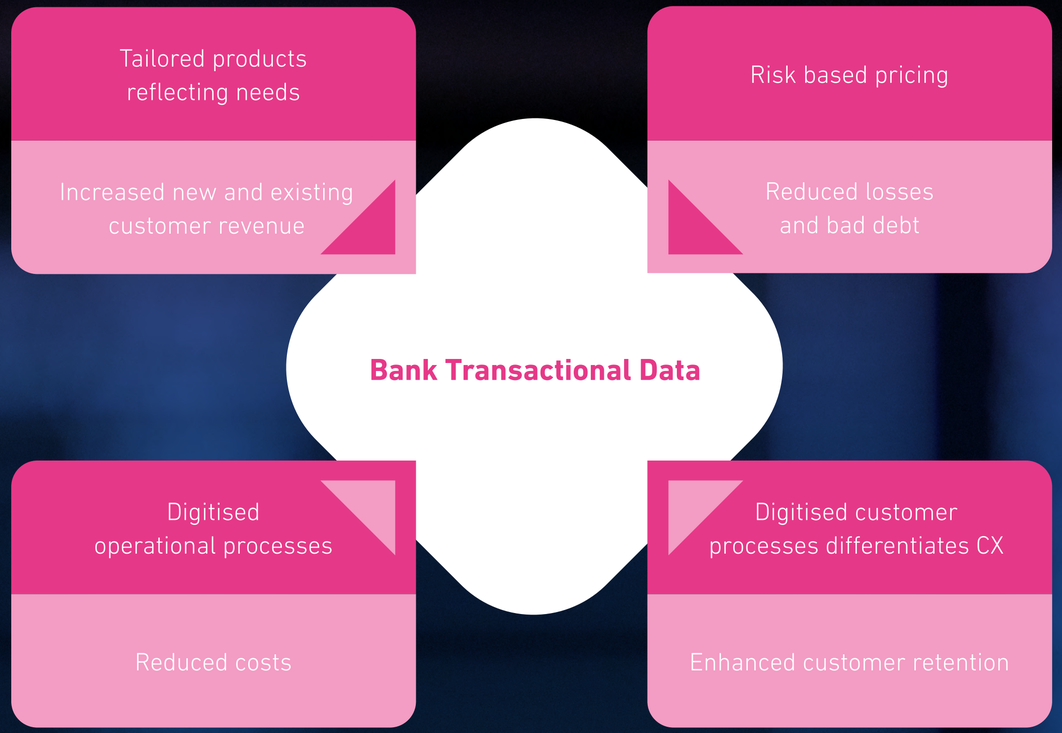
Trust, Consent and Value Exchange

Spanish Open Banking Insights

experian®

The availability of customer-consented Bank transactional data is a gamechanger. It allows businesses to understand customers' finances, risks, preferences and behaviours better than ever before.



The availability of customer-consented Bank transactional data is a gamechanger. It allows businesses to understand customers' finances, risks, preferences and behaviours better than ever before.

These insights create significant value from the perspectives of commercial strategy, risk assessment and digital transformation.

They enable the widening of product eligibility rules and more accurate personalisation to help drive revenue. They also enable these products to be more accurately risk-adjusted to help reduce losses and bad debt. Finally, they enable increased digitalisation of both customer-facing and internal processes. This delivers a highly positive and differentiated customer experience, backed by low-cost automated operational processes.

The combined effect of these factors on revenue, profitability, margin and shareholder value means that the strategic adoption of Open Banking has become essential for many businesses.

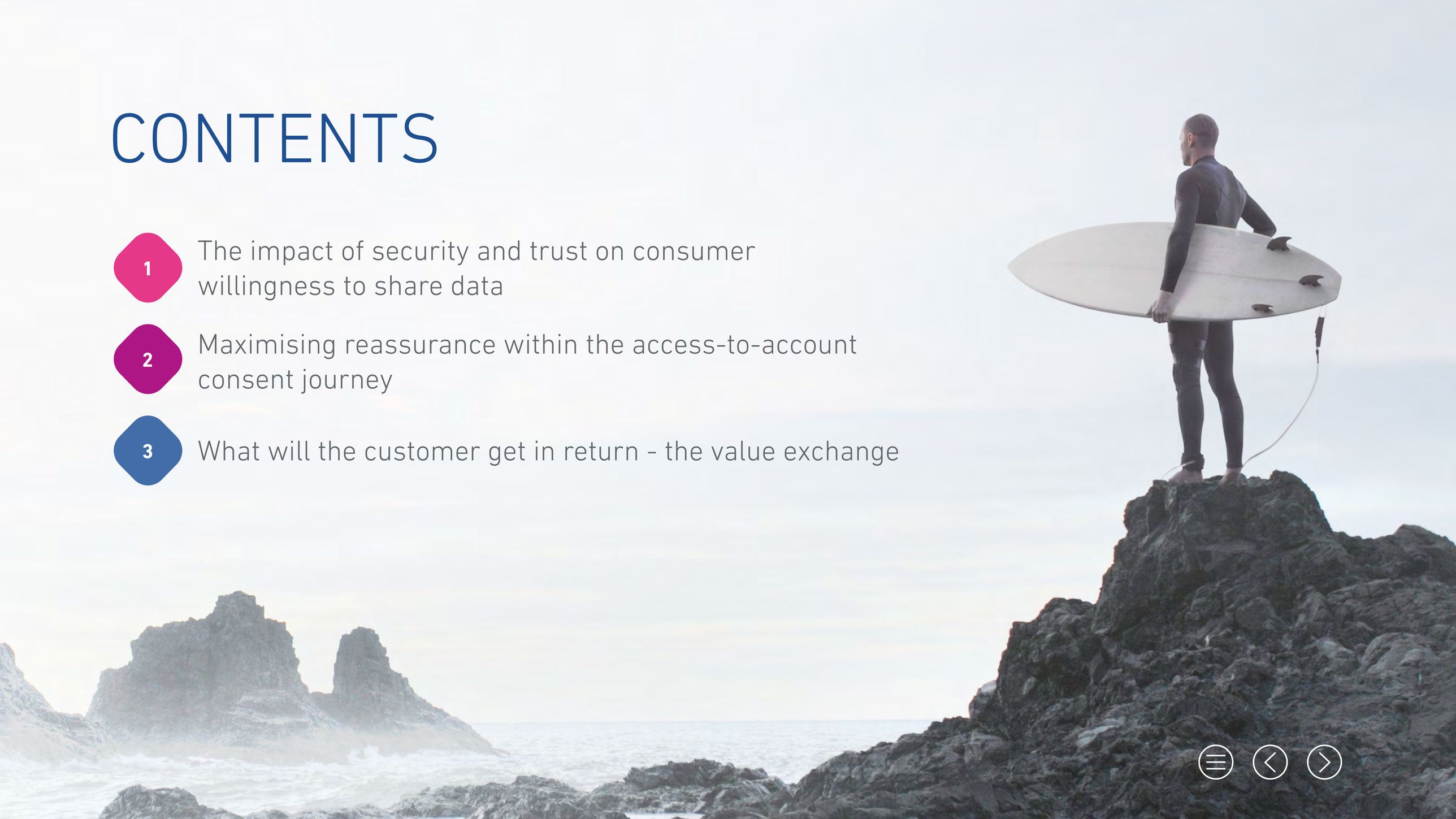
Closely aligned customer, commercial, operational, risk and financial strategies are vital, but the starting point is to ensure that the organisation can successfully obtain customer consent to access their financial data.

With this in mind, our research reveals that nearly half of senior executives at Spanish Banks and Telcos say that they are worried about consumer consent for Open Banking services.[1]

In this whitepaper, we explore the nature of consent and how to make it as compelling for the customer – in terms of maximising feelings of reassurance, trust and value.

[1] A commissioned study conducted by Forrester Consulting on behalf of Experian in August 2022, based on 104 senior executives at Spanish Banks and Telecommunications businesses.

CONTENTS

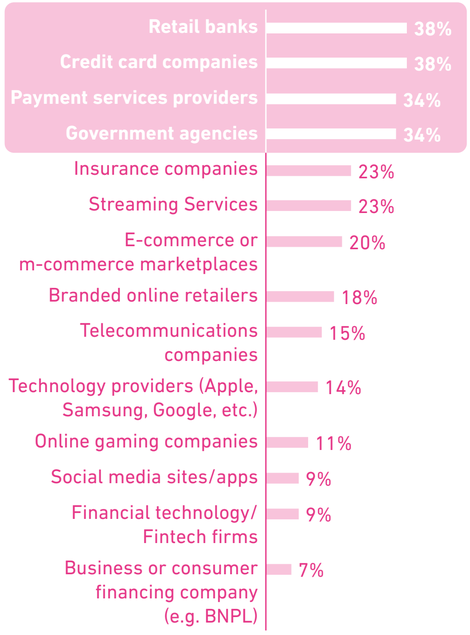


1

SECURITY AND TRUST ARE CRITICAL TO CONSUMER WILLINGNESS TO SHARE DATA

Over recent years consumers have become increasingly aware of the value of their personal data. This has resulted in an increased sense of empowerment and an expectation that they should be given something in return for allowing access to their data. Experian's Spanish research last year revealed that 68% of consumers had already been willing to share their personal data with online businesses and the majority of these could identify a benefit from having done.[2]

Spanish Consumer confidence in organisations' ability to protect and secure their personal data



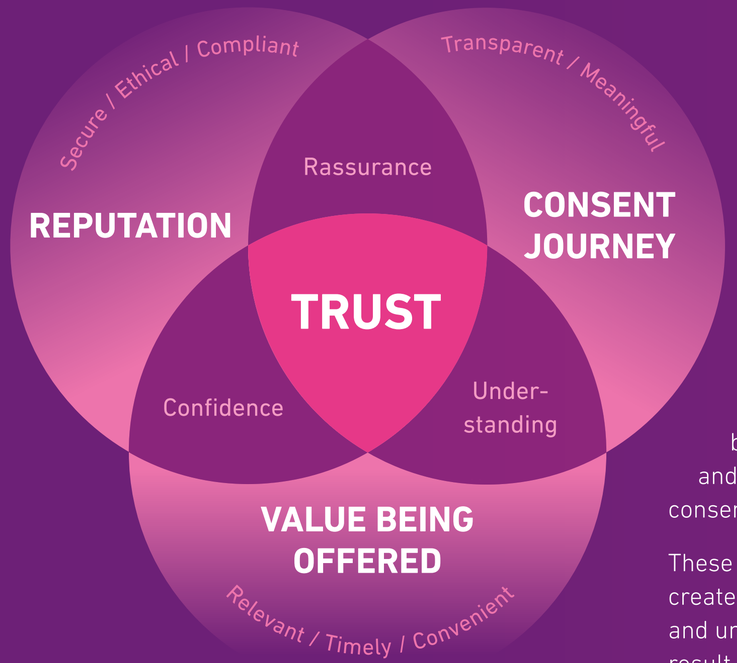
Trust is the critical foundation on which a value exchange is built

Our research also found that Spanish consumers have experienced a high exposure to fraud, and that they prioritise security and privacy far above all other factors within their online experience. They only trust those businesses in which they have confidence in their ability to safeguard data and privacy.

The top four types of organisations viewed most favourably in this regard are retail banks (38%), credit card companies (38%), payment services providers (34%) and government agencies (34%).

Percentages reflect responses from 151 Spanish consumers to the question "Please rank order the following businesses with your top 5, from the one you are most confident in protecting and securing your personal data, to the one you are least confident", Experian wave 2 global consumer research, June 2022.

[2] Experian Spanish consumer research included within global research wave 2, June 2022, base 151 Spanish consumers.



Deconstructing Trust

Given consumers' security concerns, trust is the critical factor in determining the willingness of consumers to share their data. No matter how strong the value offer may be, if they don't trust the provider making the offer, are they really going to allow access to highly personal banking data?

Trust is of course a "feeling" and as such, it is hard to define without deconstructing it. In this section, we will explore the elements that contribute towards creating and sustaining trust.

Three important drivers of trust are the organisation's brand reputation, the nature of the value offer that will be exchanged for data access consent, and the experience delivered by the consent journey.

These are all interlinked and together should create the feelings of reassurance, confidence and understanding which together should result in the decision to proceed.

Brand reputation - Consumer awareness is changing but trust is difficult to earn

One of the main drivers behind the second Payment Services Directive (PSD2) was to help drive innovation and increase customer value and choice. As a result, an ecosystem of established players and new Fintechs has developed. For all of these participants, trust and transparency are relevant.

The established Banks and Financial Services providers have both brand and consumer usage on their side. Both of these factors have a significant impact on consumer confidence levels in the ability of these organisations to protect and secure personal data.

The two things that Fintechs lacked in the past were consumer awareness and scale. This is changing dramatically and as awareness has increased so has adoption (which was accelerated by the impact of the pandemic.[3]

However, consumer use of Fintechs has been primarily based on convenience and customer experience rather than trust - as is evident from the position of Fintech in the consumer research findings summary above. This is changing and for Fintechs to gain consumer trust it is important that they increase transparency regarding how they access, use and store customer data.

[3] For more information about the significant inroads that Fintech have made into consumer lending in North America refer to Experian Whitepaper Fintech Trends – Unsecured Personal Loans December 2021.

The Value Offer

The value offer that is made to the customer should be sufficiently compelling that its perceived value outweighs any remaining concerns about security, protection and brand. In section 3 we explore this in more detail and the role of need, timeliness and convenience in maximising perception.

A transparent and meaningful consent experience

An important dimension of consumer trust is the level of transparency shown by the business in terms of data collection. Amongst the specific businesses they deal with online, only

52%

of Spanish consumers can identify specific businesses that are clearly better at communicating how they capture and use personal data.

Whilst a similar proportion (45%) believe that organisations are getting better regarding this important aspect of communication, it seems reasonable to conclude that Spanish businesses in general still need to improve in this area..[4]

The PSD2 regulations require that full transparency is provided to the user regarding how long the consent is for – in other words whether it is once-off or recurring.

They also require full transparency of the historical period over which transactional data can be viewed.

In the case of once-off consent, this can enable transactional data of up to 12 months to be accessed.

However, as well as being transparent, clear and understandable, the consent experience also has to be meaningful and engaging. For consent to be valid the consumer should be encouraged to take time to understand what it actually means rather than in any way encouraging the consumer to simply click, tick and move on.

Before data is shared it is important that customers understand the following:

- Why and how their data needs to be shared
- How their data will be protected
- How their data will be used
- How they will be able to manage their data
- What consent actually means in terms of purpose, process, duration and revocation

These elements are covered within the design of the access-to-account consent journey.

ONCE-OFF CONSENT

The user agrees to allow a third party to access their account (or accounts) on a once-off basis, which will then be automatically revoked once the data share has been completed.

RECURRING CONSENT

The user agrees to enable a third party to access their account(s) for up to four times a day over a 90-day period. After the 90 days have elapsed the consent is revoked, and the user will need to reconfirm in order to enable further data sharing.

[4] Experian Spanish consumer research included within global research wave 2, June 2022, base 151 Spanish consumers.

[5] EBA have issued a recommendation that this be extended up to 24 months.

2

MAXIMISING REASSURANCE WITHIN THE ACCESS - TO - ACCOUNT CONSENT JOURNEY

In order to ensure the delivery of the required experiential outcomes of reassurance, confidence and understanding, the access-to-account customer journey should be designed holistically even though it will require the customer to move between separate environments.

The user will move between the organisation with whom they are doing business (in other words the provider or “host” of the value offer), the third-party provider(s) of the data acquisition and associated analytical services, and the consumer’s Bank.

At the start of the journey, the role of each of these actors needs to be made very clear to the customer with the handoffs between them being both secure and clearly signposted as the customer travels along it.

Customer consent journey

“Host” organisation making value offer

PSD2 Account Information Service Provider (AISP)

Customer’s bank

Experian's best practice approach to journey design

Within the account access consent journey, Experian is a regulated Account Information Service Provider[6] (AISP). Our role is to enable the data transfer to happen and then provide analytical services that can be used by the host within their value offer. In performing these services, Experian is a data processor in accordance with the GDPR.

Our access-to-account consent journey reflects proven best practices acquired within the UK where we have been providing similar services since 2017.

We recommend that the host organisation making the value offer to the consumer provides an initial high-level explanation to reassure the customer regarding security and protection.

This is best done by highlighting the combination of the highly regulated nature of Open Banking, the management of the journey by a specifically regulated specialist data processor (the AISP) and the use of the Bank's own comprehensive security measures. An example of the initial explanation is shown on the right.

After this initial explanation, the customer is sent a web link which will take them to a dedicated secure Experian Open Banking app. Here the user will see a very clear explanation of what their consent will mean and their privacy rights.

> "Our approach is based on obtaining once-off consent from the user rather than recurring 90-day consent."

Example initial explanation of the account access consent process

Your protection within this process is critical and as a result this process is highly regulated and can only be offered a suitably licensed 3rd party.

We have chosen Experian to provide this service and it can be accessed through a secure link that we are sending you.

This link will take you though a clearly structured journey which will enable you to select your bank and then provide it with your consent to directly share your data with Experian.

This will involve you being transferred to your bank where you should log-in as you would with on line banking. Your log in details, passwords and credentials are neither visible nor accessible in any way by Experian.

Having confirmed your consent to the transfer, Experian will then conduct specialist financial analysis which will enable us to assess your application in real time and share the result with you.

[6] Our regulated entity is Experian Ireland Limited which is an Account Information Service Provider authorised for the provision of account information services and directly regulated by the Central Bank of Ireland.

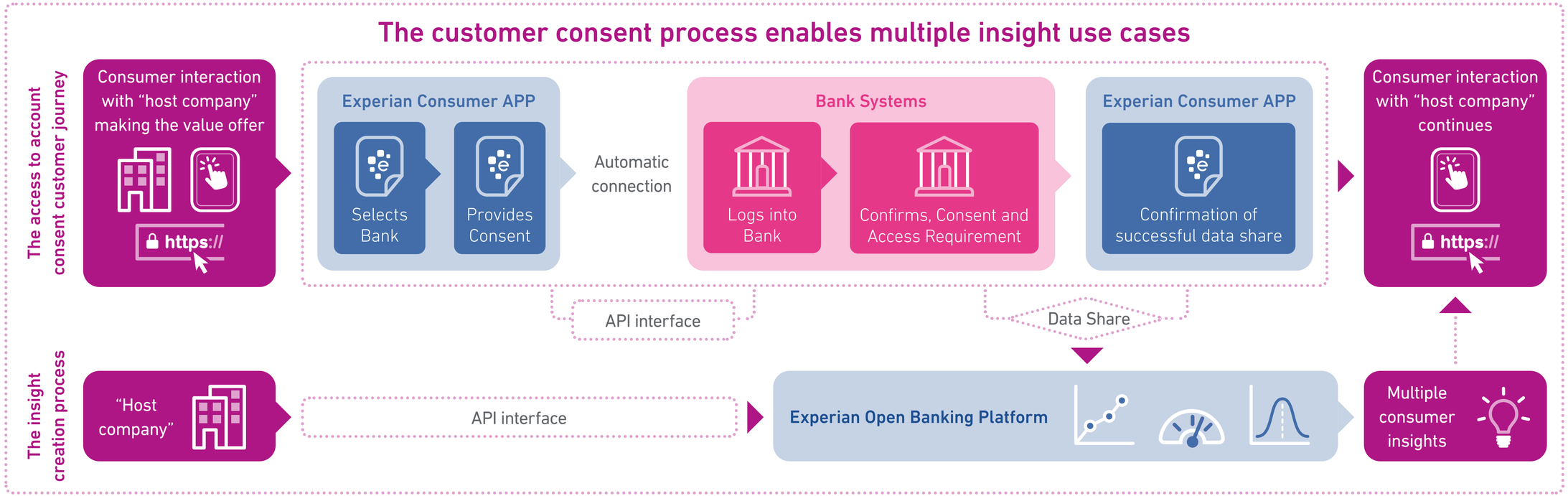
This approach is more consistent with the provision of an immediate and timely value exchange - such as to increase the likelihood of acceptance of an application for credit. It also enables a far more meaningful assessment to be made of historical debt over a 12-month rather than a 3-month period. In addition, once-off consent mitigates potential problems regarding user trust as the API stays open for just 24 hours, which is enough to calculate the output, before being automatically revoked.

Having selected their Bank/s and account/s, the user then moves into the Authentication Stage where they are redirected to their Bank for the next part of the consent journey.

Here, the user enters their banking identity credentials for verification and is again assured that these credentials cannot be accessed by the third-party provider (Experian). In accordance with the PSD2 regulations, the verification process has to meet the requirements for Strong Customer Authentication (SCA). Typically, this will mean that the user is following the same security processes that they are already familiar with when they log into their Bank. This familiarity should provide a further level of reassurance.

The final stage is the formal authorisation by the user to the Bank. Here the Bank explains what information has been requested and directly seeks the user's authorisation to transfer the data to the third-party provider (Experian as AISP).

At this stage, the user is returned to the Experian app where they receive confirmation that the data share has been successful.



The fact that the user is moving between these environments is regarded as creating "positive friction." Whilst user friction commonly seen as something that damages the experience and increases the risk of abandonment, researchers have found that where important actions are being taken, certain types of friction can have a positive effect on the users' understanding.[7]

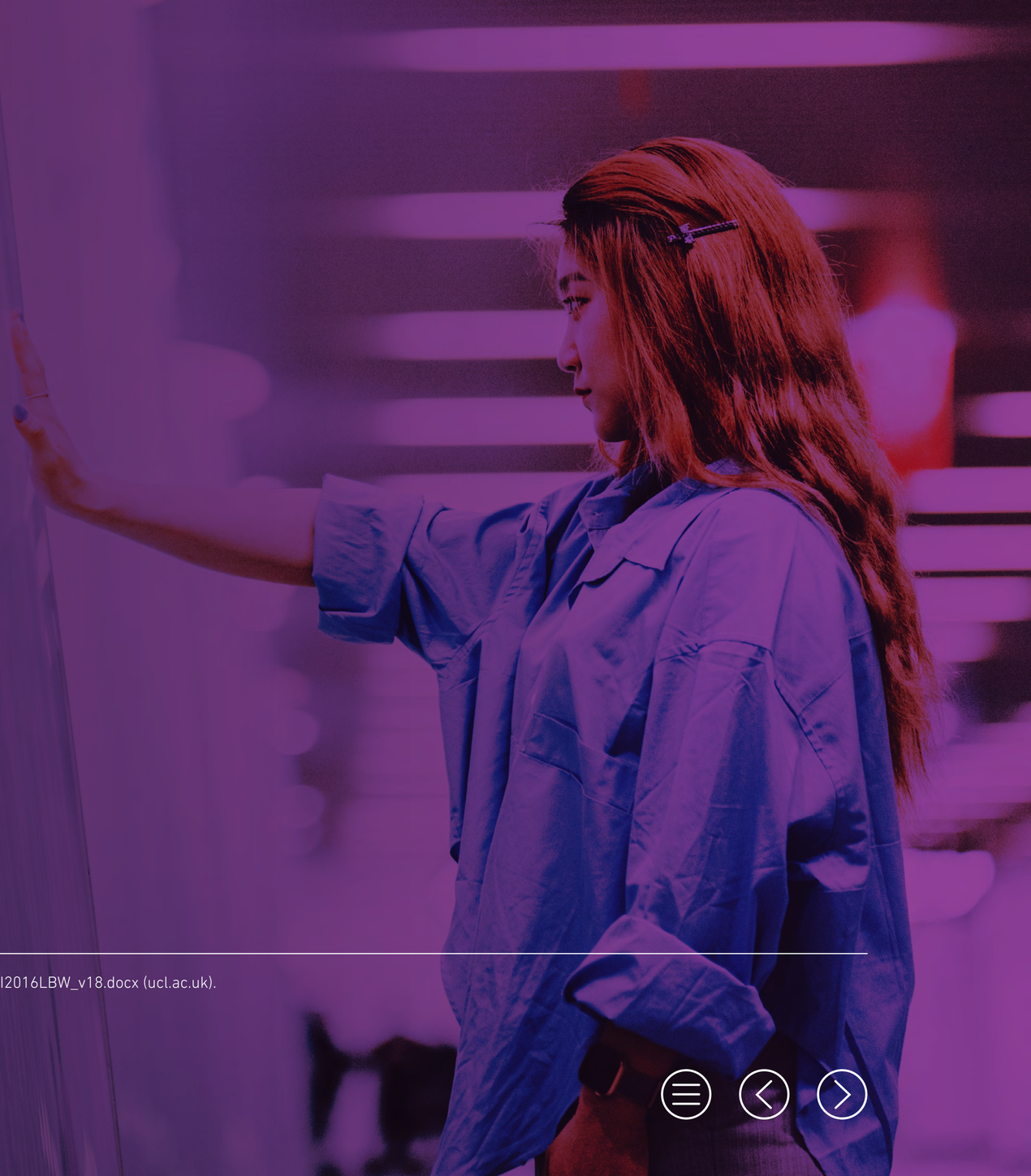
The friction associated with moving between the environments within the access-to-account journey is a good example of this. Provided that the user has been given a clear explanation of what the journey and process will consist of, the positive friction will help make the user more aware and mindful of the exact nature and importance of their actions. As such it should help ensure maximum understanding which will help provide further reassurance and a sense of security and protection.

Strong customer authentication and reassurance of active identity verification

Another form of positive friction that can have a reinforcing impact on user feelings of security is the use of physical biometrics within the SCA process. Requiring the customer to physically do something is a great way of demonstrating the provider's commitment to security.

Our Spanish consumer research[8] revealed that the use of physical biometrics within authentication and verification processes has the highest positive impact on customer feelings of security.

Having completed the account consent customer journey, the user then returns to the host organisation. They then receive the details of the value offer that the host considers to be most appropriate based on the results of Experian's analysis of their transactional data.



[7] "Design Frictions for Mindful Interactions: The Case for Micro boundaries" - University College London, 2016 Design Frictions_CHI2016LBW_v18.docx (ucl.ac.uk).

[8] Experian Spanish consumer research included within global research wave 2, June 2022, base 151 Spanish consumers.

3

WHAT WILL THE CUSTOMER GET IN RETURN – THE VALUE EXCHANGE

Spanish consumers were included in a global study conducted last summer.[9] This investigated how willing they would be to "share their personal data with online businesses". No reference was made to personal banking data.

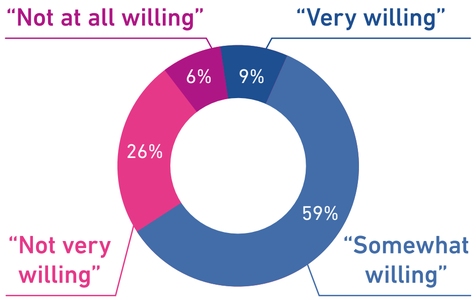
This revealed that 68% of Spanish consumers described themselves as being either "very willing" or "somewhat willing".

A wider study of Spanish consumers formed part of our exclusive Forrester research in August 2022.[10]

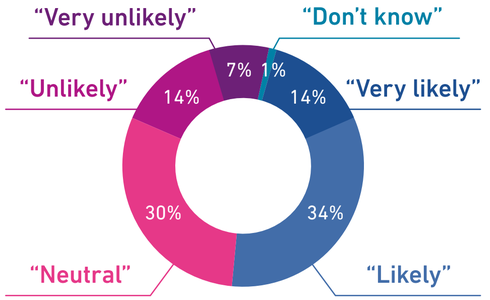
Unlike the earlier study, this made specific reference to allowing access to consumers' banking financial information and also allowed respondents to describe themselves as "neutral".

This revealed that 48% of Spaniards described themselves as being either "very likely" or "likely" to share their banking data, 30% neutral and 28% either "unlikely" or "very unlikely".

Willingness to "share personal data with online organisations"[9]



Willingness to "allow access to financial information from your bank to help with checks for online applications for finance products and services"[10]



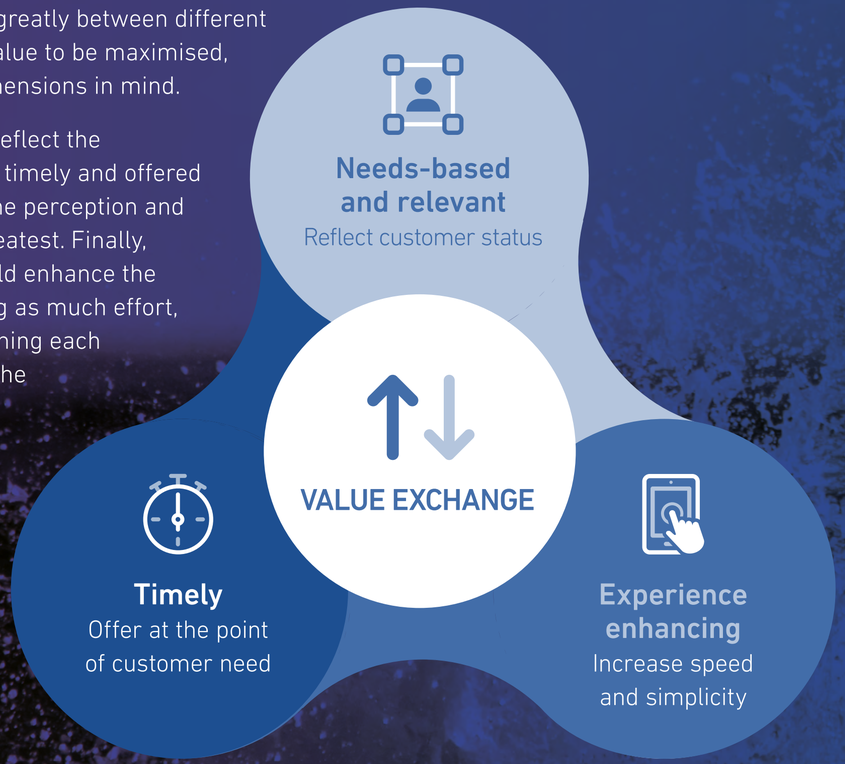
[9] Experian Spanish consumer research included within global research wave 2, June 2022, base 151 Spanish consumers.

[10] Research conducted by Forrester Consulting on behalf of Experian in August 2022, based on 527 Spanish consumers.

Assuming that the user receives the reassurance of security and protection (as previously outlined within this paper), converting this broad “willingness to share data” into the tangible action of providing consent will depend on the level of value that the user feels they will obtain in return.

Levels of user-perceived value will vary greatly between different value offers. In order for the perceived value to be maximised, offers should be designed with three dimensions in mind.

Firstly, the offer should be relevant and reflect the customers’ needs. Secondly, it should be timely and offered at the point of needs realisation where the perception and appreciation of the value will be at its greatest. Finally, the way the offer is made available should enhance the overall customer experience by removing as much effort, delay and complexity as possible. Combining each of these value dimensions will increase the likelihood of a positive response.



The table below illustrates three examples of customer value offers and how they potentially meet each of these three value criteria.

Value Offer	Needs-based and relevant	Enabling (Speed / Convenience)	Timely
Helping a new auto-finance customer complete their application faster.	Customer wants peace of mind to know they have successfully secured the car that they want.	Digital-first customer experience covering real-time identity verification, bank checking, affordability and credit risk assessment.	Offer complete end-to-end process at the point the customer has selected the car - this could be fully digital or hybrid face-to-face and digital within the car dealership.
Helping an existing credit customer manage the risk of default through a personalised and actionable payment plan.	Customer is showing signs of increased vulnerability.	Immediate access to personalised planning tools to create a revised payment plan.	Request for consent to access data at the point of observed delinquency. Timeliness maximises customer's perceived value, and increases the likelihood of a positive response.
Helping a potential new telco customer get access to a personalised offer quickly and effortlessly.	Customer is able to quickly acquire the phone they desire and access details of any personalised upgrade relating to its purchase at the point of sale.	Ability to fast-track order and acceptance without the requirement to visit a branch or produce additional ID verification documentation or conduct checking of IBAN bank details.	Request for consent at the point at which the customer views the product and as the enabler to access / unlock special terms or offers.

48%

As we have already seen from the Forrester research, 48% of Spaniards described themselves as being either "very likely" or "likely" to share their banking data. This response was based on an explanation of the concept of giving consent in return for a more attractive offer.

52%

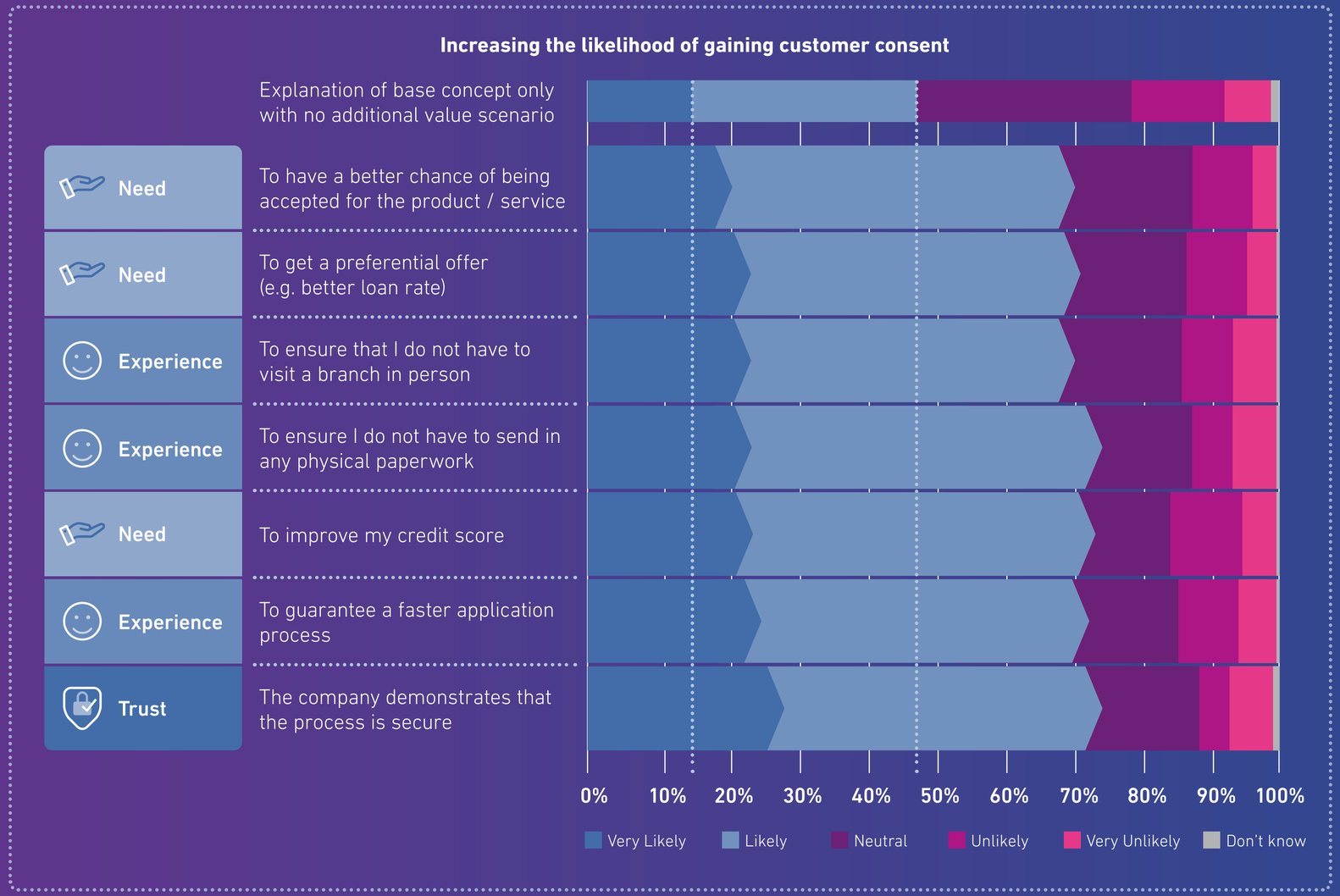
The 52% that did not initially respond favourably, were then asked seven supplementary questions – each of which referred to a different scenario based on differing types of value offers. The first six value offers reflected differing types of needs and convenience. The final scenario did not refer to a specific value offer but instead just referred to the company (host) being able to demonstrate that the process is secure.

The responses to each of these various scenarios led to a reduction in the number of consumers describing themselves as “neutral” and an increase in the number of positive responses.

The graph shows the combined effect of the initial explanation of the concept plus the impact of the supplementary question on the reduced consumer base (i.e., Those who responded as “neutral”, “unlikely” or “very unlikely”.

These research findings illustrate the impact that a clear explanation can have in maximising a positive response. It should be noted that security has the highest overall positive response level.

When the research was conducted, each of these 7 scenarios were offered independently of the others. By combining multiple aspects of need, convenience and trust to make the overall value offer as compelling as possible is likely to increase the probability of the customer providing their consent above the levels illustrated.



HOW WE CAN HELP YOU EXPLOIT THE POTENTIAL OF OPEN BANKING

Experian's access-to-account consent journey helps organisations create fully integrated, compelling and brand-enhancing experiences that increase feelings of trust and reassurance for both individual consumers and SMEs.

This is just one element of our Open Banking services which are delivered through our categorisation and consent platform. Following acquisition, the transactional data is data is then instantly categorised and analysed using powerful, continuously improving machine learning techniques based on sophisticated and highly localised data sets.

> "The resulting outputs provide client organisations with multiple actionable insights and the ability to verify important digital customer data, all of which we then help them to both consume and optimise."

Find out more

Check the Experian Academy and download details brochure to find out more about our Open Banking services.