feel and behave. In a customer journey context, such nudges usually take the form of prompt notifications on customers' devices to inform them of a product or service that could be better tailored and suited to them.

Conduct risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms

- Firms should be able to identify and address vulnerability at various points during the customer journey. Artificial Intelligence/Machine Learning (AI/ML) solutions could be leveraged to scan for indicators of potential vulnerability, for example by analysing customers' clicks on the website and the language/tone used on chatbots.
- Where the AI/ML solution identifies indicators of customer vulnerability, the firm should have systems and controls in place to hand the customer over to a dedicated team, where necessary. In such cases, the recommendation or treatment of the vulnerable customer by the firm should take account of the customer's needs rather than aggravate their vulnerability.
- Firms should ensure that people who do not have access to the technology/solution offered, or refuse to use it (such as when they ask to turn nudges off) are not excluded from the service or receive a higher/unfair price for their product/service.

*Nudges can be defined as prompts or actions that aim to inform customers and change the way they feel and behave. In a customer journey context, such nudges usually take the form of prompt notifications on customers' devices to inform them of a product or service that could be better tailored and suited to them.

Conduct risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms

- Firms should ensure that the use of customer data underpinning AI/ML solutions does not result in poor customer outcomes. For example, by exploiting behavioural biases or "protected characteristics", such as gender, faith or disability.
- The data used to train the algorithms, and the algorithm itself, should be updated and tested regularly for potential bias which could result in customers not being treated fairly.

*Nudges can be defined as prompts or actions that aim to inform customers and change the way they feel and behave. In a customer journey context, such nudges usually take the form of prompt notifications on customers' devices to inform them of a product or service that could be better tailored and suited to them.

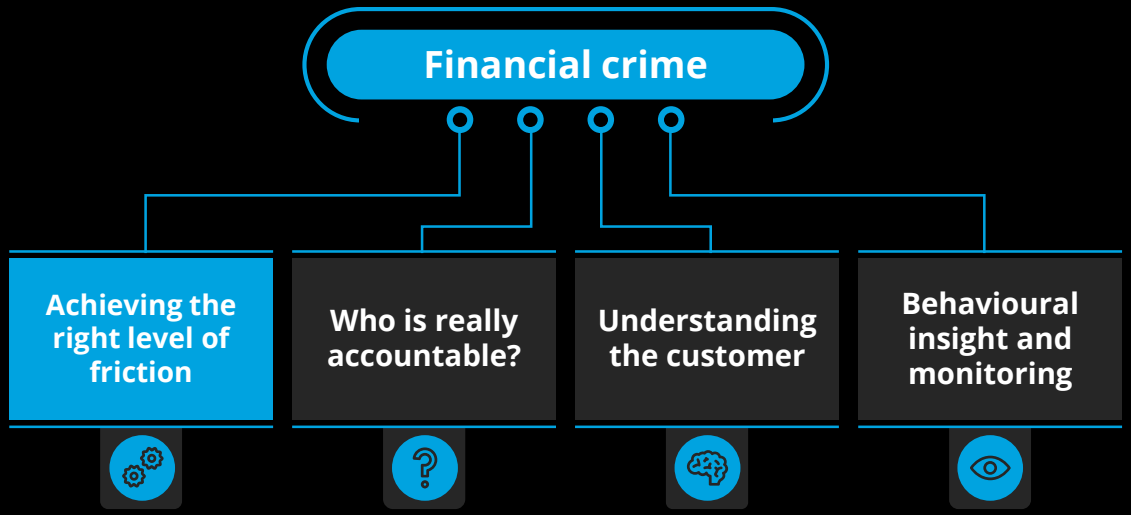
Financial crime risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



- Removing all friction from the customer journey may result in fewer controls, checks and balances. The challenge for firms is to achieve the “right” level of friction: applying robust controls digitally and seamlessly, but without compromising on quality.
- Being digital is not an excuse for collecting less information about customers. Firms must find a way to ask the right questions of their customers in a simple way without reducing the validity or usefulness of the information.
- Streamlining data collection at on-boarding often requires leveraging third party data sources and reference agencies. Firms should select trusted and reliable vendors and third parties across the on-boarding lifecycle, and interact with them through real-time APIs to make the process as efficient as possible.

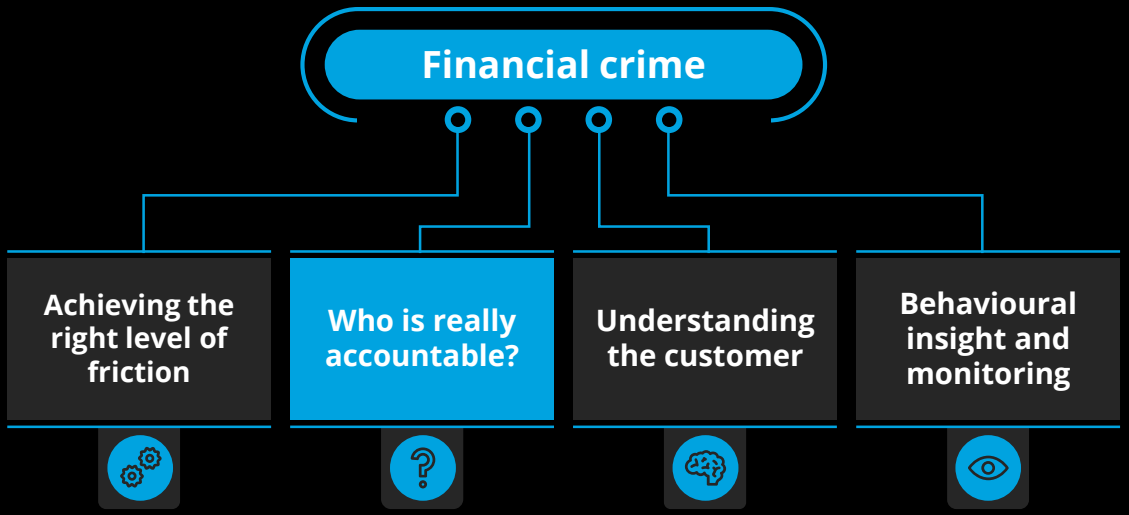
Financial crime risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



- Achieving an effective marketplace or network-banking model requires customers to be seamlessly on-boarded between providers. This has significant implications for the regulatory accountability for customer risk management.
- Firms must consider how customers are on-boarded to downstream providers. Simply transferring customer data may result in GDPR, privacy and trust issues. Relying on the due diligence performed by another provider brings issues with accountability and requires alignment of financial crime policies and requirements across providers.

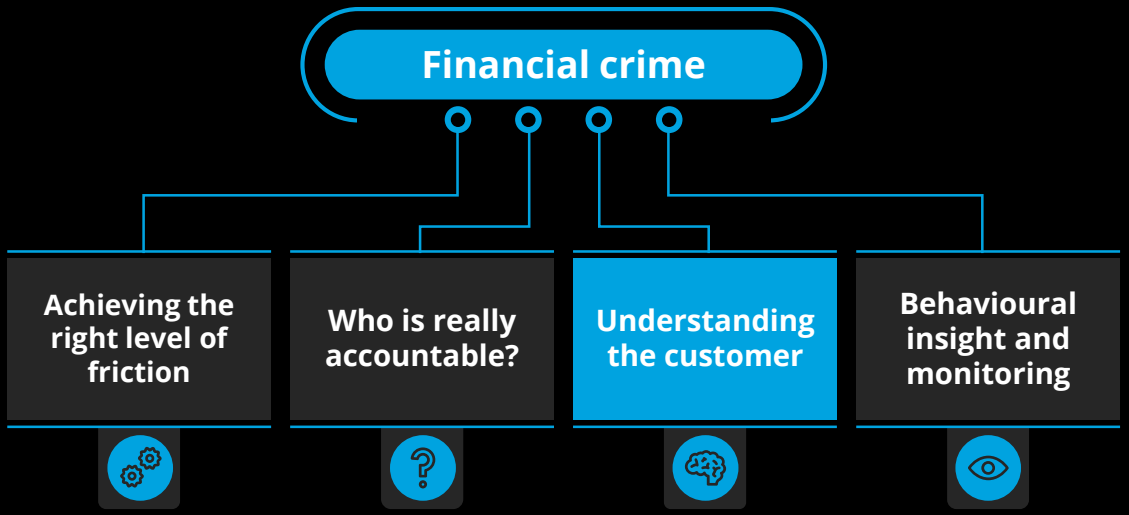
Financial crime risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



- In digital customer on-boarding, firms must put greater focus on anti-impersonation and fraud to mitigate the absence of human interaction. Biometrics, facial recognition and electronic Identity and Verification methods are possible solutions.
- Firms must conduct a robust money laundering risk assessment to identify higher-risk customers and to determine where enhanced due diligence measures should be applied. Firms must find a way to perform customer screening and risk assessment in real-time to the same standard that would be expected through any other channel.
- Firms should be ready to supplement digital journeys with human customer interactions where risk management requires it, even if this means breaking the “digital only” principle. Firms should incorporate effective cross-functional operational teams and a range of customer contact methods (e.g. in-App chat, video calling) into risk management practices.

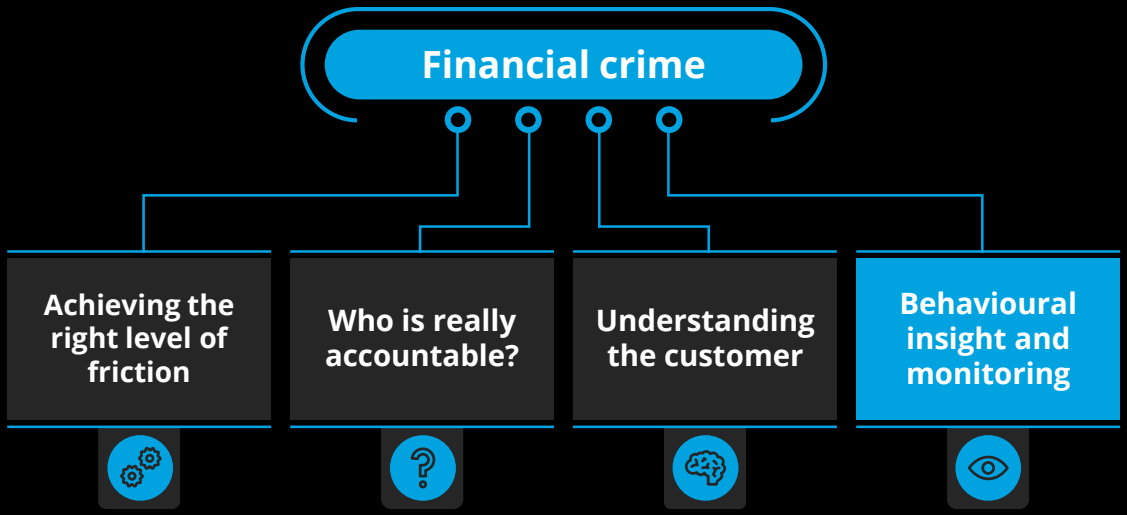
Financial crime risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



- On-boarding is just the start of the customer lifecycle, and firms must continuously monitor customer behaviours to identify new risks, and take appropriate actions to maintain the management and mitigation of customer risk. New products and digital delivery channels give rise to new risk typologies.
- Firms must undertake a comprehensive risk assessment to understand what new risks they are exposed to, and to ensure that on-going behavioural monitoring is effective across all financial crime risk domains, including Anti-Money Laundering (AML), fraud and anti-bribery and corruption.
- With the introduction of Open Banking and account aggregation solutions, firms now have the ability to see a broader scope of customer transactions, which can be used to gain greater insight into underlying customer behaviours across multiple providers.

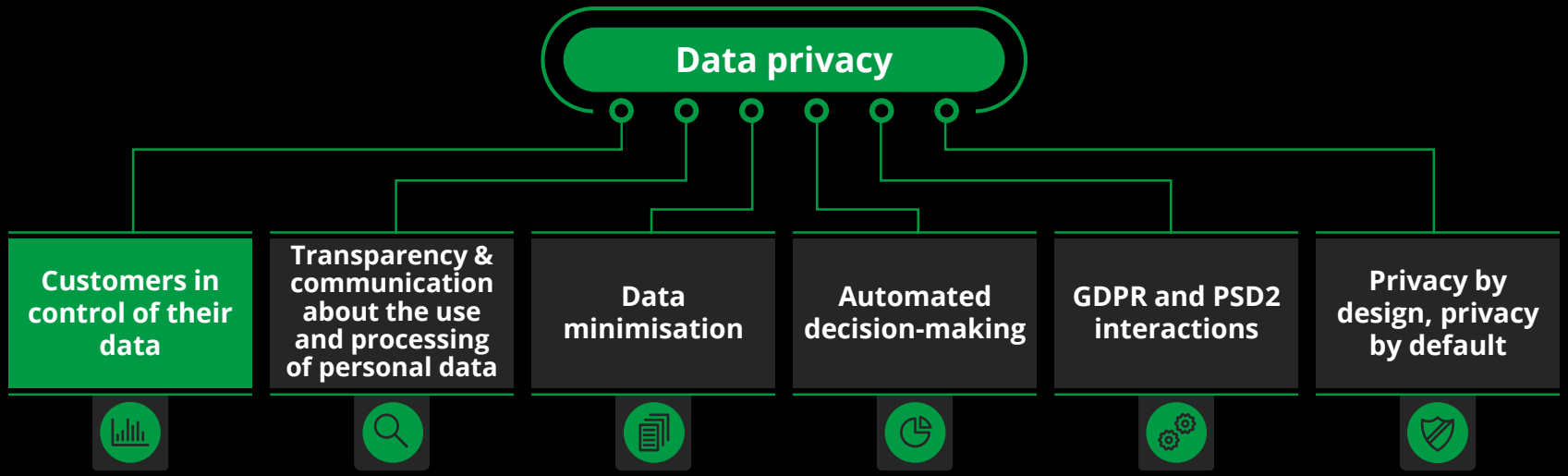
Data privacy risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



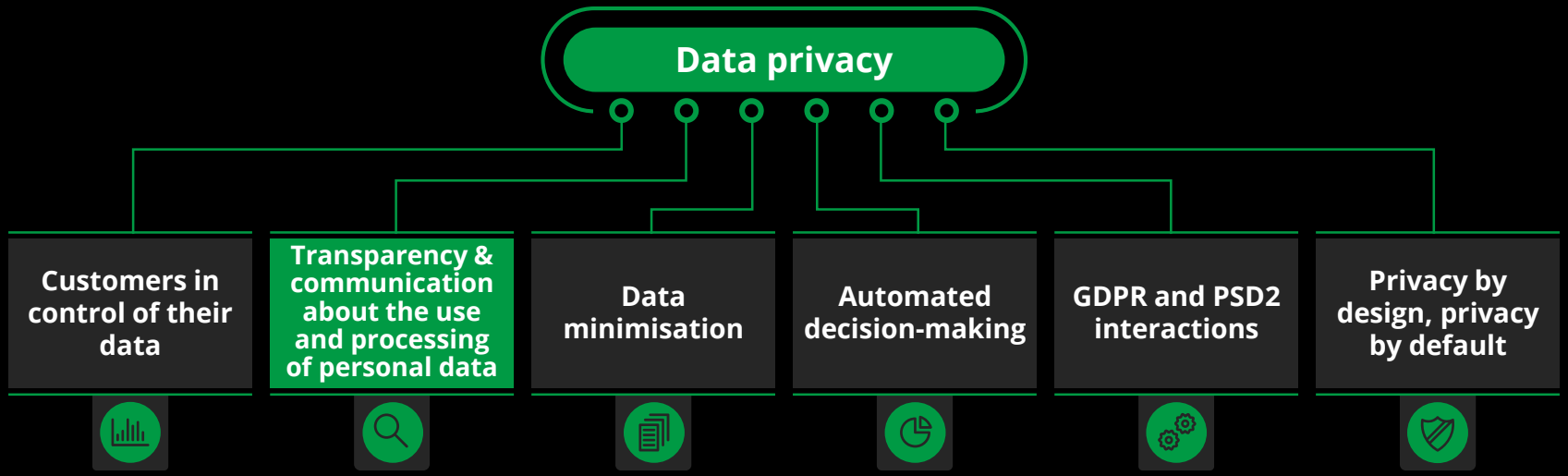
- Firms will need to ensure that the data protection principles and requirements applicable under GDPR are enshrined into the design and deployment of the customer journey, in a way that puts customers in control of their data. Compliance with these requirements should not prejudice the quality of the customer journey, which should be as frictionless as possible from a data privacy perspective.

Data privacy risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

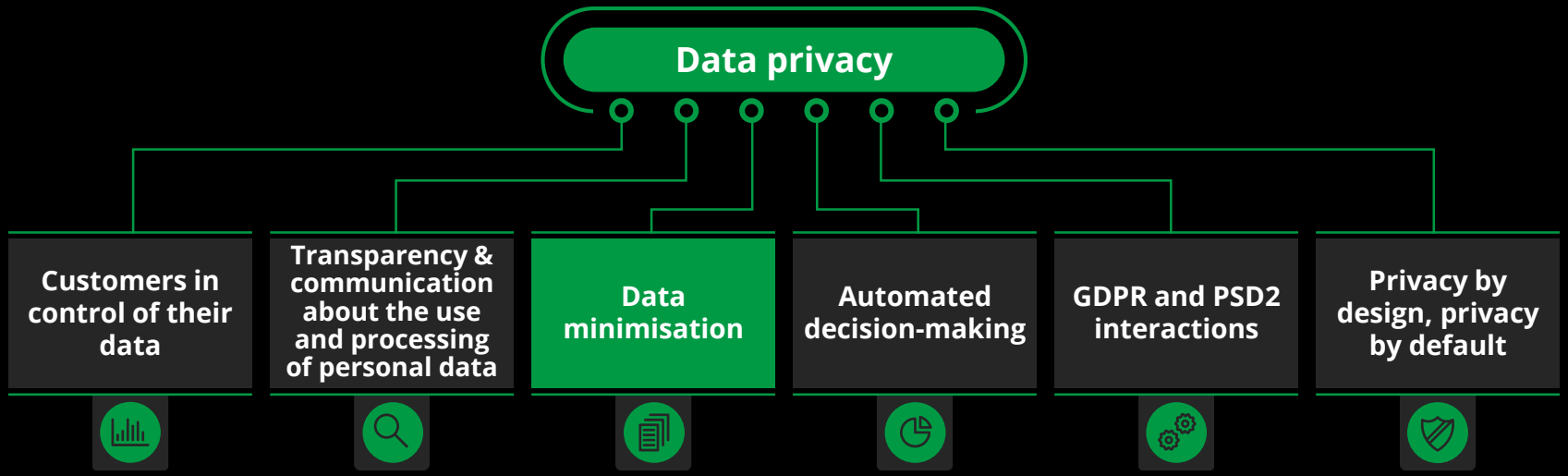
- Firms will need to inform their customers of their rights with regard to data protection, and respect any requests for the firm to stop processing their personal data for direct marketing at any time. Firms will need to give customers the option to turn the nudges off.
- Firms will need to communicate in a complete but concise and easily understandable way with their customers about how and why they collect and process their data (e.g. profiling, calculating premium, etc) and ensure they have a valid basis on which to do so.
- Firms will need to receive, and regularly ask for, customers' explicit consent before collecting and processing their data, and more generally, to perform any activity that requires the use of customers' personal data. They will also have to prove that processing the data is necessary for entering into, or the performance of, a contract.

Data privacy risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

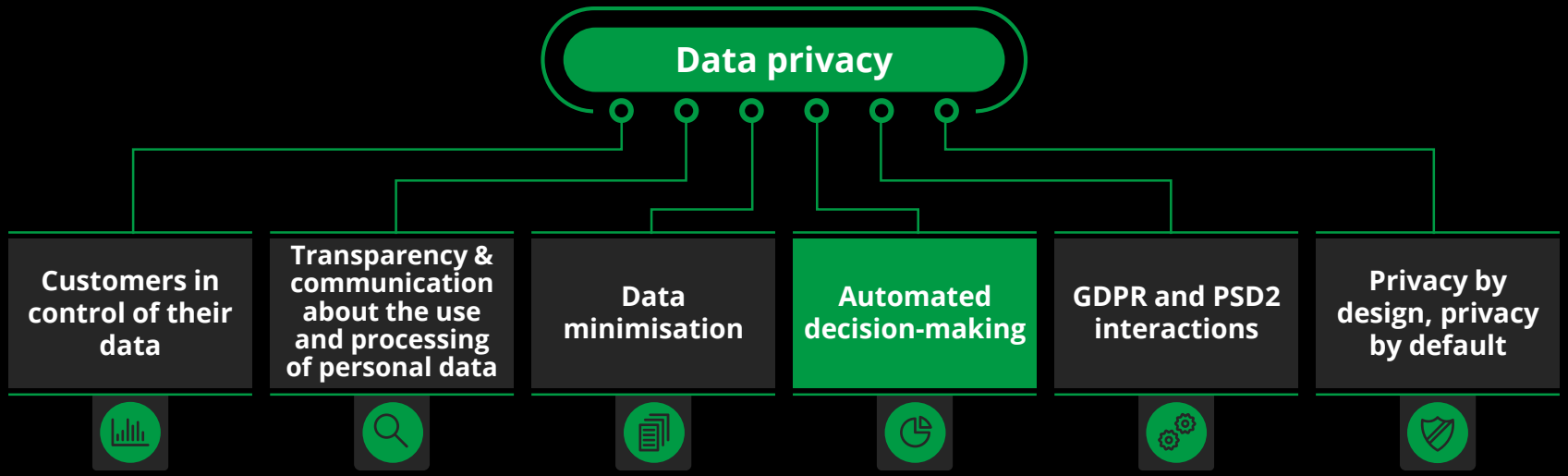
- Firms will need to ensure that they only collect and analyse the minimum amount of data necessary for the performance of the contract/activity. The personal data collected should be “adequate, relevant and limited to what is necessary for the purposes for which they are processed”.

Data privacy risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- When using automated decision-making, firms will need to give easy and clear access to a human adviser able to explain the outcome of the automated solution (Article 22 of GDPR). The key fundamental rights under GDPR (including the right to explanation and right to be forgotten) will also apply to automated decision-making.
- When using automated decision-making, firms will need to be able to demonstrate that they have considered how the data processing may affect the individual, that they have been clearly informed that automated decision-making is involved and of the possible consequences of the processing, and that they are aware of their rights (including the right to an explanation and human review in some cases).

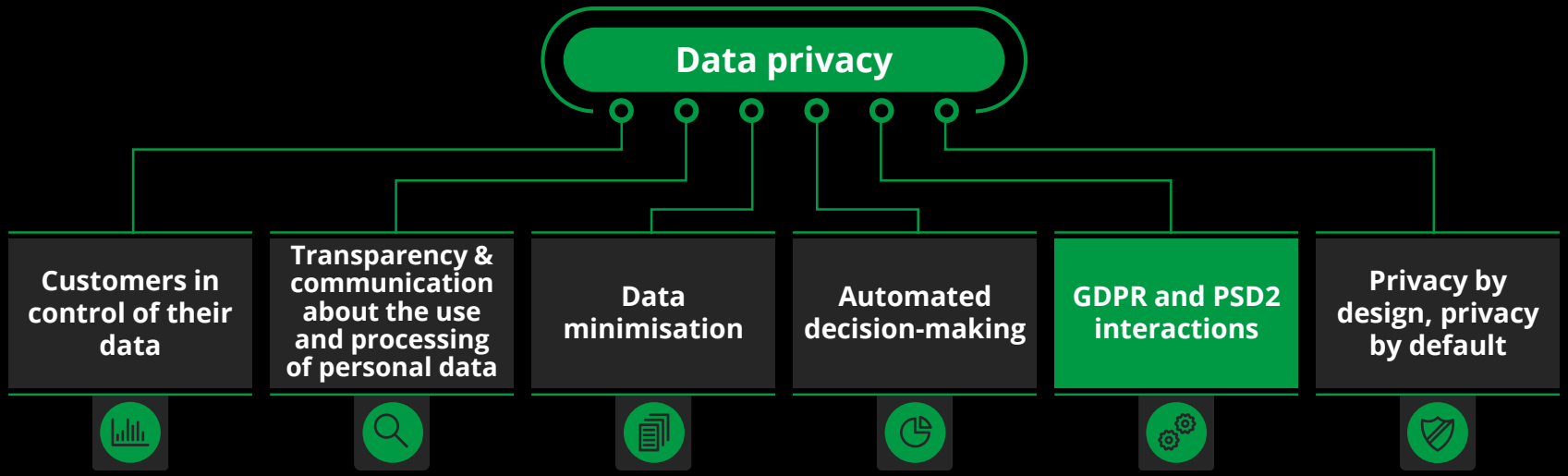
Data privacy risks

Click on a theme to learn more

Risk Area

Themes

Considerations for firms



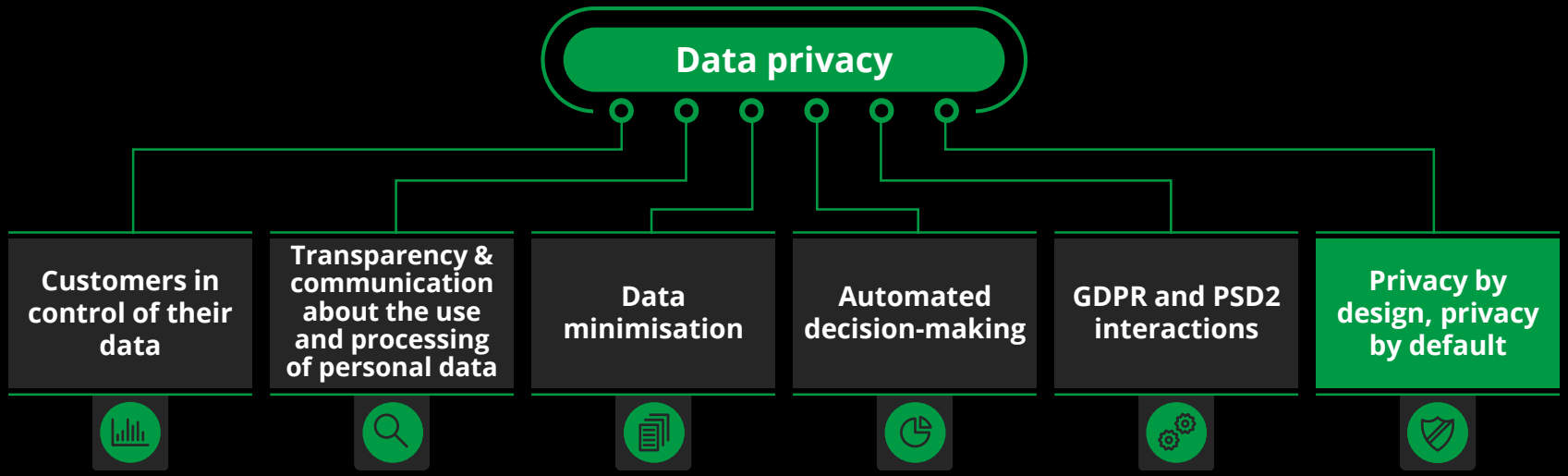
- Customers will have to give their explicit consent to sharing their data with other market participants on a platform or marketplace, and, where relevant, data transfers will have to be done via platforms compliant with the requirements on "Strong Customer Authentication and Common and Secure Open Standards of Communication" under PSD2.

Data privacy risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

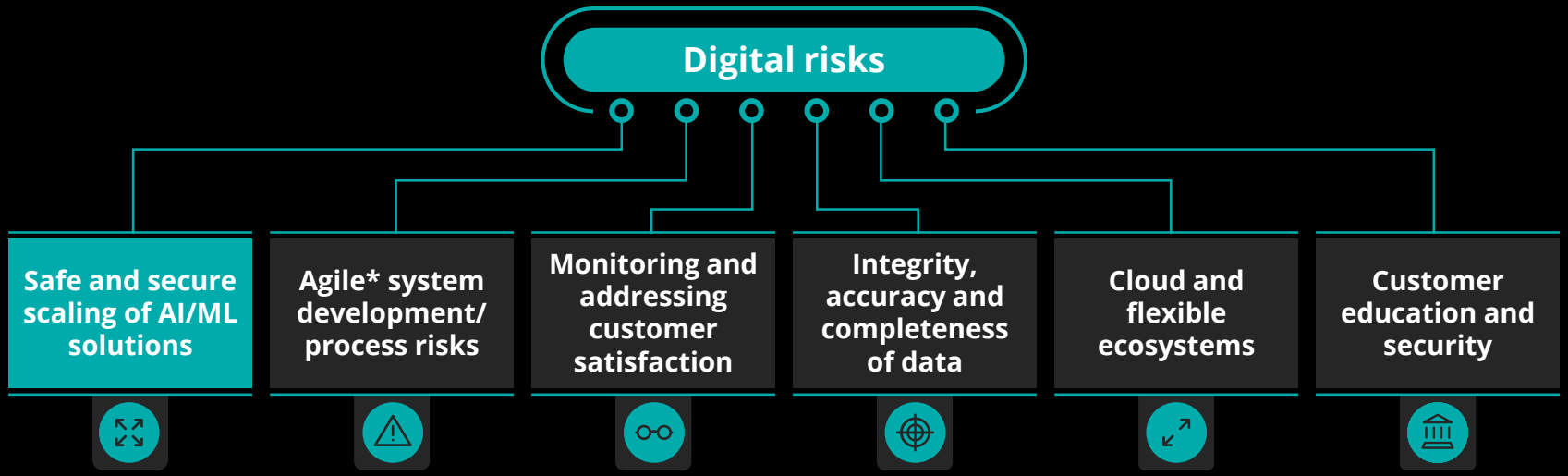
- Firms should conduct a Data Protection Impact Assessment (DPIA) for processing that is likely to result in a high risk to individuals and should enshrine the principles of Privacy by design and Privacy by Default in any new solution, including those based on AI/ML, they create and which uses customers' personal data.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- From the design phase through to development and deployment, firms will need to ensure that the algorithm and the training data are tested regularly and updated to prevent potentially unfair or biased outcomes for customers. The systems and controls will have to be implemented at the design phase of the algorithm, and followed through to the development, deployment and monitoring phases. Training data, as well as data sources after the deployment of the algorithm, should be validated by the relevant teams. The relevant conduct and risk teams should also be involved in the design and review of the algorithm.
- Customers may feel unease at the perception of "robots" taking decisions on their access to and use of financial products. Firms will need to ensure that the appropriate governance and controls are applied to their AI/ML solutions, to ensure that they work as intended, and do not produce unfair outcomes or discriminate against certain customers.

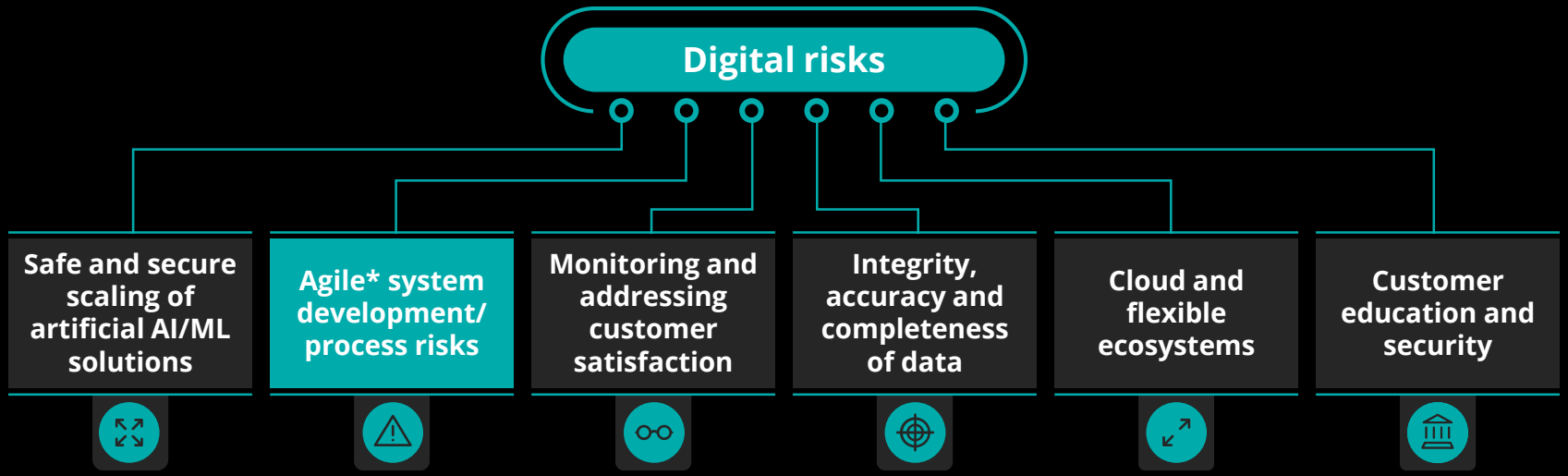
*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- Multi-channel banks will need to ensure the effectiveness of their legacy governance frameworks for agile deployments.
- Customers may see an increase in outages and bugs if the agile delivery approach is not controlled appropriately, which could degrade customer experience and potentially lead to incidents such as data losses. Firms will need to automate key control processes and risk management during the deployment of their agile delivery approach.
- Firms will need to take a flexible, risk-based approach and ensure that the use of digital channels/technologies does not expose them to risks outside their appetite.
- Firms will need to define and embed optimised controls and controls assurance processes to address process risks.

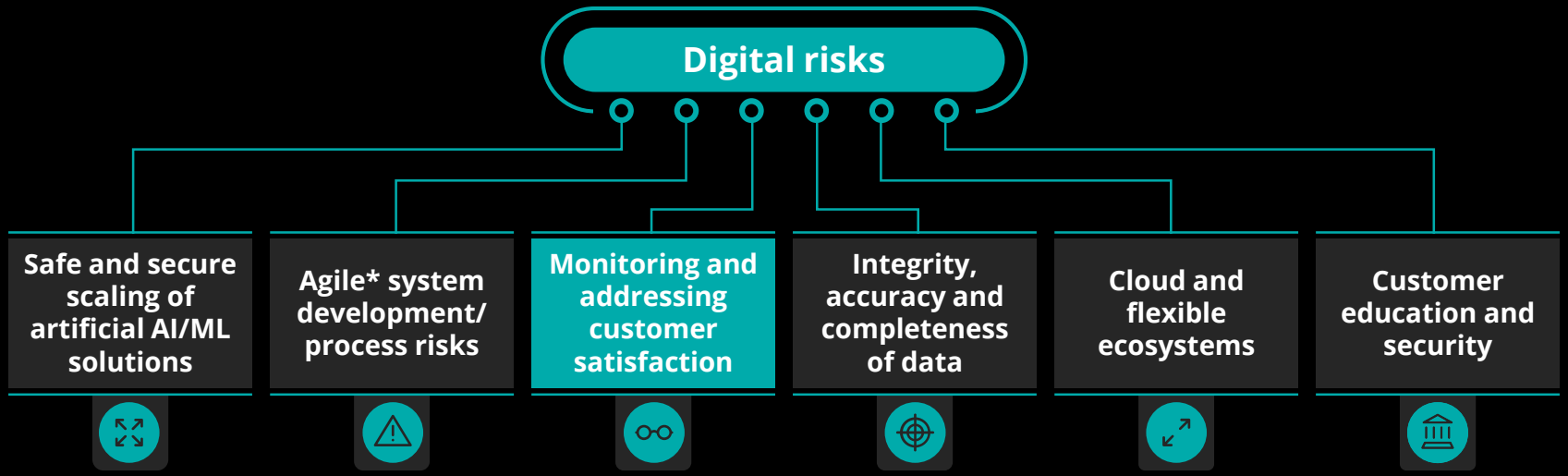
*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- Customers' satisfaction may degrade over time if the customer journey/experience offered through digital channels does not meet their expectations. Firms should implement adequate governance and oversight, monitor and measure continuously customer feedback and the value created from the digital transformation, and ensure that it remains aligned to the wider business strategy.
- Firms will need to develop robust systems and controls to ensure that they are able to identify complaints made through digital channels (e.g. chatbots) and address these complaints in a timely manner.

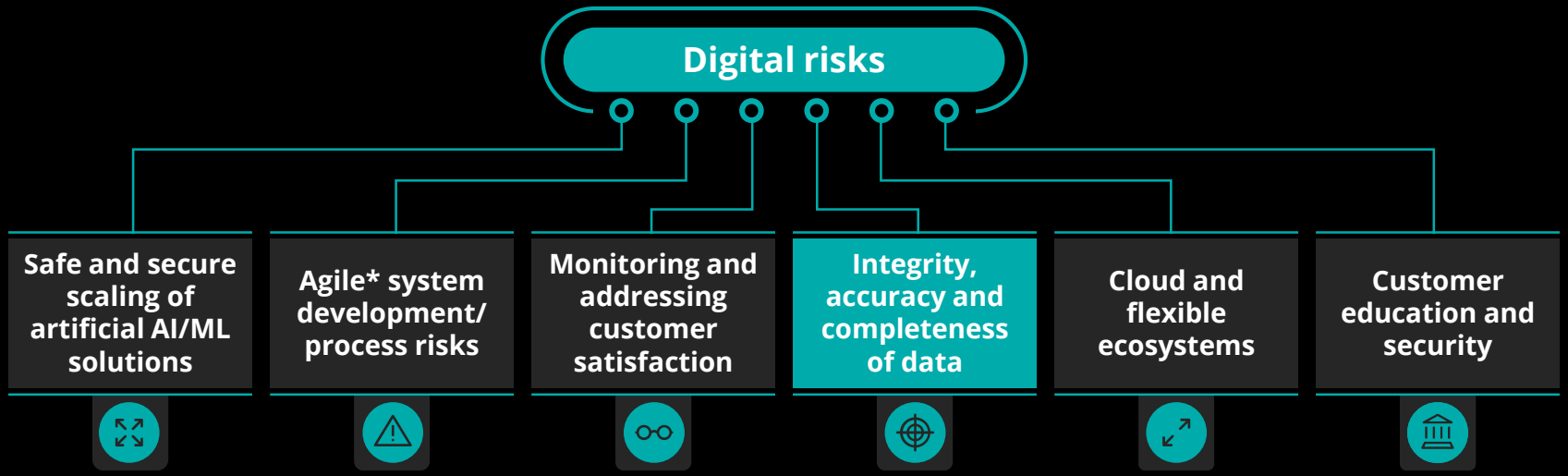
*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- Firms will need to ensure that transferring or receiving data from other firms does not impair the integrity, accuracy and completeness of the data. They will need to implement robust governance, systems and controls to ensure that data is not corrupted, stolen or lost during transfers. Any change in the terms or conditions regarding the processing of data will have to be duly reflected in the App and communicated clearly to customers.
- Firms will need to ensure that the data collected through digital channels (e.g. chatbots, AI/ML) can be accurately and fully reported to a human adviser. Both the information collected digitally and by the human adviser will need to be combined to address as efficiently as possible the customer's case, particularly when the latter is signalling vulnerability.

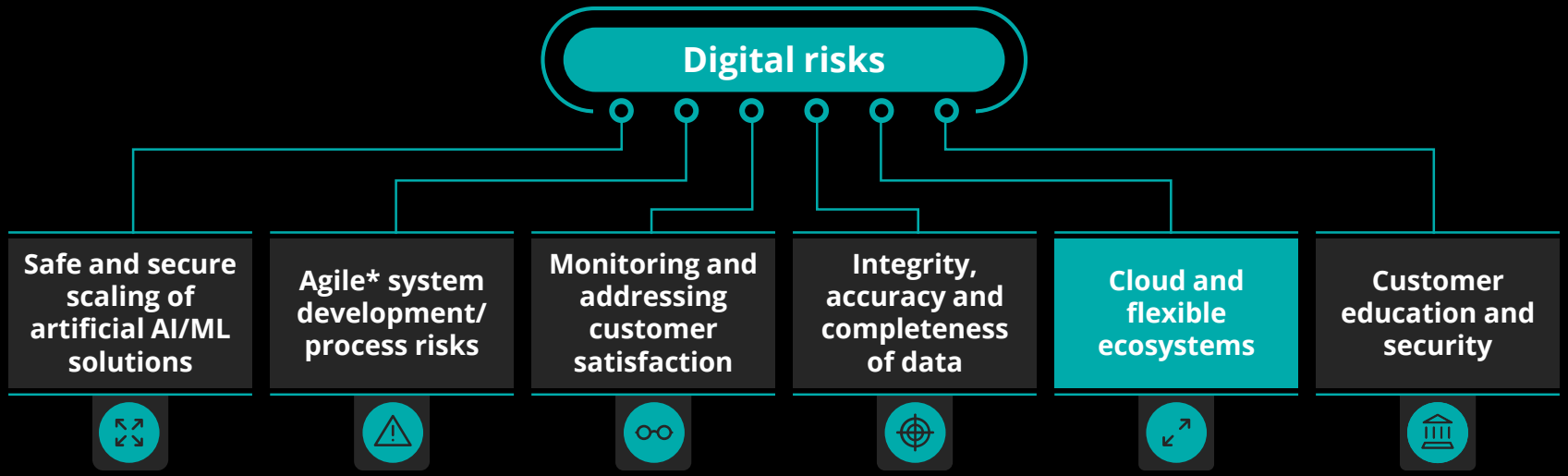
*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- Firms will need to apply adequate governance and oversight of third party risks arising from the use of a Cloud architecture. This will include the implementation of business continuity plans in case of an IT outage or external cyber attack targeting the cloud service provider (CSP).

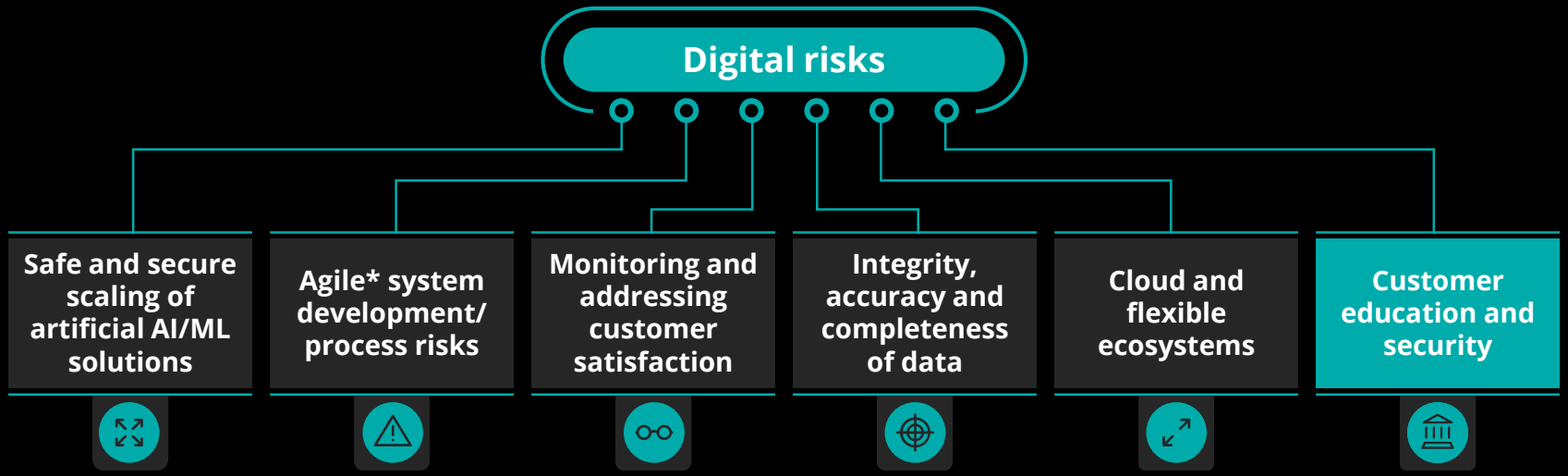
*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Digital risks

Click on a theme to learn more

Risk Area

Themes



Considerations for firms

- Firms will need to demonstrate how customers can use their App, and express clearly the split of responsibilities around security risks between the firm and the customer (e.g. in case of lost device or a cyber attack).

*Agile has roots in accelerated software development and has evolved as more processes move into a "digital first" model of operation for businesses and teams. At the core is a set of ways of working for transformation and business teams, using methodologies that differ significantly from a traditional planned "Waterfall" task delivery; with more emphasis on individuals and interactions between specialists, early access to real prototypes, iterative requirements with customer collaboration, flexibility, speed and responsiveness to change.

Step 1

Sarah downloads a financial management aggregator App to manage her budget, and opens a new current account with a digital bank

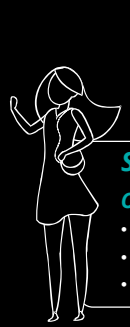
Background

Sarah decides to download a financial management aggregator App – ***CleverBudget***, to manage her finances and facilitate money transfers between Bank A and Bank B.

By analysing her payments data, ***CleverBudget*** sends a notification to Sarah, recommending ***MyNewBank***. She decides to act on it by downloading ***MyNewBank***'s App on her phone.

MyNewBank uses a facial recognition solution for on-boarding clients, and has an AI tool to identify vulnerability (including by looking at potentially "erratic clicks", which could signal stress in customers).

Both ***CleverBudget*** and ***MyNewBank*** operate fully on the Cloud.



Sarah's perspective

Opportunities

- Single customer view of all her accounts.
- Ease of transfers.
- Better interest rate.

Concerns

- Uses and security of her personal data.
- Security of the App.

Regulatory hotspots

Conduct

- Transparency about the size of market scanned to perform the nudge – financial promotion.
- Customer vulnerability.
- Forbearance.
- Ethics and fairness.

Financial crime

- Increased risk of fraud and impersonation.
- Comprehensive risk assessment to drive differing levels of due diligence.
- Risks of digital channels and products to be understood.

Data privacy

- Transparency and communication around the processing of personal data.
- Data minimisation.
- Security and compliance with GDPR of data transfers from Bank A and B to *CleverBudget*.

Digital risks

- Reliance on third parties (CSPs).
- Integrity, accuracy and completeness of data transfers – performance of API feeds.
- Customer education and security.
- Design and governance of AI solution/chatbot.

Considerations for firms

CleverBudget

- Be registered as an Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP) under PSD2. Register to the Open Banking Directory in the European Banking Authority's register for EU operations.
- Perform DPIA, obtain Sarah's consent, and be transparent about how her data is collected and processed; collect and analyse only the minimum amount of data necessary for the performance of the contract.
- Apply Strong Customer Authentication under PSD2.
- Clarify Sarah's responsibilities for the security of the App.
- Perform continuous testing and validation of integrity, accuracy and completeness of the data received through API feeds from Bank A and Bank B.
- Apply robust governance to contracts with CSPs.
- Be transparent about the size of the market scanned for the recommendation and the arrangement in place with *MyNewBank*.
- Ensure that the recommendation of *MyNewBank* meets Sarah's needs, and is based on sufficient information and documentation collected from her.

Bank A and Bank B

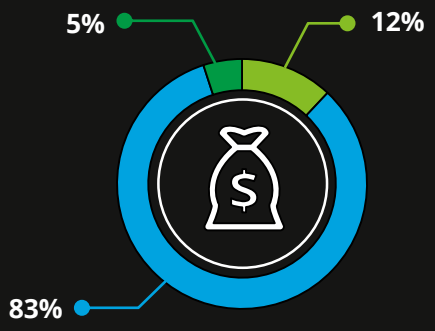
- Secure and regularly renew Sarah's consent to transfer her data to *CleverBudget*.
- Ensure the integrity, accuracy and completeness of the data transferred to *CleverBudget*. Regularly test the performance of API feeds.

MyNewBank

- Possible use of consumer behavioural analysis to present terms and conditions in an accessible and user friendly way to ensure Sarah fully understands them.
- Apply robust governance and controls to the facial recognition solution and AI solution to ensure that they are not biased against Sarah.
- Apply robust governance to contracts with CSPs.

Our survey revealed that a large majority of people do not have an App to manage their money, the main reasons being that they do not think they need one, or that they do not want to share their financial details with an App.

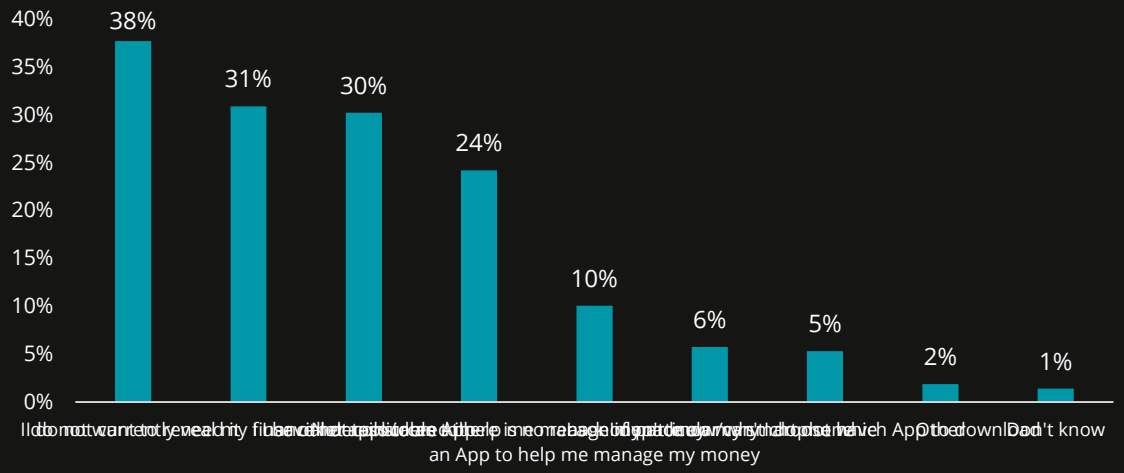
Do you have an App on your smartphone which helps you to manage your money (e.g. by providing advice on budgeting, savings, etc.)?



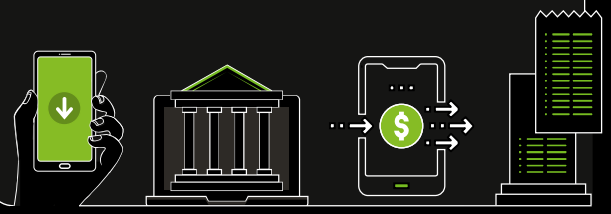
- Yes, I do
- No, I do not
- Don't know/can't recall

You previously mentioned that you do NOT have an App on your smartphone which helps you to manage your money (e.g. by providing advice on budgeting, savings, etc.).

Which, if any, of the following are your reasons for this?*



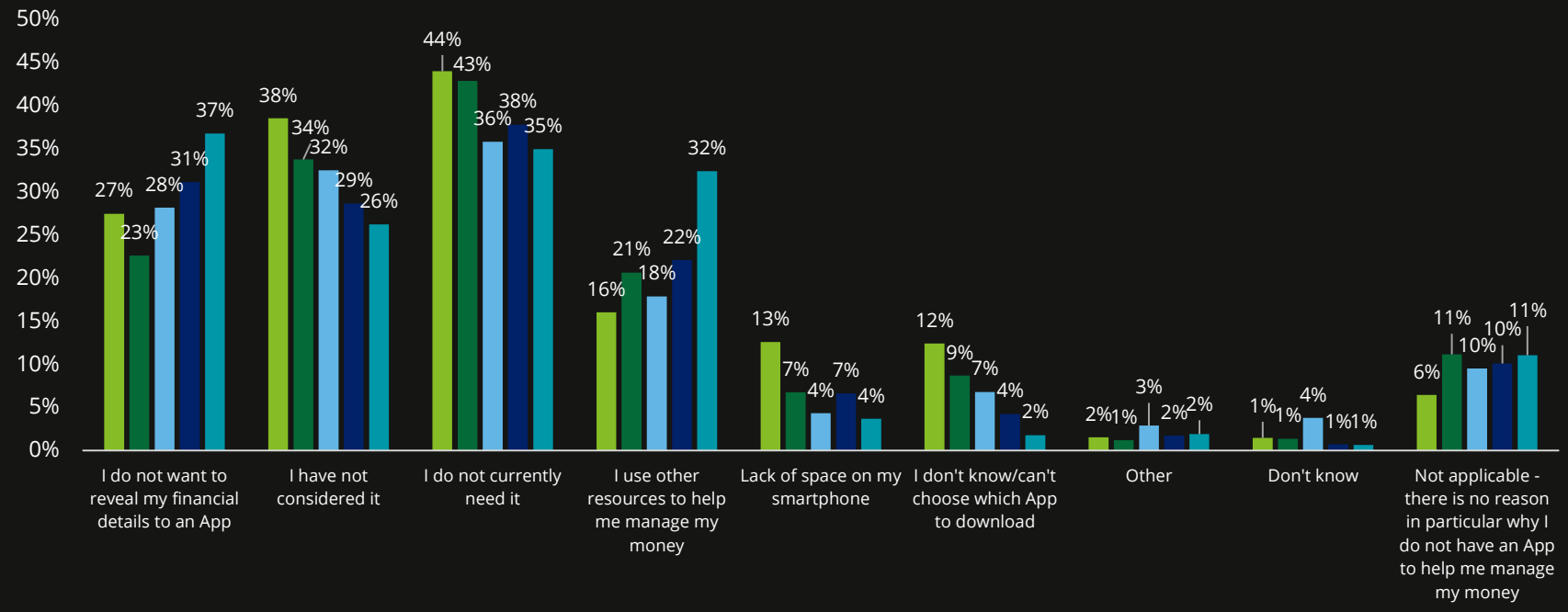
* Survey participants could select more than one reason.



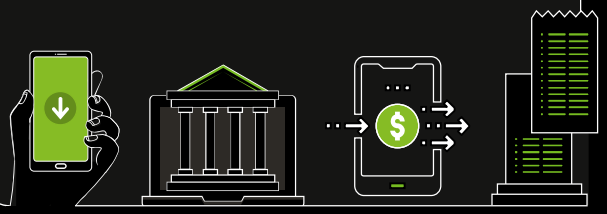
Why do people not have a financial management App?

Comparing across age groups, those in the 18-34 group do not have an App mainly because they do not think they need it, while the main reason given by those in the 55+ group for not having an App is their reluctance to share their financial data with a budget management App, followed closely by not needing it.

You previously mentioned that you do NOT have an App on your smartphone which helps you to manage your money (e.g. by providing advice on budgeting, savings, etc.)...Which, if any, of the following are your reasons for this?*

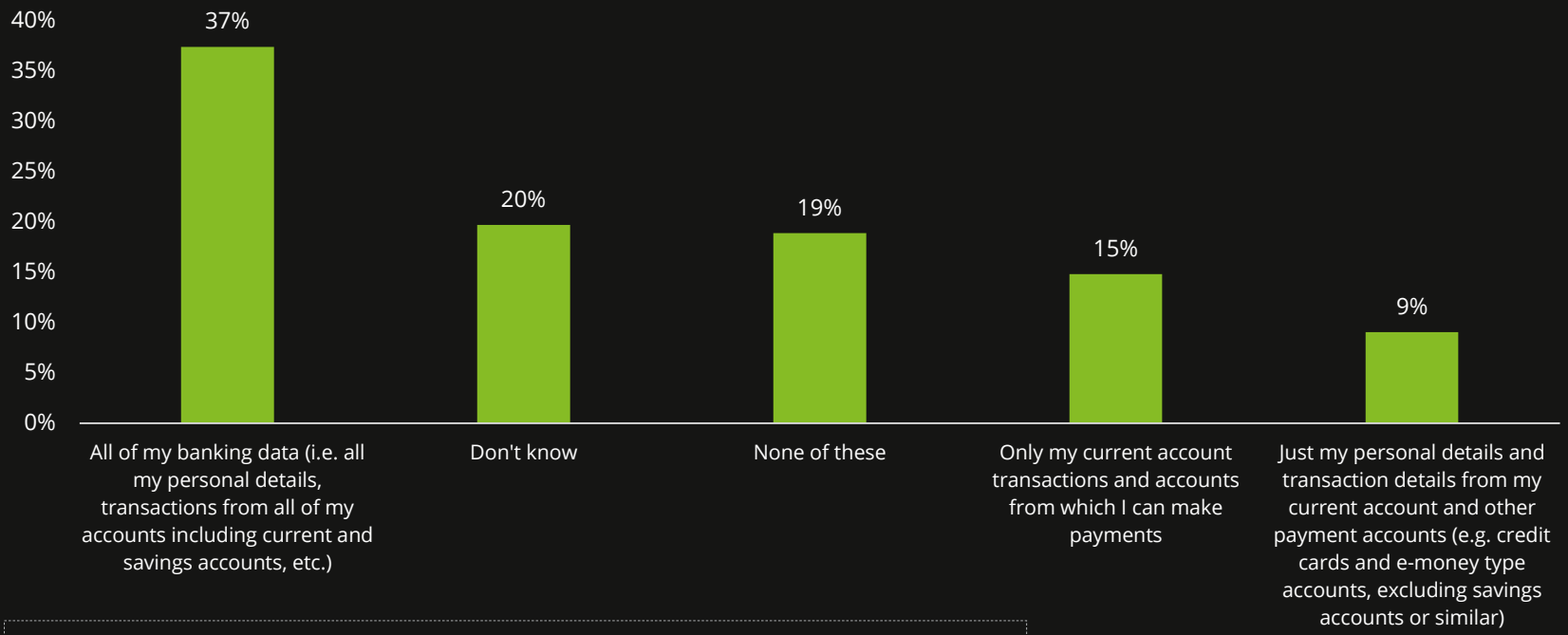


* Survey participants could select more than one reason.

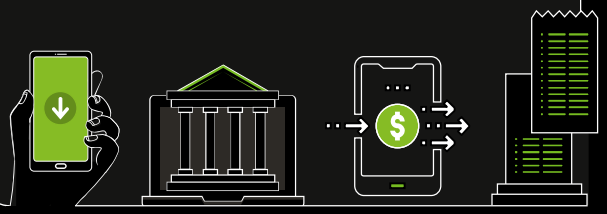


Most of the people surveyed do not know, or have misconceptions about, what banking data their App can have access to through Open Banking APIs.

Imagining that you have decided to download a money management App on your phone and give the App permission to access and collect your banking data, how much information do you think the App will have access to?

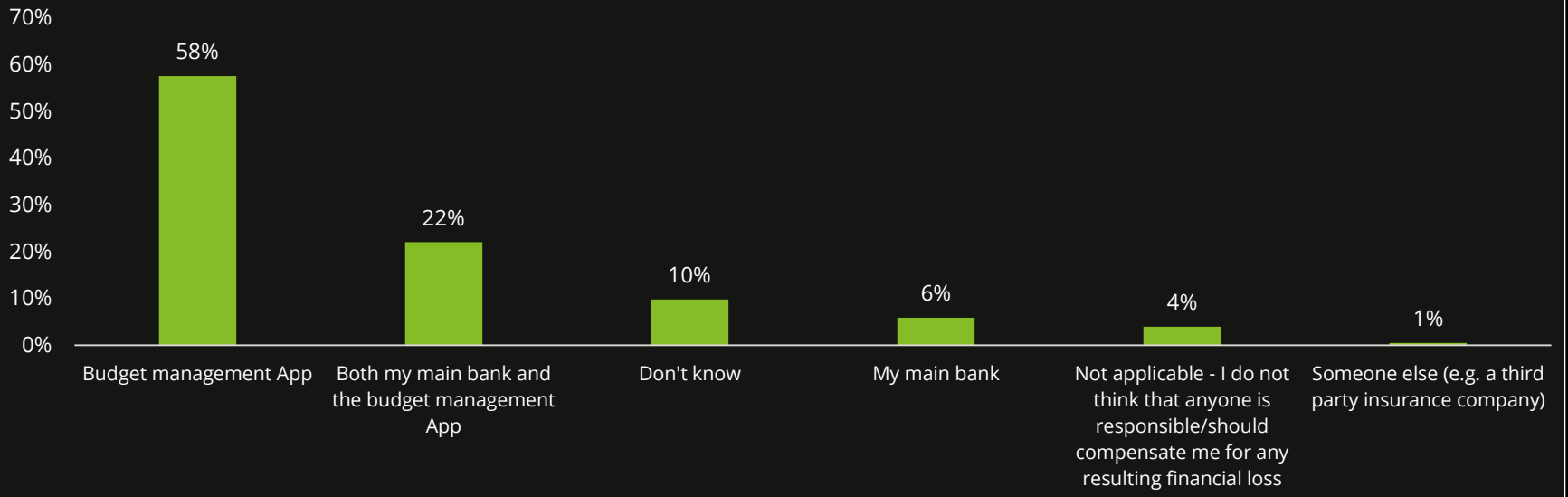


PSD2 allows authorised third parties to access transactional data as well as some selected personal information, such as the name of the account owner and the account number, solely from accounts that can be used to make and receive payments. If customers have multiple payments accounts, third parties need to specify clearly which accounts they would like to access, and receive customers' consent before doing so.

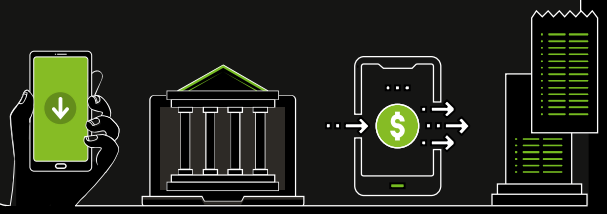


Additionally, most people had misconceptions about who should compensate them, were the budget management App (that accesses banking data through Open Banking APIs) to be subject to a cyber attack.

Please imagine that your budget management App has faced a cyber attack and your data has been stolen...In this scenario, who, if anyone, would you say is responsible and should compensate you for any resulting financial loss? (Please select the option that best applies.)



Under PSD2, the institutions (e.g. a bank) where customers hold their payment account(s) are liable to their customers for any unauthorised/fraudulent transactions and any compensation that may apply. Account providers may then be able to seek compensation from any involved third party, depending on the specific circumstances. However, whether or not it leads to any financial detriment, third parties will be liable for any theft, loss, or mis-use of any customer personal data and/or service disruption.



Step 2

Sarah applies for a recommended mortgage with MyNewBank

Background

Looking at her banking data, ***MyNewBank*** sends a nudge to Sarah and recommends to her one of its mortgage products.

MyNewBank uses an external agency, ***AICScore***, to produce a credit score for Sarah. ***AICScore*** collects Sarah's data by using a chatbot, and uses an algorithm to calculate the credit score. Sarah initially receives a low score, despite having a regular income and always servicing her debts on time. Sarah wants to contact ***AICScore*** to ask why she received a low credit score.

MyNewBank uses a chatbot to collect information from Sarah to conduct her affordability check. It also uses Bank A's API to collect information on monthly income and expenditure. A human adviser checks the information collected by the chatbot/API and performs an advised sale.

Sarah's perspective

Opportunities

- *MyNewBank's* nudge prompts her to apply for a mortgage with *MyNewBank*.
- The use of a chatbot and AI for the credit score calculation and affordability check makes the process smoother and quicker.

Concerns

- Sarah may get a low credit score and not know who to speak to in such case.

Regulatory hotspots

Conduct

- Transparency around the basis of the recommendation.
- Personal recommendation – ensuring the mortgage is suitable for Sarah's needs.

Financial crime

- Regulatory accountability for customers on-boarded between providers.

Data privacy

- Data minimisation, transparency and communication.
- GDPR compliance for automated decision-making – explainability and ability to speak to a human adviser.

Digital risks

- Design and governance of AI solutions.
- Monitoring of outcomes of AI solutions (e.g. feeds) and complaints through digital channels.

Considerations for firms

MyNewBank

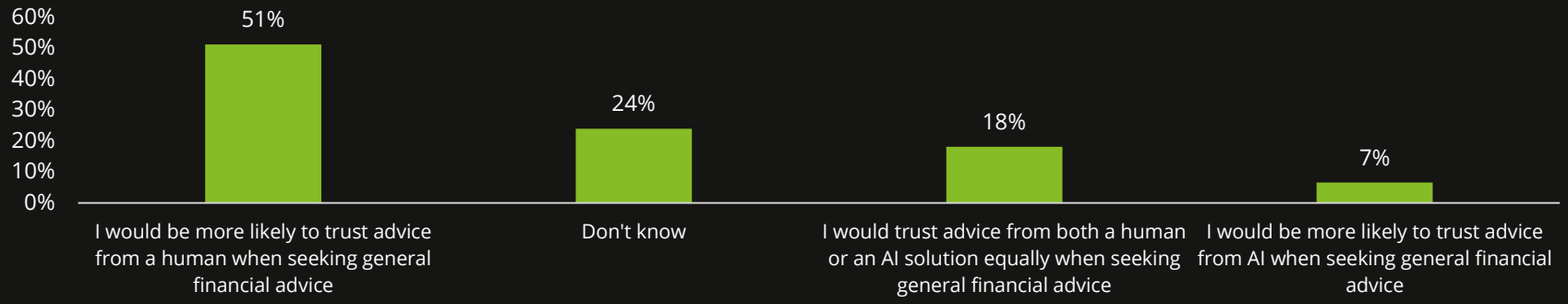
- Perform DPIA, secure and regularly renew Sarah's consent, and be transparent about how her data is used and collected by the chatbot. Only the minimum amount of data should be collected and analysed.
- *MyNewBank* needs to ensure the mortgage is suitable to Sarah's needs and circumstances and requires regulatory permission to conduct the advised sale of the mortgage.
- Ensure the chatbot/API collects Sarah's information accurately and records the conversation feeds so that a human adviser can advise Sarah on a product that meets her needs and circumstances.
- Give access to a human adviser whenever Sarah requests it who is able to explain the outcome of the automated solution (affordability).
- Ensure processes and controls work appropriately to permit timely handovers.
- Ensure quality, accuracy and relevance of API data received from Sarah and Bank A, on which the nudge and then the advised sale are based.

AICScore

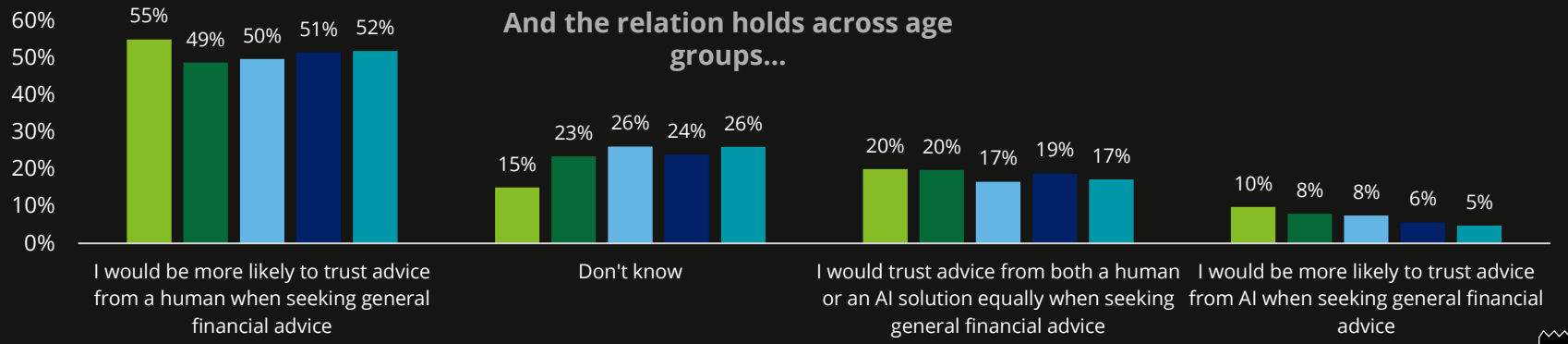
- Perform DPIA, secure and regularly renew Sarah's consent, prove the lawful basis for processing personal data, and explain how her data is used and collected by the chatbot.
- Give easy access to a human adviser to explain the outcome of the algorithm's calculation of Sarah's credit score and mitigate any unintentional negative outcome with regard to her credit score.

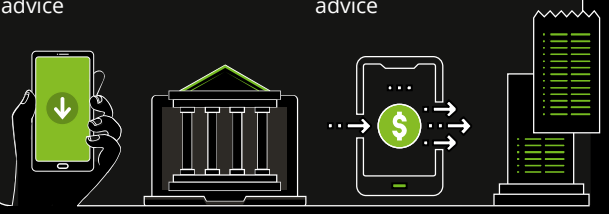
Over half of the people surveyed placed more trust in a human adviser over AI, for financial advice. This holds across all the age groups.

Would you be more likely to trust financial advice provided by Artificial Intelligence (AI) or a human, or would you trust them both equally?



And the relation holds across age groups...





Step 3

As a condition of securing her mortgage, Sarah buys home insurance through MyNewBank's marketplace

Background

MyNewBank requires Sarah to have home/building insurance as a condition for granting her mortgage and suggests she looks at providers on its marketplace, which brings together a small group of FS providers.

Sarah finds ***InsurHome*** which provides home insurance and currently offers 50% (automatic) discount on the home insurance policy premium if Sarah purchases its home security devices (camera, alarm, etc). ***InsurHome*** uses AI to calculate Sarah's monthly premium, based on the information collected through ***MyNewBank's*** API (different from its marketplace). It then uses the data it collects though the security devices on a continuous basis to adjust the premium each month. ***InsurHome*** pays a commission to ***MyNewBank*** if Sarah takes out an insurance policy with it. Sarah buys home insurance from ***InsurHome***.

Sarah's perspective

Opportunities

- Sarah enjoys the ease with which she can take out the home insurance.

Concerns

- Sarah is uneasy about being "tracked" continuously by the insurance firm, even if it means a lower premium.

Regulatory hotspots

Conduct

- Transparency of the commission paid to *MyNewBank*.
- Ethics and fairness of using Sarah's data to calculate the premium.
- Guidance vs personal recommendation.
- Potential for poor outcomes driven by cross-subsidisation by *InsurHome*.

Financial crime

- Customer risk to be re-assessed based on new products.
- Reliance on KYC performed by other providers.
- Accountability for performing financial crime controls for new products.

Data privacy

- Data minimisation, transparency and communication.
- GDPR compliance for automated decision-making.

Digital risks

- Governance of AI solutions.
- Customer satisfaction and monitoring of outcomes of AI solutions.
- Integrity, accuracy and completeness of the data transferred to *InsurHome*.
- Cyber security concerns with the collection of data by the home security device.

Considerations for firms

MyNewBank

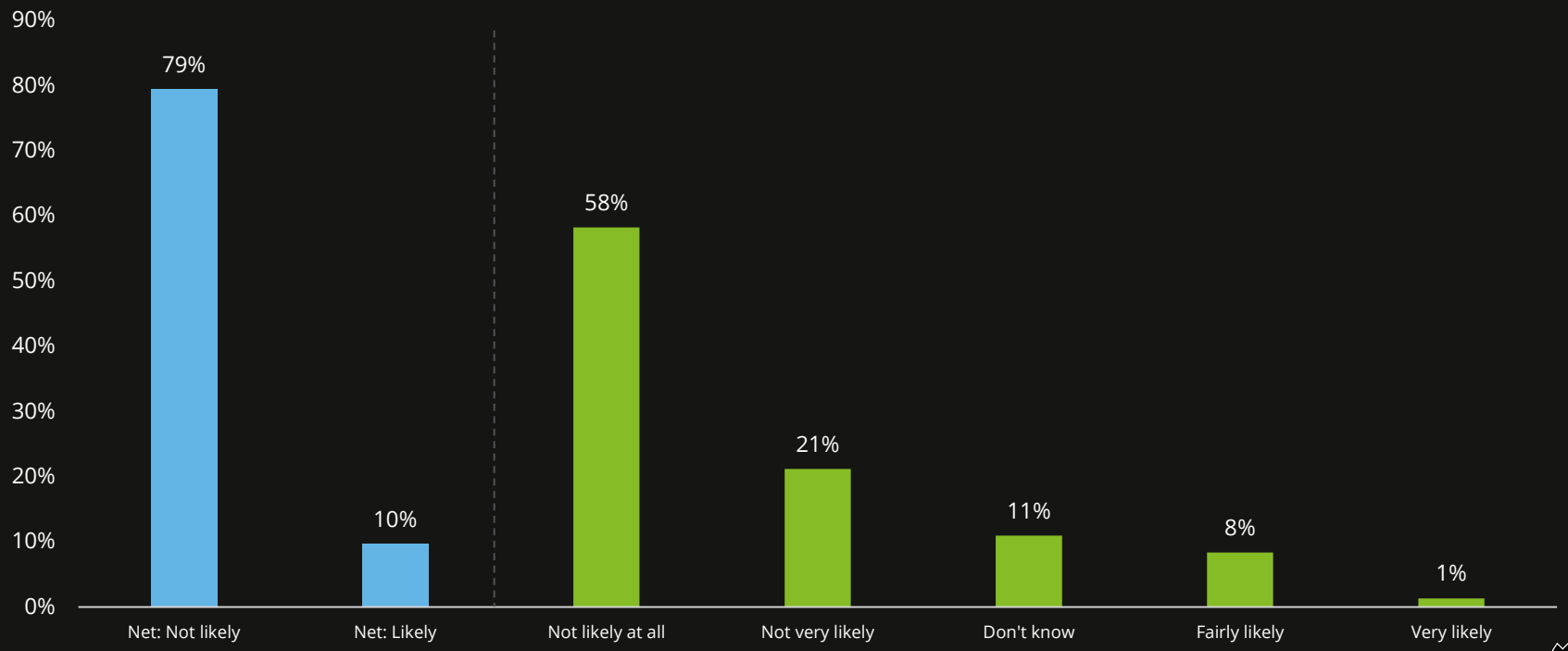
- Be transparent about the existence of any commission received from *InsurHome*.
- As *MyNewBank* only gives guidance here and does not recommend a specific provider or product, it will need to make this clear to Sarah, and highlight that the marketplace only brings together a few select providers and that she could also shop around.
- Implement controls to maintain the integrity, accuracy and completeness of the data transferred to *InsurHome*.
- Ensure the API is compliant with PSD2. Ensure data transfers are limited to what is required and compliant with GDPR.

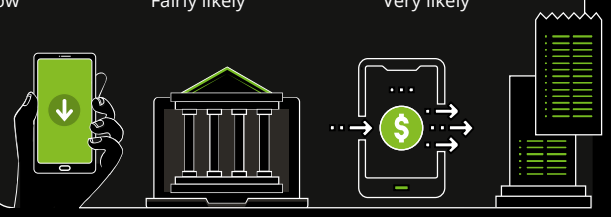
InsurHome

- Be registered as an AISP under PSD2.
- Before using Sarah's data to calculate Sarah's premium, *InsurHome* will need to conduct a DPIA, obtain her consent, build-in privacy by design and default within the algorithm, and ensure the algorithm only collects and processes the minimum amount of data necessary. The firms will need to explain why and how her the security device data will be used and how it may affect future premiums.
- Ensure the algorithm does not rely on data that implicitly or explicitly relates to Sarah's "protected characteristics" (e.g. age race, religion, disability, etc) to calculate her premium.
- Ensure that the insurance policy is consistent with Sarah's demands and needs, based on information obtained from her.
- Understand whether its business model is dependent on cross-subsidisation from the sale of the security device as this may drive poor outcomes for customers. Give access to a human adviser whenever Sarah requests it. Ensure processes and controls work appropriately to permit timely handovers.
- Ensure quality, accuracy and relevance of API data received from Sarah, and *MyNewBank*, on which the nudge and then the advised sale are based.
- Apply robust systems and controls to prevent any loss or theft of Sarah's collected data by the home security device.

A large majority of the people surveyed responded negatively to sharing banking data with an insurance company.

How likely, if at all, would you be to allow an insurance company to access your banking data through your budget management or banking App?





Step 4

Sarah loses her job and needs to review her entire portfolio

Background

Sarah's firm has restructured, and she is made redundant.

She has found a temporary zero hour contract (variable income). So far, she has managed to service her mortgage, but she has delayed paying some of her other bills, and has been increasingly using her Bank A and Bank B credit cards for day-to-day payments.

The next month, ***MyNewBank*** notices, through the API that connects it with Bank A, that Sarah's salary income has become variable and that she has increased her usage of her credit cards. ***MyNewBank*** has deployed AI tools to analyse customer behaviours and identify potential vulnerability: a natural language processing solution to listen to calls, and a chatbot where customers can ask questions (the feed is recorded on a continuous basis, and accessible by human advisers).

Sarah's perspective

Opportunities

- The AI tool is a way for Sarah's vulnerability to be picked up more rapidly and, if deemed necessary, activate the forbearance process for her mortgage.

Concerns

- Sarah may want to speak to a human adviser rather than a chatbot to discuss her situation.

Regulatory hotspots

Conduct

- Transparency and communication about the use of AI to analyse customer behaviour.
- Identification of vulnerability.
- Forbearance.

Financial crime

- Unusual customer/transactional behaviours to be identified across providers.

Data privacy

- Data minimisation, transparency and communication.

Digital risks

- Governance of AI.
- Customer satisfaction and monitoring of outcomes of AI solutions – ability to flag vulnerability.

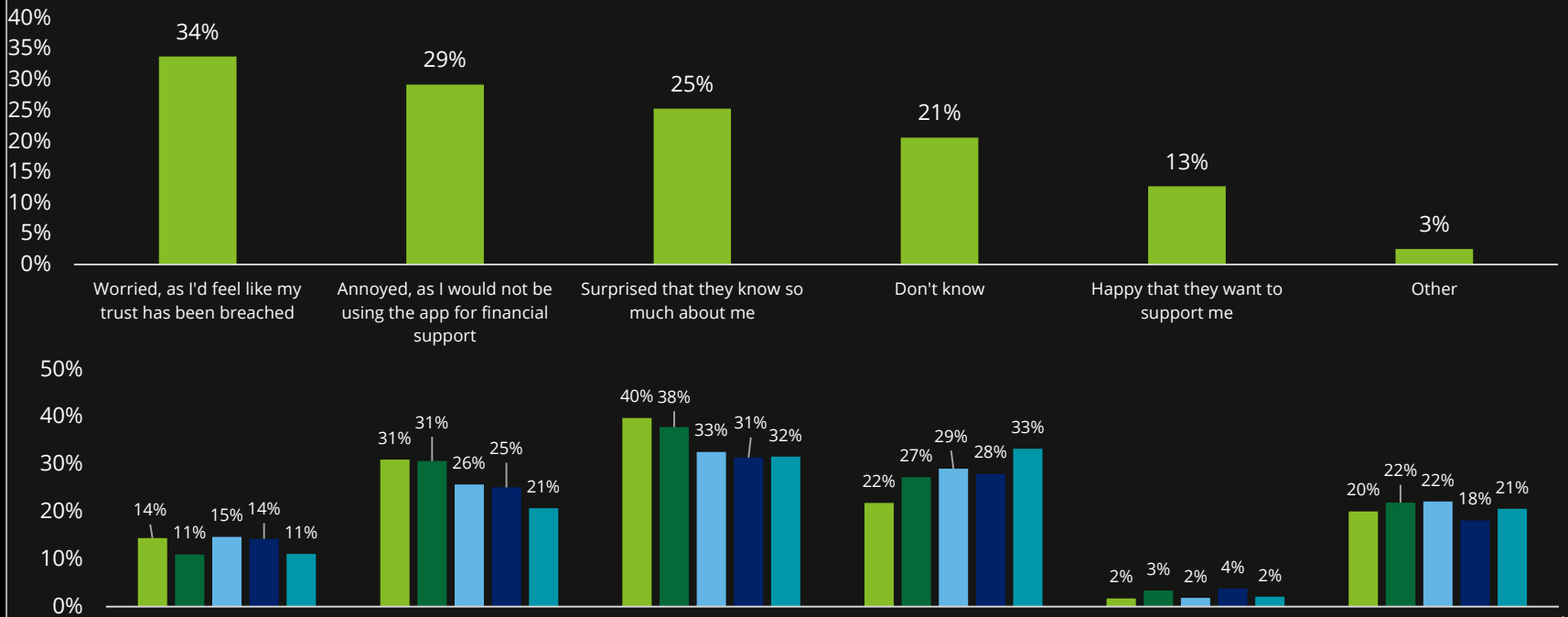
Considerations for firms

MyNewBank

- Perform DPIA for the processing of Sarah's data through AI solutions to flag potential signs of vulnerability. Secure and regularly renew Sarah's consent, be transparent about the processing of her personal data and explain how the AI solution is used to track and collect her data. Keep the data for no longer than required, and only collect the minimum amount of data necessary.
- Ensure that its various customer communication channels (e.g. chatbot) are able to detect indicators of Sarah's financial stress and to report it to the relevant skilled staff in a timely manner to allow them to explore options to support Sarah including forbearance options, if necessary.
- Ensure that it keeps a record of all feeds and information collected by various channels, to inform the relevant staff about Sarah's vulnerability and, if deemed necessary (i.e. if she becomes unable to service her mortgage), offer her the best forbearance option adapted to her situation and needs.

During periods of vulnerability, the survey revealed that people would be worried, annoyed or surprised if the budget management App or another bank that has access to their main banking data, proactively reached out to them to discuss changes in their income.

If suddenly your income pattern becomes more variable (e.g. if you were to move from full time work to temporary shift work)...Which, if any, of the following statements describes how you would feel if either your budget management App or your new digital bank were to contact you to discuss this change?*



* Survey participants could select more than one answer.

Authors

Morgane Fouché
Assistant Manager
EMEA Centre for Regulatory Strategy
mfouche@deloitte.co.uk

Valeria Gallo
Manager
EMEA Centre for Regulatory Strategy
vgallo@deloitte.co.uk

Key contributors

Tom Kohler
Director
Risk Advisory
tkohler@deloitte.co.uk

Nicola L Vincent
Director
Risk Advisory
nivincent@deloitte.co.uk

Tom Bigham
Director
Risk Advisory
tbigham@deloitte.co.uk

Daniel Apple
Director
Financial Advisory (Financial crime)
dapple@deloitte.co.uk

Steven J Bailey
Director
Risk Advisory
sjbailey@deloitte.co.uk

Matt Papasavva
Associate Director
Risk Advisory
mpapasavva@deloitte.co.uk

Orla Hurst
Senior Manager
EMEA Centre for Regulatory Strategy
ohurst@deloitte.co.uk

Contacts Luxembourg

Roland Bastin
Partner – Risk Advisory
rbastin@deloitte.lu

Laurent Berliner
Partner - EMEA FSI Risk Advisory Leader
lberliner@deloitte.lu

Eric Collard
Partner – Risk Advisory
ecollard@deloitte.lu

Pascal Eber
Partner - Operations Excellence & Human Capital
peber@deloitte.lu

Thierry Flamand
Partner – Insurance Leader
tflamand@deloitte.lu

Francois Kim Huge
Partner – RegTech Leader
fkhuge@deloitte.lu

Stephane Hurtaud
Partner – Risk Advisory
shurtaud@deloitte.lu

Patrick Laurent
Partner | Technology & Innovation Leader
palaurent@deloitte.lu

Jean Pierre Maissin
Partner - EMEA FSI Analytics Leader
jpmaissin@deloitte.lu

Michael Martin
Partner – Risk Advisory
michamartin@deloitte.lu

Pascal Martino
Partner – Banking Leader & Digital co-Leader
pamartino@deloitte.lu

Jean Philippe Peters
Partner – Risk Advisory
jppeters@deloitte.lu

Simon Ramos
Partner – IM Advisory & Consulting Leader
siramos@deloitte.lu

Ronan Vander Elst
Partner – Deloitte Digital co-Leader
rvanderelst@deloitte.lu

Deloitte.