OPEN BANKING

How to Guide: Consent Model

Part 2: User Experience

Open Banking Read/Write API
December 2017
Version 1.1

Contents

1 Introduction

The 'How to Guide: Consent Model, Part 1: Implementation' document describes how Account Servicing Payment Service Providers (ASPSPs) and Third Party Providers (TPPs) should implement the customer consent, authentication and authorisation steps (Consent Model) in the context of the Open Banking Read/Write API specifications.

This document should be read alongside, and provides insights and recommendations that could be used within the Consent Model based on extensive customer research. It will be useful for any participant (both ASPSPs and TPPs) wishing to provide products or services using Open Banking Read/Write APIs, and explains customer preferences on how the consent, authentication and authorisation steps should be communicated. Distinctions are made between how this should look for both TPPs and ASPSPs, and how each should manage the process.

It is recognised that Open Banking participants will introduce wide and varied customer services and experiences based on their individual business models. However, an underlying consistency of approach is recommended, particularly in the language used and presentation of the user interface. This is intended to enable participants to optimise the Open Banking user experience, and thus drive customer engagement, adoption and trust.

This document is supported by example customer journeys. Links to these are attached at the end of this document.

Open Banking therefore advises that TPPs and ASPSPs consider the recommendations made in this document and the associated example customer journeys in order to enable the delivery of a consistent and ubiquitous experience which will be familiar and trusted by customers.

All participants are solely responsible for their compliance with the relevant regulations applicable to their service offering and are encouraged to seek external legal advice. This document is purely advisory and does not in any way constitute legal advice.

2 The Consent, Authentication and Authorisation process

The customer research has shown that the initial reaction to Open Banking is one of caution. Granting TPPs access to an account in order to provide a service is sometimes seen as an unavoidable trade-off for the convenience of being able to use it. However, the customer research has also shown that where the TPP's product or service is seen as highly useful and beneficial, the associated perception of risk is reduced.

It is noted the control and choice the Open Banking Consent Model provides to customers is seen as a key benefit.

Account information, verbatim comments taken from the customer research:

"I feel OK with sharing information, I've got nothing to hide, I'm not a private person, so I don't mind. I get advertising that I'm interested in, like on Facebook, which is nice. But I guess there needs to be a balance"
37 Male, London, 'technophobe'

"I don't like giving any out if I can help it, obviously sometimes you can't help it, but I think these kind of things can be hacked. I understand financial information is more widely available, like credit checks etc. but I want to limit it being shared with any more people or entities if I can help it"
44 Male Birmingham, multi-banked

TPPs will create differentiated online experiences, via websites and mobile apps, for their customers - either consumers or SMEs - depending on their individual business model and the products or services they may be offering. However, common to these experiences is the three-stage process of consent, authentication and authorisation. The three stages can be summarised as follows:

- **Consent:** The process by which a PSU gives a TPP permission to approach their ASPSP in order that the TPP can be granted access to the PSU's account to provide a service to the PSU. This must be explicit, informed and time-bound
- **Authentication:** The process by which an ASPSP verifies the identity of the PSU, for example, when the PSU logs into their online account with the ASPSP
- **Authorisation:** The process by which the PSU confirms that the ASPSP may respond to the request from the TPP to whom the PSU has given consent

The three-step process described above is itself pertinent to building customer confidence and trust. Not only does it bring clarity to an unfamiliar process, but it also clarifies the individual roles of ASPSPs and TPPs in the customer's mind. Standardising this process as much as possible across TPPs and ASPSPs will create familiarity and confidence that will in turn encourage customer engagement and adoption.

Customers have a need for security balanced by a need for quick and simple processes. The approaches contained within this document are not intended to instruct how to implement the three-step process, but are rather intended to show how to optimise it, creating that balance between speed and demonstrable security. For implementation, participants should refer to the 'How to Guide: Consent Model, Part 1: Implementation' document.

2.1 Consent Step

Overall, the customer preference is to explicitly 'opt-in', avoiding the option of having to explicitly opt-out. It should also be made clear at the point of requesting consent how consent may be revoked by the customer.

Account Information Consent Request

The customer research has indicated that customers are concerned about the level of data a TPP might request, and whether it is absolutely necessary in order to provide the product or service. Therefore, TPPs should request the minimum data they require to provide the service to the customer. TPPs should explain for what purpose the data is needed and how it will be used. The use of standardised data clusters at the 'consent step' aids trust and familiarity and is discussed later in this document.

Payment Initiation Consent Request

It is recommended, that when consent is requested it explicitly mentions that:

- The payment is a single (one-off) payment and;
- It will be submitted to the bank for execution after authorisation

Combined Consent Request

A TPP may also want use the 'consent step' to request additional consents that may be needed to support their business model. This is discussed further in the 'Combined Consent' section later in this document.

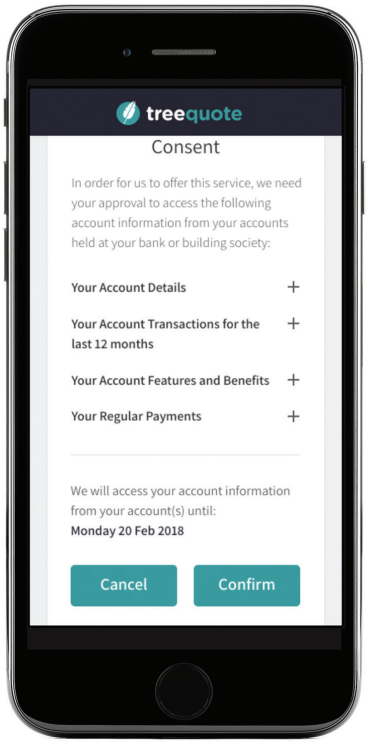


Figure 2.1
Consent Step - Account Information

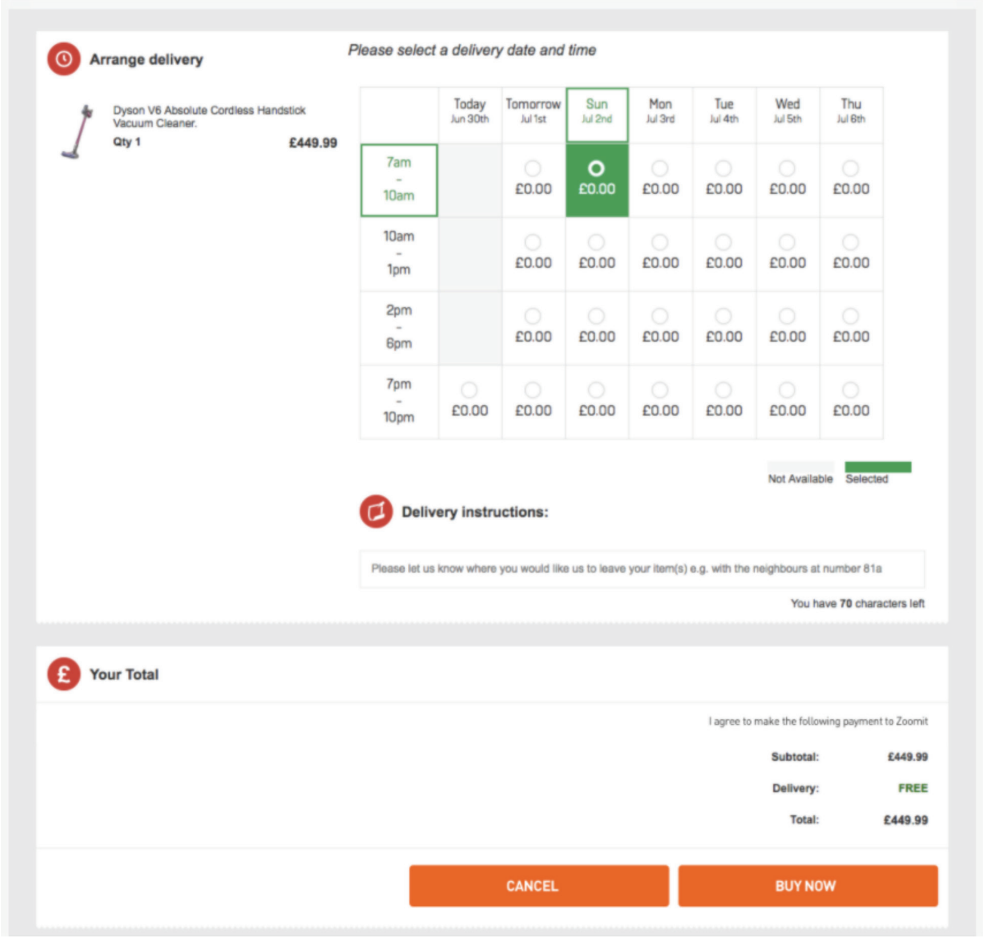


Figure 2.2 Consent Step - Payment Initiation

2.2 Authentication Step

The research has highlighted some suggestions to make this step more customer friendly:

- The presence of the ASPSP's branding and logo at this step are critical to engendering customer confidence and trust in the entire process
- The more distinctive the authentication step when compared to the TPP's online/mobile experience, the better
- The more consistent this ASPSP experience is to the online/mobile banking experience of the ASPSP, the more familiar it seems to the customer, therefore the greater the sense of security and trust it engenders
- Customers would welcome an authentication step which could be shortened without compromising safety and security of the process e.g. touch id etc
- Assurance was needed that no information being shared by the customer during this step is being made available to or is visible to the TPP

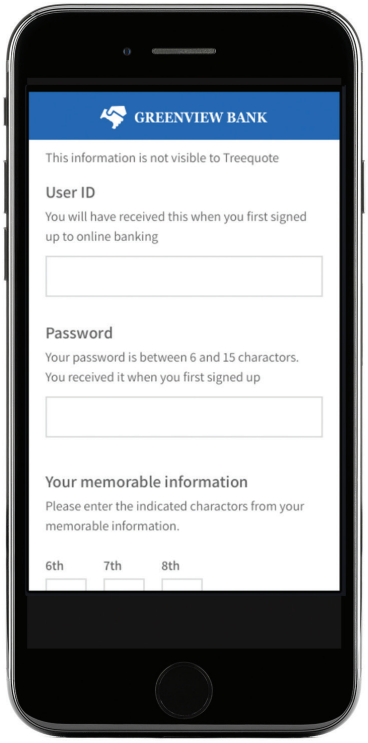


Figure 2.3 Authentication Step

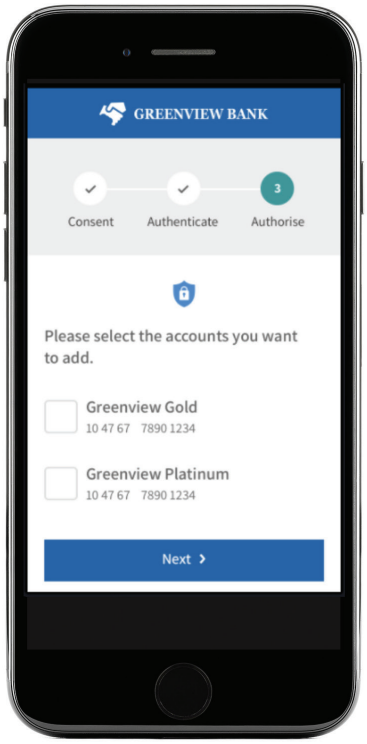


Figure 2.4
Authorisation step - Choose accounts

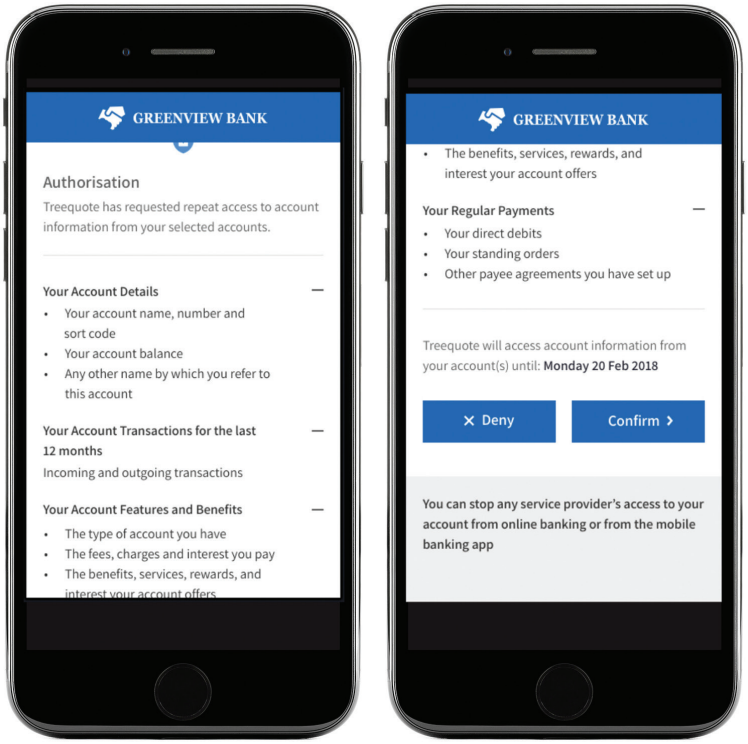


Figure 2.5 Authorisation step - Authorise the ASPSP

2.3 Authorisation Step

It should be made clear at the point of requesting authorisation how it may be revoked. The use of standardised data clusters during the authorisation request aids clarity, trust and familiarity. These are discussed later in this document.

Account Information Authorisation Request

The customer should not be able to de-select any of the data clusters presented as part of the authorisation request. However, they should be able to accept or reject the authorisation request in its entirety.

Payment Initiation Authorisation Request

The research has shown that an ability to view up-to-date account balance information, and being able to choose an account to pay with based on that information, is of benefit and of importance to the customer. However, the research also suggested that customers might also require some reassurance that their balances are not available or visible to the TPP. This could be achieved by including the following text - 'This information is not visible to [TPP name]'.

It is also recommended, that the authorisation requested explicitly mentions that:

- The payment is a single (one-off) payment and;
- It will be submitted by the ASPSP for execution after authorisation

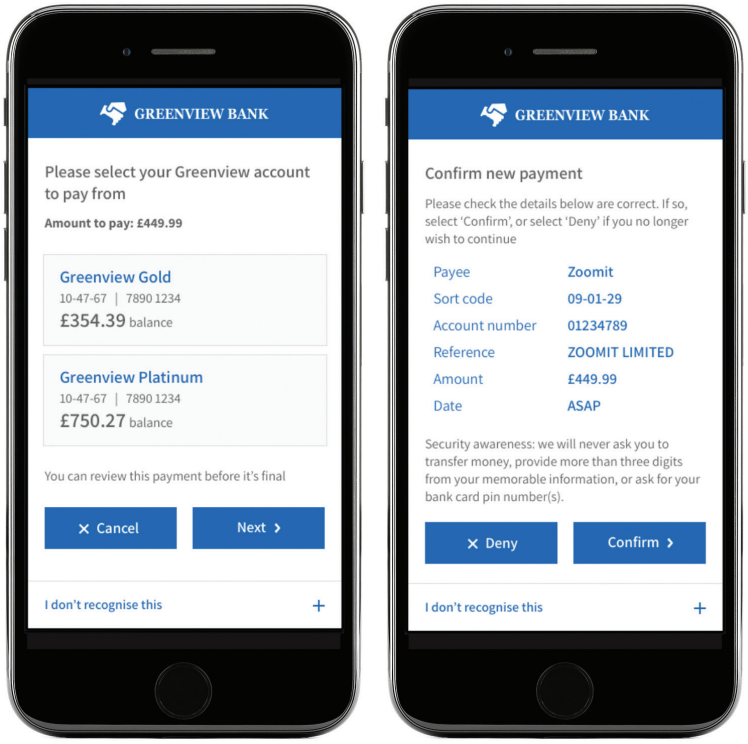


Figure 2.6 Authorisation Step

2.4 Standardising the Authorisation step

The experience of the 'consent step' on the various TPPs' websites/apps may vary, therefore, for most online customer journeys, the authorisation step will be the standardising factor and will bring clarity to what customers are agreeing to.

It is therefore important that the information displayed and the language used is standardised across ASPSPs, including the use of data clusters discussed later in this document.

The research revealed that consumer segments such as Technophiles, Financial Progressives and Early Adopters preferred a hybrid model, where the authentication and authorisation steps are combined. This was viewed as a good compromise between a customer understanding their actions and the simplicity/speed of the process. Although these segments represent a large minority (estimated to be around 20%), the majority of the Open Banking addressable market showed a clear preference for a separate authorisation step.

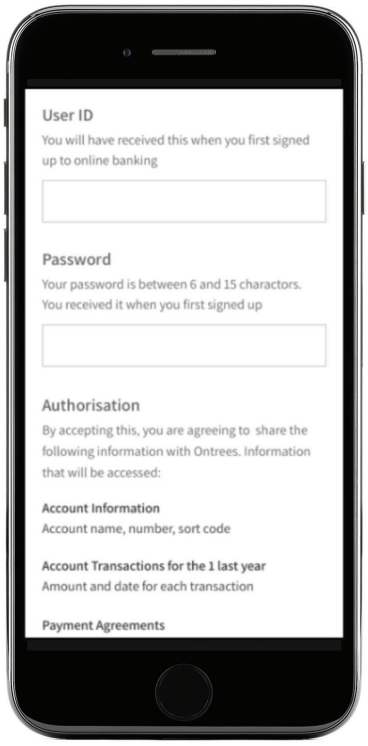


Figure 2.7
Combined Authentication & Authorisation Step

2.5 Redirection

At launch the Open Banking consent, authentication, and authorisation steps follow the redirection model. This is where the customer is redirected from the TPP's domain, to the ASPSP's domain for authentication and authorisation. Redirection screens will be presented between the 'consent' and the 'authentication steps', and then after the 'authorisation step' when the customer is redirected back to the TPP's domain.

The research has suggested that the redirection screens are a useful part of the process, providing customer trust. The following reasons are noted:

- They help customers navigate their online journey and inform them of what is going to happen next
- They help create a clear sense of separation between the TPP's domain and the ASPSP's domain.
- The research has suggested the messaging on the redirection screens serves to reassure the customer that they are in control, and helps engender trust. For example, customers will be more willing to trust the process if they feel there is a partner (TPP or ASPSP) on their side (use of 'we', 'our') that is known and reputable. In this sense, use of words that indicate that the customer is in control and taking the lead are key, as these are indications that the TPP or the ASPSP is working with or for the customer

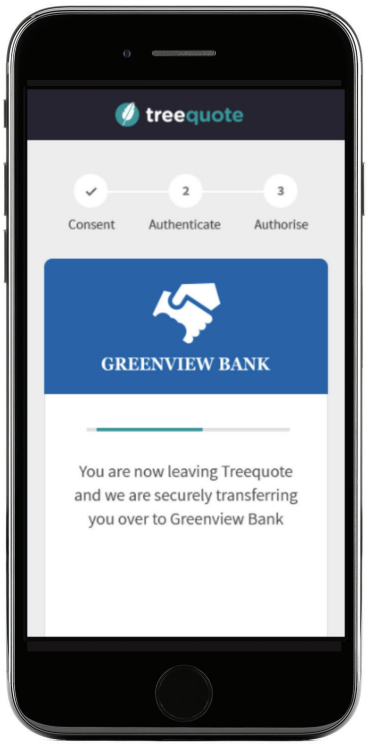


Figure 2.8
TPP to ASPSP redirection

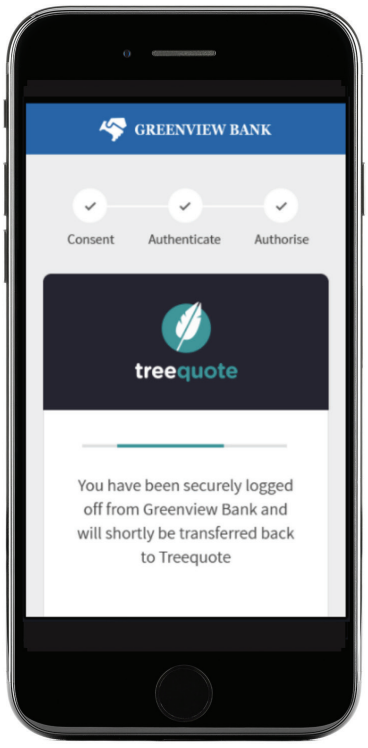


Figure 2.9
ASPSP to TPP redirection

2.6 Ongoing Authentication and Authorisation

When a customer gives consent to a TPP, who is an Account Information Service Provider (AISP), so that the AISP can access the customer's account information on an ongoing basis, the AISP will require the customer to authenticate themselves with their ASPSP and authorise the request at the ASPSP. Further detail is included in 'Consent Model Guidelines, Part 1 – Implementation document' (see Links).

The TPP would be required to notify the customer, whenever the customer needs to authenticate themselves and authorise the ASPSP, therefore the optimum point to request the customer to do so is as soon as the customer logs into the AISP's mobile app/ website. Figure 2.10 shows the language that could be used to position such a request with the customer.

The end-to-end ongoing authentication and authorisation journey in the 'Links' section demonstrates this. This is where the customer is using an account aggregation app called 'Treequote' to get a single view of their finances. Soon after they login, the customer is requested to authenticate themselves with their respective ASPSPs and authorise their ASPSP so that Treequote can access their account in order to provide the customer with an account information service, for example, a consolidated view of their finances.

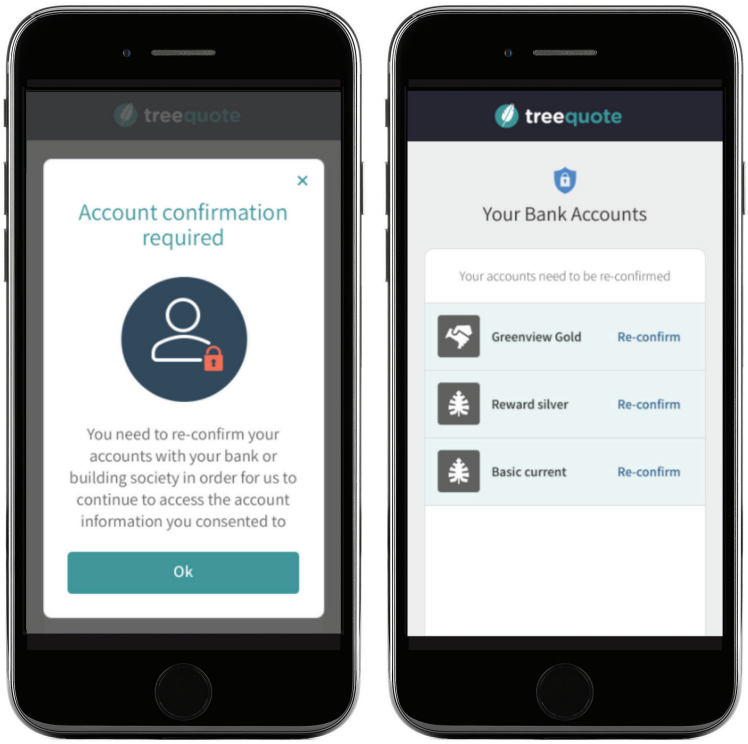


Figure 2.10 Authentication and authorisation request

3 Understanding Data Clusters & Permissions

3.1 What are Data Clusters?

When seeking consent to access customer data it is important to ensure that the customer clearly understands what they are consenting to. The Open Banking language research recommends that permissions can be grouped into four data clusters as shown below. For details on permissions, participants should refer to the 'How to Guide: Consent Model, Part 1: Implementation' document. In addition, the research has recommended descriptive text that is easily understood by customers for each permissions.

- **Cluster:** Your Account Details
- **Permission:** Account Basic: **Description:** *Any other name by which you refer to this account*
- **Permission:** Account Details: **Description:** *Your account name, number and sort code*
- **Permission:** Balances: **Description:** *Your account balance*

- **Cluster:** Your Regular Payments
- **Permission:** Beneficiaries Basic: **Description:** *Payee agreements you have set up*
- **Permission:** Beneficiaries Details: **Description:** *Details of Payee agreements you have set up*
- **Permission:** Standing Orders Basic: **Description:** *Your Standing Orders*
- **Permission:** Standing Order Details: **Description:** *Details of your Standing Order*
- **Permission:** Direct Debits: **Description:** *Your Direct Debits*

- **Cluster:** Your Account Transactions
- **Permission:** Transaction Basic Credits: **Description:** *Your incoming transactions*
- **Permission:** Transaction Basic Debits: **Description:** *Your Outgoing transactions*
- **Permission:** Transaction Detailed Credits: **Description:** *Details of your incoming transactions*
- **Permission:** Transaction Detailed Debits: **Description:** *Details of your outgoing transactions*

- **Cluster:** Your Account Features and Benefits
- **Permission:** Products

  Description: *The type of account you have*
  The fees, charges and interest you pay
  The benefits, services, rewards, and interest your account offers

Consent should be requested at the data cluster level, however the TPP should only request the minimum data under each cluster that is actually needed to provide the service. Find below the recommended mapping of data clusters and permissions.

Data Cluster Language	API End Points	Permissions	Permissions Language	Information Available
Your Account Details	Accounts	Accounts Basic	*Any other name by which you refer to this account*	Currency of the account, Nickname of account (E.g. 'Jakes Household account')
		Accounts Detailed	*Your account name, number and sort-code*	Account Name, Sort Code, Account Number, IBAN, Roll Number (used for Building Society)
	Balances	Balances	*Your account balance*	Amount, Currency, Credit/ Debit, Type of Balance, Date/ Time, Credit Line
Your Regular Payments	Beneficiaries	Beneficiaries Basic	*Payee agreements you have set up*	List of Beneficiaries
		Beneficiaries Detailed	*Details of Payee agreements you have set up*	Details of Beneficiaries account information (Name, Sort Code, Account)
	Standing Orders	Standing Order Basic	*Your Standing Orders*	SO Info, Frequency, Creditor Reference Info, First/Next/ Final Payment info
		Standing Order Detailed	*Details of your Standing Orders*	Details of Creditor Account Information (Name, Sort Code, Account)
	Direct Debits	Direct Debits	*Your Direct Debits*	Mandate info, Status, Name, Previous payment information,
Your Account Transactions	Transactions	Transactions Basic Credits	*Your incoming transactions*	Transaction Information on payments made into the customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Does not include information about the entity that made the payment.
		Transactions Basic Debits	*Your outgoing transactions*	Same as above, but for debits
		Transactions Detailed Credits	*Details of your incoming transactions*	Transaction Information on payments made into the customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Includes information about the entity that made the payment.
		Transactions Detailed Debits	*Details of your outgoing transactions*	Same as above, but for debits
Your Account Features and Benefits	Products	Product		Refers to customer account product details defined in the Open data API (the fees, charges, interest, benefits/rewards)

The data clusters and their naming conventions have been derived from customer research and have no bearing on the Open Banking API. The API only allows data requests at the permissions level. The next section shows some examples of how consent could be requested by TPPs at the data cluster level to request only the data that they need.

3.2 Using Data Clusters

Find below examples of some potential consent requests.

1. **Example of an Account Aggregator TPP that only shows daily Balances**

Your Account Details
- Your account balance

2. **Example of an Account Aggregator TPP that shows detailed account spending and income analysis**

Your Account Details
- Your account name, number and sort code
- Your account balance

Your Account Transactions
- Details of your incoming transactions
- Details of your outgoing transactions

3. **Example of an Account Aggregator TPP provides cash flow analytics and overdraft prevention alerts**

Your Account Details
- Your account name, number and sort code
- Your account balance

Your Regular Payments
- Details of your Standing Order
- Your direct debits

Your Account Transactions
- Details of your incoming transactions
- Details of your outgoing transactions

4 Consent communications and messaging

The research has suggested that vocabulary used within the three-step process is one of most important factors in creating customer trust. To enable customers to understand and trust the new functionality and services that Open Banking supports, it is recommended that a consistent messaging framework is used in the 'consent' and 'authorisation' steps.

The research has shown that customers feel more comfortable if they fully understand, in clear and concise language, where they are in the journey and what they are being asked to do.

To support this, Open Banking recommends that the following words or phrases are used appropriately by Open Banking participants.

When you are articulating to a customer what you are asking them to agree to, then it should be described as:

- 'Consent' for TPPs
- 'Authorisation' for ASPSPs
- 'Authentication' or 'verification' worked equally well for proving their identity

4.1 Third Party Providers

Customers need assurance upfront, even before they register with the TPP, that their data will not be shared without their permission. Therefore, upfront splash screens and landing pages should have wording to the effect of 'We will never share your financial information without your permission'.

Consistent use of language should be continued by Account Information Service Providers (AISP) or Payment Initiation Service Providers (PISP) when assisting the customer in choosing their ASPSP by showing:

- *Select your bank/building society*

As a reference to the choice the customer has in identifying their bank / building society and, once the customer has made their choice, a clear indication or reminder of your terms and conditions should be presented, followed by the consent request.

- *For details read our Terms & Conditions and Privacy Policy*

When you are referring to a customer's account, then the inclusion of a reference to bank or building society is clearly understood:

- *Your Bank/Building Society Account*
- *Add a Bank/Building Society Account*

For AISPs the account information request should be described as:

- *Granting access to your bank account (followed by the appropriate data clusters and timelines)*

For PISPs the payment initiation process should be described as:

- *Making a Payment (followed by the details of the payment, date of the payment, value, beneficiary, reference, whether the authorisation is a one-off and the charges for the service (if applicable))*

With the name of who the payment is being made to being referred to as:

- *Payee details/Beneficiary details (Payee is more recognisable to consumers)*

Consent requests for both AISPs and PISPs should show the period for which the customer has consented to e.g.

- *This access is valid until xx/xx/xxxx*
- *This is a one-time access requirement*
- *This request is for a period starting xx/xx/xxxx and ending xx/xx/xxxx*

When referring to frequency of access, use of the term 'repeat access' is the recommended approach. This was felt to be less invasive / casual than alternatives such as 'regular access' and less awkward than 'repeat download'.

After the specific details around the request have been displayed, explicit customer consent must be requested. This must be clearly understood, and the consent request should provide two simple, final choices of equal prominence ('Deny' and 'Confirm') to signify the consent agreement.

- *By clicking confirm you will be consenting to xxxxx to make this xxxxxx request to your bank for the above details*

The redirection of the customer from the TPP to the ASPSP is important as it signposts the customer's journey and provides guidance of what is going to happen next.

- *The phrase 'You are now leaving us and we are securely transferring you over to your bank/building society' is the preferred wording identified in customer research for the redirection screen.*

The research has shown that customers may have security concerns and a reduced sense of control when multiple TPPs are involved in servicing them. This is also true where consent needs to be requested by the customer facing TPP for themselves and other TPPs in the chain.

To help a customer comfortably understand that another party is involved, the following phrases are recommended.

- *To offer this service, we source the following information through our partner xxxxxxxxx*
- *Please wait while our trusted partner xxxxxxx securely accesses information on your account.*

Guidance where multiple TPPs are involved, are covered in the 'How to Guide: Consent Model, Part 1: Implementation' document.

4.2 Account Servicing Payment Service Providers

It is important that a customer feels safe and fully in control of what they are authorising the ASPSP to undertake. The customer must clearly see the appropriate details of the request that the TPP has submitted. This requires the ASPSP to play back to the customer the same level of content.

There should be a clear explanation which enables the customer to provide the ASPSP with authorisation, as well as the ability to cancel the authorisation:

- *XXX has requested the following/above information about your bank account. If you agree to us providing this specific information, then please click the 'confirm' button below.*

Finally, the redirection of the customer back from the ASPSP to the TPP is equally as important and provides a final sense of security and control to the customer by stating that the customer is now logged out of their ASPSP website and is being transferred back to the previous website. Words such as the following should be used:

- *You have been securely logged off from [bank or building society name] and will shortly be transferred to [TPP]*

The research also indicated that customers feel more in control and secure if they are provided with notification of their activity by either the TPP or their ASPSP, by notification of the activity (in the same way payment notification is provided today). Customers responded better to the process being described as 'notification', rather than other descriptions. The notifications or 'receipts' provided by either party, should replicate the consent or authorisation information.

5 Combined Consent

TPPs, in addition to using the Open Banking read/write API, may look to request data from other sources such as the customer's accountancy package, Companies House for company information etc. The TPP will need to request consent for each separately.

The TPP may choose to request all the consents in one combined consent request. The challenge for a TPP using a combined consent request when requesting data from multiple data sources, is striking the balance between the level of information provided to obtain the required consent (so that customers understand what they are consenting to) and a good customer experience. Regardless of the complexity of the combined consent request, the elements that relate to the Open Banking API-enabled product or service must be explicit, informed and time-bound.

Find below guidance on how a combined consent request may be structured:

- Group together similar elements to make it easy for customers to understand
- Present only the grouping titles for readability and avoiding clutter
- Provide explicit unticked opt-in check boxes per grouping title to ensure customers consent to each grouping
- Allow individual groupings to lead to more detail through expandable sections or overlay popups that provide more information
- Provide two choices of equal prominence at the end e.g. Cancel and Confirm

Right is an example of how a TPP could request consent explicitly when using Open Banking APIs in combination with other APIs, such as accountancy packages.

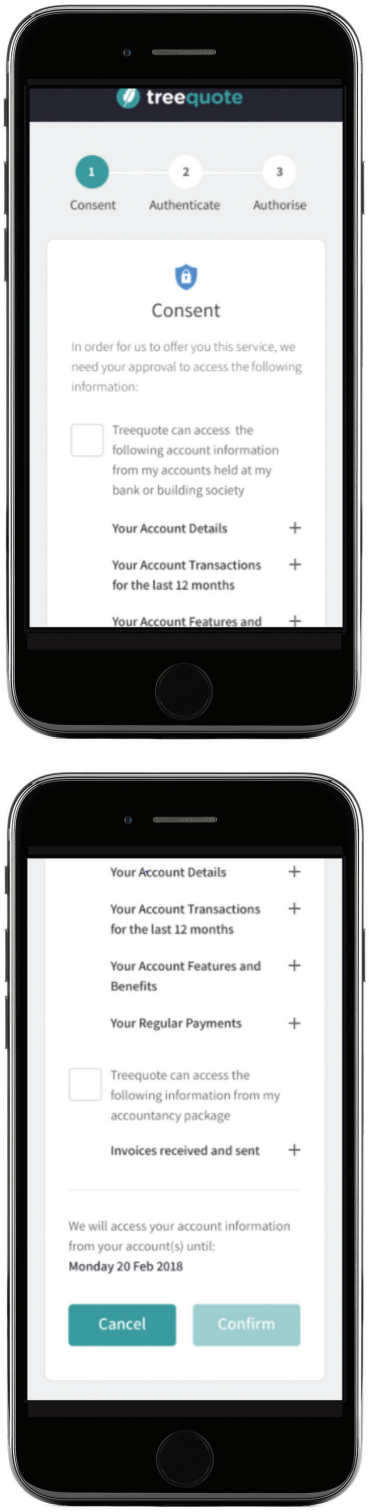


Figure 5.1
Combined Consent Step

6 Decoupled Secure Customer Authentication and Authorisation

The Open Banking design allows for decoupled 'authentication' and 'authorisation' steps i.e. out-of-band authentication and authorisation for additional security.

This is where, for example:

- The first factor of the authentication step takes place on the same device as the TPP app/website
- The second factor of the 'authentication step' and 'authorisation step' take place on the ASPSP's app/website on another device

The end-to-end price payment journey in the 'Links' section demonstrates this. This is where the customer is purchasing a vacuum cleaner from 'Zoomit's' website and uses Open Banking to pay for it. The customer completes the first factor of the authentication step on the ASPSP's (Greenview Bank) website. The second factor of the authentication step and the authorisation steps are completed on the ASPSP's mobile app.

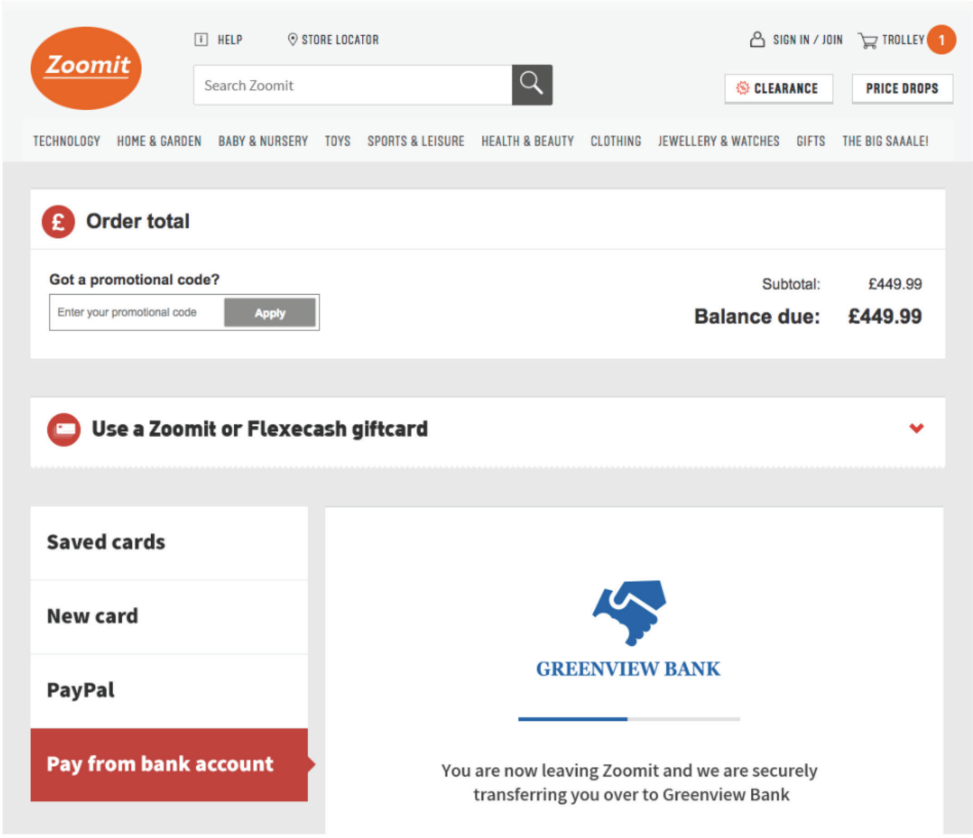


Figure 6.1 TPP to ASPSP redirection from the TPP's site

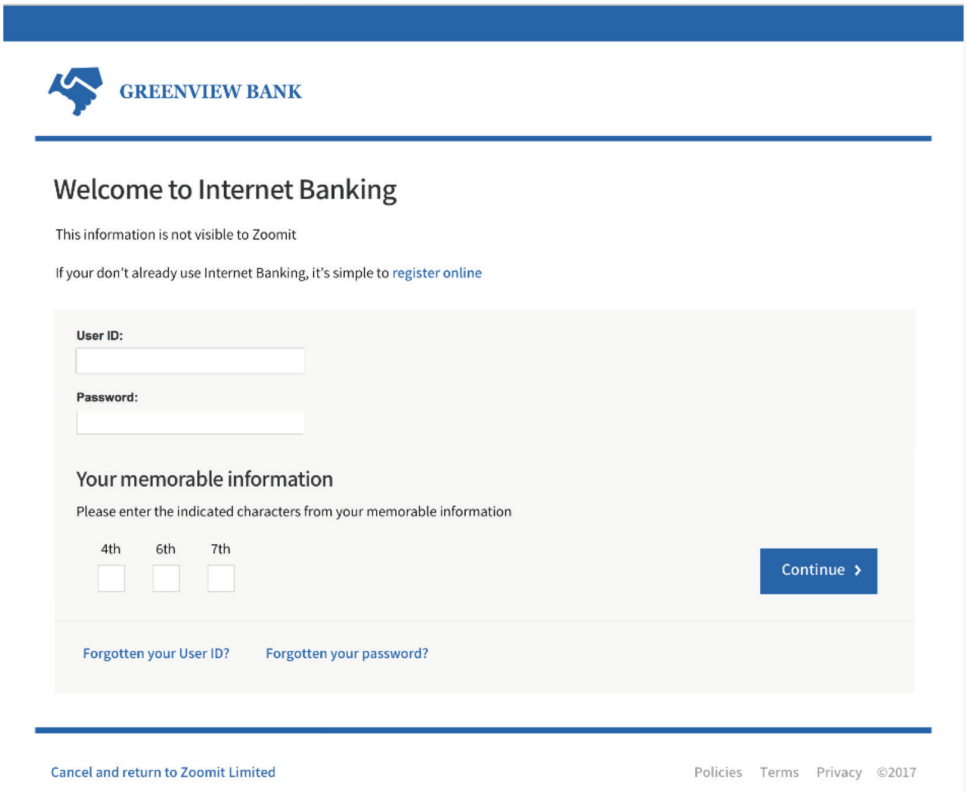


Figure 6.2 First factor of the Authentication step on the ASPSP's site

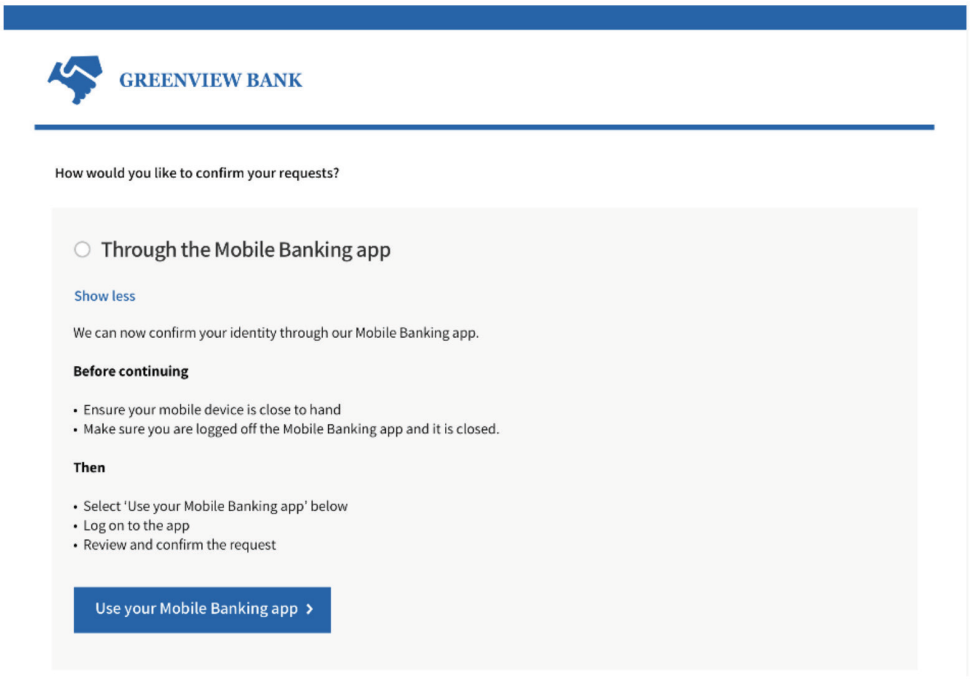


Figure 6.3
The customer chooses the mobile banking app for the second factor of the Authentication step on the ASPSP's site

Figure 6.4
Second factor of the Authentication step on the ASPSP's app

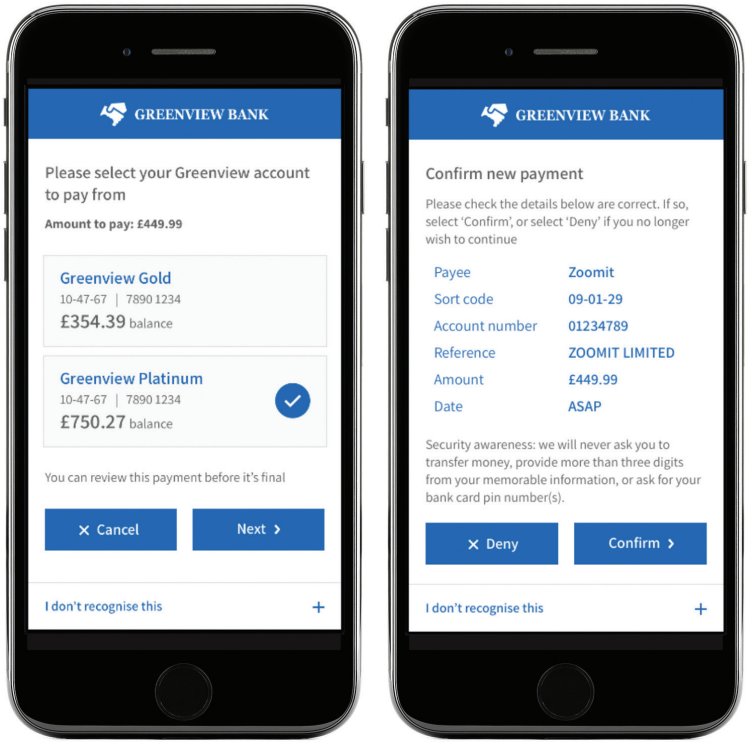


Figure 6.5 The Authorisation step on the ASPSP's app

7 Management of consent and authorisation

The research has shown that customers expect to be able to view and revoke the consents they have given to TPPs.

They would like to be able to do this with both TPPs and their ASPSP i.e. view/revoke consent from the TPP and view/revoke authorisations for a TPP from the ASPSP. Therefore, both TPPs and ASPSPs should offer dashboards that allow customers to manage consents and authorisations accordingly. Although the research suggested that the customer preference was for a dashboard, it also indicated that certain customer segments would value consent and authorisation receipts or notifications as an alternative or addition to a dashboard.

8 Management of consent at the TPP

8.1 Consent dashboard

The customer consents to the TPP in order for the TPP to provide the customer products and/or services. This could include consent for repeat access to their data from various sources; Open Banking could be one such source of data. Therefore, for the customer to be able to view/revoke those consents, the TPP should provide a consent dashboard. Find below an example of this:

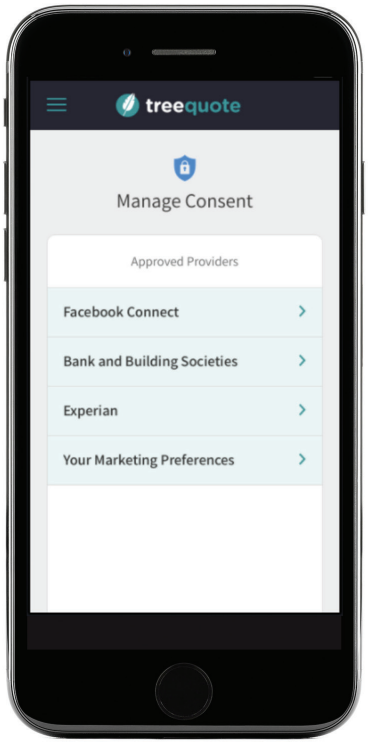


Figure 8.1 Consent Dashboard

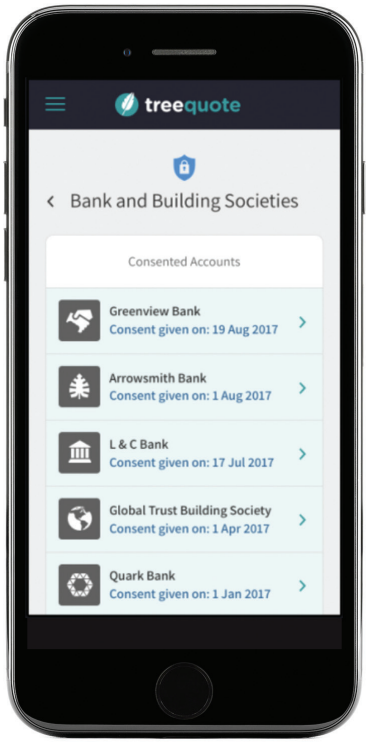


Figure 8.2
Open Banking Consent Dashboard

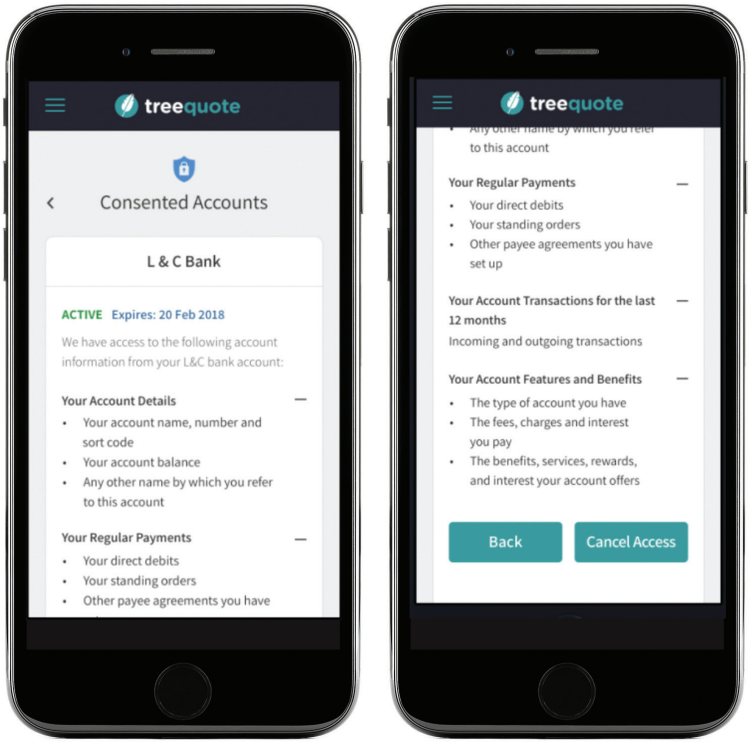


Figure 8.3 View Consent

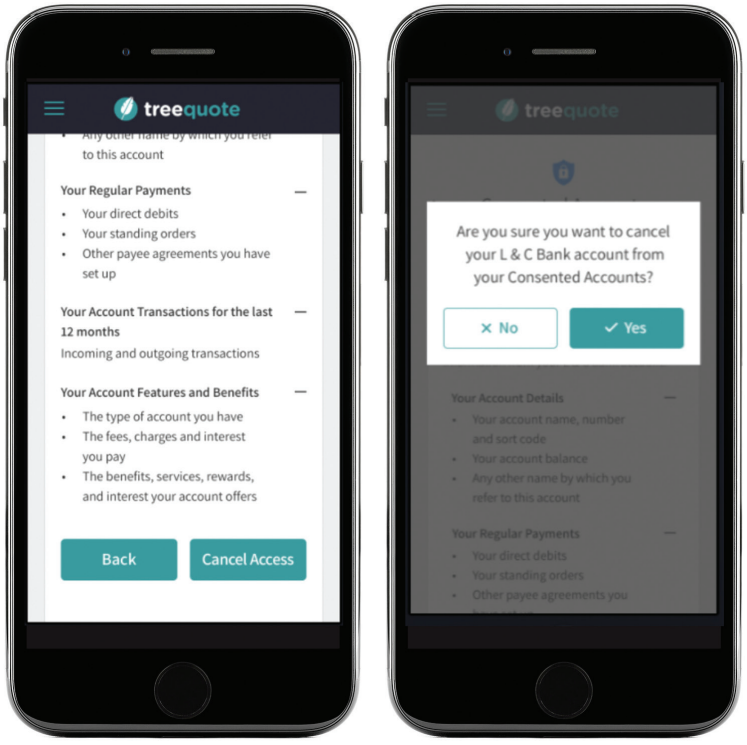


Figure 8.4 Revoke Consent

The research has shown that dashboards are popular amongst customers. Below are some verbatim comments from the research:

"It shows that you are in control".
Multi-banked, Birmingham

"When I want to cancel something I want to get rid of it. It needs to be clear".
Early Adopters, London

The same components that were displayed at the point of requesting consent should be displayed when viewing/revoking consent from the consent dashboard:

- Name of the TPP that is requesting the consent
- The data clusters that have been requested
- The purpose of the data request and how that data will be used
- The period for which the transaction data has been requested for
- When the TPP's access to the data will expire
- How frequently the data will be accessed (this is limited to 4 times in 24 hrs without the presence of a PSU)
- The date the consent was granted

It should be noted that consent for single immediate payments will not be stored and cannot be revoked, therefore this information will not feature on dashboards. However, consent receipts/notifications could be provided for these types of payments.

8.2 Consent receipts

The research has suggested that customers would like a receipt or notification for each consent they have given. Receipts are considered to provide reassurance that an action has happened and to alert customers to the occurrence of any unfamiliar transactions. Receipts are more popular with older, more cautious customers but viewed as potential information overload for some younger, savvier customers. For these customers, the use of dashboards means a lesser need for a digital trail so receipts are considered unnecessary for future reference. It should also be noted, there is a strong dislike of the inclusion of links in the receipt as customers perceived this to pose a potential security threat (e.g. possibility of phishing, virus etc.).

The preference would be to receive these receipts via SMS or email. In addition, the same components displayed at the point of requesting consent should be displayed through the consent receipt:

- Name of the TPP that is requesting the consent
- The data clusters that have been requested
- The purpose of the data request and how will the data be used
- The period for which the transaction data has been requested for
- When the TPP's access to the data will expire
- How frequently the data will be accessed (this is limited to 4 times in 24 hrs without the presence of a PSU)
- The date the consent was granted

For payment initiation, the same components that were displayed at the point of requesting consent should be displayed through the consent receipt:

- Name of the TPP that is requesting the payment The amount of the payment request in GBP
- What the payment is for
- The beneficiary of the payment
- The reference of the payment
- Any remittance information
- The payer's account details, if they have been provided by the customer to the initiating merchant
- The date the consent was granted

There should be controls available to switch on and off the consent receipts capability. However, for most segments a highly functional dashboard that is easily accessible is more valuable than receiving receipts.

9 Management of authorisation at the ASPSP

9.1 Authorisation dashboard

The research has shown that customers expect to view and revoke TPP authorisations given to the ASPSP. When multiple TPPs are involved in serving the end customer, both the regulated TPP making the account information request, and the other TPP in the chain, should also be displayed within the authorisation dashboard for each authorisation, see Figure 9.2 - Open Banking Authorisation Dashboard. The regulated TPP making the account information request should be shown first and then the other TPP should be shown in brackets. For details on when multiple TPPs are involved, participants should refer to the 'How to Guide: Consent Model, Part 1: Implementation' document.

Find below an illustration of an authorisation dashboard to which customers had responded positively during the research. Revoking TPP authorisations could have unintended consequences for the customer, therefore, care must be taken with how this is positioned with the customer. Open Banking recommends that revoking the authorisation should be seen as an additional option to revoking consent at the TPP.

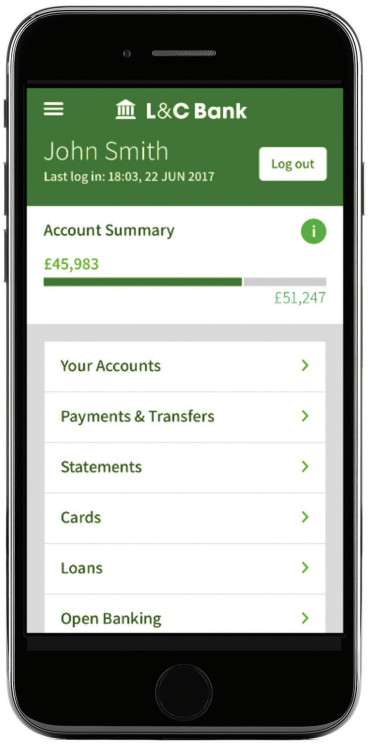


Figure 9.1 Bank account summary

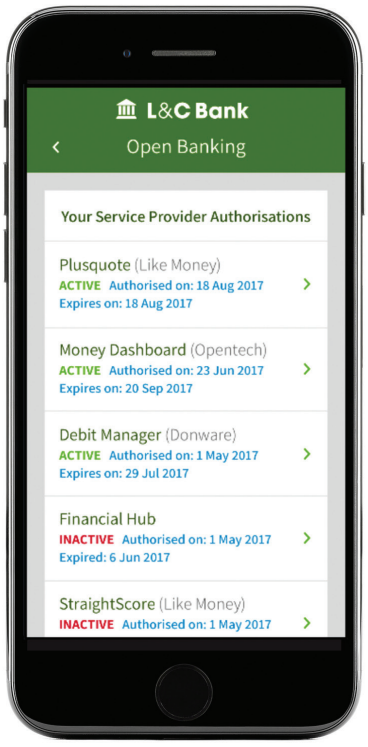
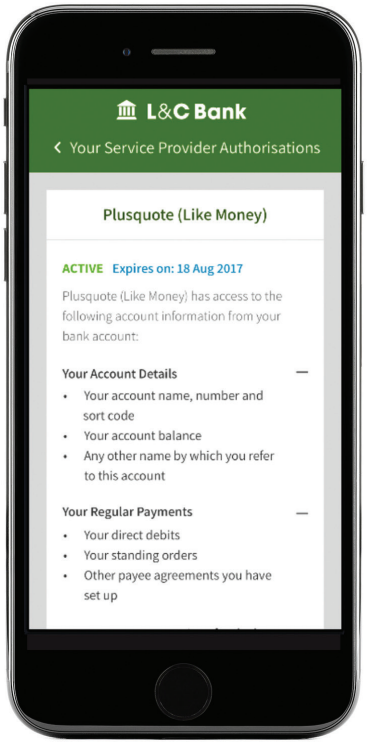


Figure 9.2 Open Banking Authorisation Dashboard

The list view as displayed in Figure 9.2, should be used for each authorisation:

- Name of the TPP that is requesting the consent
- The status of the authorisation e.g. Active/Inactive
- When the TPP's access to the data will expire
- The date the authorisation was granted



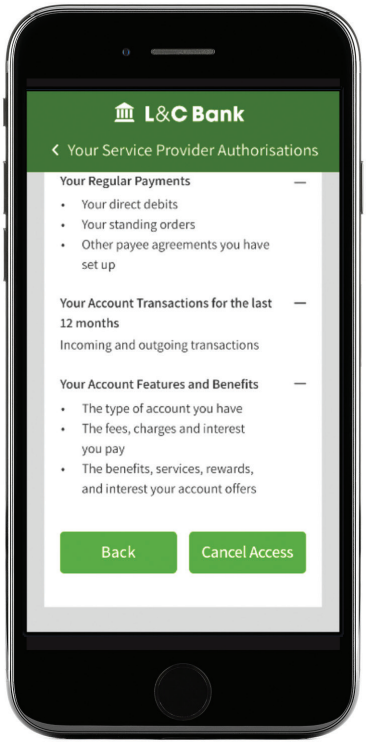


Figure 9.3 View Authorisation

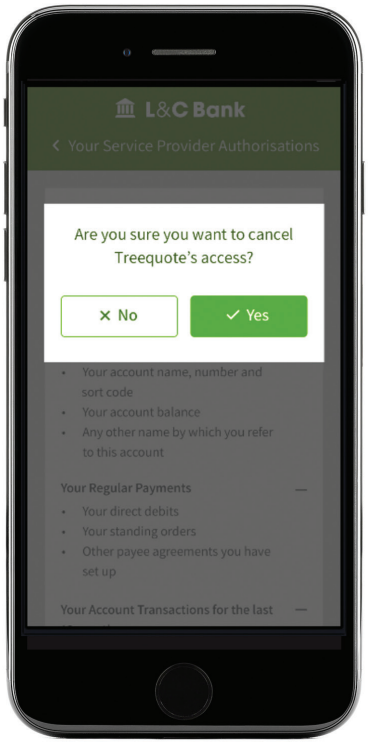


Figure 9.4 Revoke Authorisation

The same components that were displayed at the point of requesting authorisation should be displayed when viewing/revoking an authorisation on the Open Banking authorisation dashboard:

- Name of the TPP that is requesting the consent
- The data clusters that have been requested
- The period for which the transaction data has been requested for
- When the TPP's access to the data will expire
- The date the authorisation was granted

It should be noted that authorisations for single immediate payments cannot be revoked and therefore should not feature on dashboards. However, it will be possible to provide authorisation receipts/notifications for these payments.

9.2 Authorisation receipts

The research has suggested that customers would like a receipt or notification of authorisations they have given. Receipts are considered to provide reassurance that an action has happened and to alert customers to the occurrence of any unfamiliar transactions. Receipts are more popular with older, more cautious customers but a potential information overload for some younger, savvier customers. For these customers, the use of dashboards means a lesser need for a digital trail, so receipts are considered unnecessary for future reference. There is a strong dislike of the inclusion of links in the receipt as they are perceived as posing a potential security threat (e.g. possibility of phishing, virus etc.)

The preference would be to receive these via SMS or email. The same components that were displayed at the point of requesting authorisation should be displayed through the authorisation receipt:

- Name of the TPP that is requesting the consent
- The data clusters that have been requested
- The period for which the transaction data has been requested for
- When the TTP's access to the data will expire
- The date the authorisation was granted

For payment initiation, the same components that were displayed at the point of requesting authorisation should be displayed through the authorisation receipt:

- Name of the TPP that is requesting the payment
- The amount of the payment request in GBP
- What the payment is for
- The beneficiary of the payment
- The reference of the payment
- Any remittance information
- The payer's account details, if they have been provided by the customer to the initiating merchant

Customers have rated authorisation receipts as more valuable than consent receipts as they are already used to receiving such notifications from their banks whenever they setup new payees or standing orders with their ASPSP. Furthermore, notifications from the ASPSP act as an added assurance that the customer has indeed engaged with their ASPSP via the TPP as part of the three-step process when granting consent. There should be controls available to switch on and off the authorisation receipt capability. Overall, most segments preferred a highly functional dashboard that is easily accessible over receipts.

10 Signposting

The research has shown that given the wide and varied customer experiences that would be made available by the various TPPs and ASPSPs, there is a clear need to signpost the consent, authentication, and authorisation steps of the process so that they can be easily recognised, irrespective of the TPP or ASPSP.

The research has suggested that it could be a major source of reassurance for the following reasons:

- Gives the customer understanding of the process as a whole - consent, authentication, authoris
- Gives customers a sense of where they are in the process
- Encourages engagement and demonstrates the process to be short
- Reveals the relationship between the ASPSP and TPP

A signposting scheme that was tested with customers and worked well can be found below:

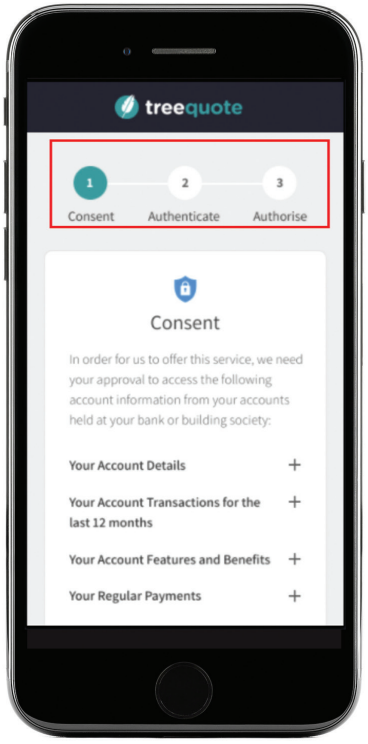


Figure 10.1 Consent step

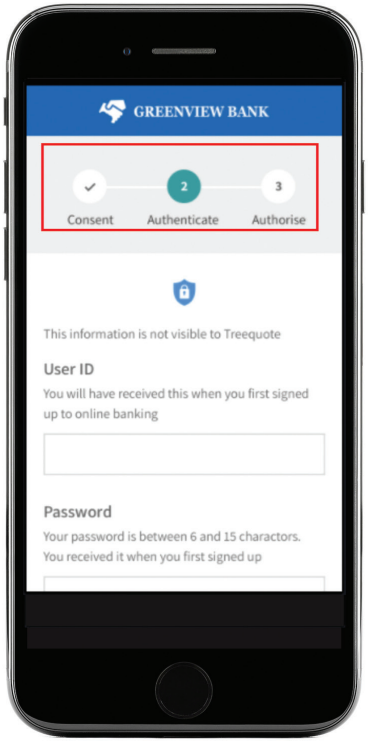


Figure 10.2 Authentication step

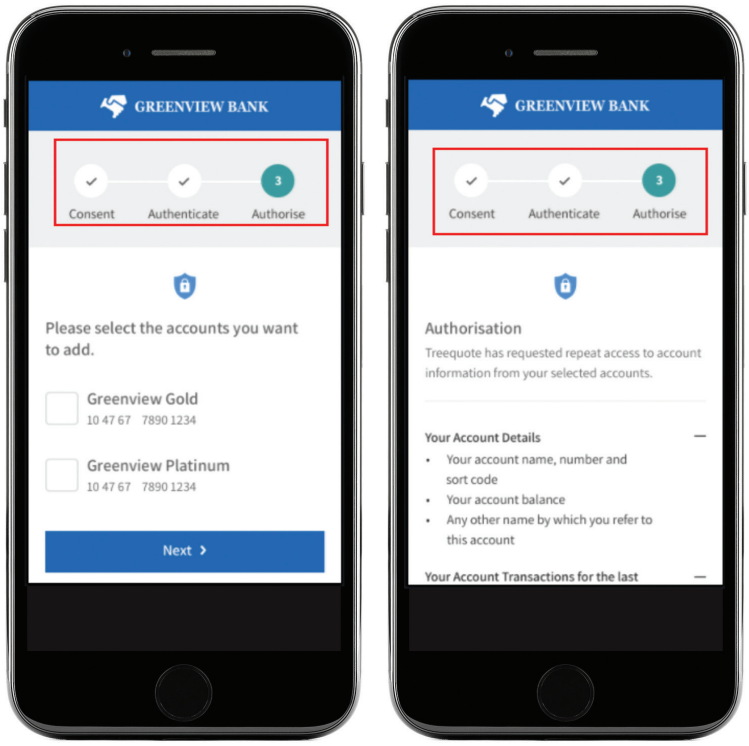


Figure 10.3 Authorisation step

The same scheme needs to be adopted across the board by TPPs and ASPSPs in order for this to work in an effective manner.

11 Role of positive friction

The research has shown that a proportion of customers are skimming through the information presented to them as part of the consent, authentication, and authorisation steps.

This same research has indicated that many customers, once they have completed the three-step process, cannot spontaneously describe what they just agreed to. These issues are particularly relevant in the context of vulnerable members of society such as people with mental health issues.

Therefore, in the context of consent and data privacy, where there could be unintended consequences of not considering carefully what is being agreed to, it is important to find ways to slow customers down within their online journeys. This can be achieved by introducing positive friction. Open Banking explored various ways of introducing positive friction in the three-step process as follows:

- By introducing a three second delay on the redirection screens
- By spreading the same information across multiple screens

The research has shown that providing the same information on multiple screens acts as a good source of positive friction in the context of the three-step process. The authorisation step was very effective in creating positive friction as it provided a final chance to pause and review what customers had agreed to, and prevents the tendency to click through the consent process without considering the implications.

ASPSPs should consider the information that customers need to understand as part of the authorisation step.

Explicit unticked opt-ins also act as a good source of positive friction as they require an action from the customer. However, a balance is required as too many options can overwhelm customers and have the opposite effect.

12 Links

How to Guide: Consent Model, Part 1 - Implementation Document can be found here:
https://www.openbanking.org.uk/read-write-apis/

Open Banking Read/Write API specifications can be found here:
https://www.openbanking.org.uk/read-write-apis/

Open Banking Interim Guidelines for Read/Write Participants can be found here:
https://www.openbanking.org.uk/directory/

In order to demonstrate the consent, authentication, and authorisation steps, as well as highlight the learnings from the various customer research initiatives, non-branded customer journey prototypes have been created. You can access these journey prototypes via the links below. The links below should be copied and pasted into a browser's URL window, preferably Chrome. They showcase specific areas as follows:

Journey type	Links	Areas showcased
End to end account aggregation journey	https://invis.io/ZTD2DYOXN#/248946024_00_-_Onboarding_1	• 3-step process in the AISP context (mobile) • Sign-posting • Mandatory data cluster presentation • Optional data cluster presentation • Redirection
End to end account aggregation journey	https://invis.io/HRD581EU6#/249743076_01_-_TPP_Log_In	• Same as above • Incremental consent
End to end ongoing authentication and authorisation journey	https://invis.io/CREYAGOHX	• Ongoing authentication and authorisation in the AISP context
End to end payment journey (Finish the desktop journey and then go to the mobile journey)	**Desktop:** https://projects.invisionapp.com/share/KTD3IUJ3W#/scr eens/249280764_01_-_Product **Mobile:** https://invis.io/EWD3LDJY2#/249299416_01_-_Sms	• 3-step process in the PISP context • Decoupled secure customer authentication and authorisation • Real-time balance check and account selection
End to end price comparison journey (Finish the desktop journey and then go to the mobile journey)	**Desktop:** https://invis.io/NDD4MNS54#/249591328_01_-_Product **Mobile:** https://invis.io/D3D4MO6JR#/249596261_01_-_Who_Are_You	• 3-step process in the AISP context (website) • Multi-party consent and authorisation
Authorisation dashboard	https://invis.io/S7D3T29YA#/249354597_01_-_Who_Are_You	• Revoking single TPP authorisation • Revoking multi-party TPP authorisation
Account aggregation consent dashboard	https://invis.io/D2D581SYG#/249771004_01_-_TPP_Log_In	• Presentation of Open Banking and non- Open Banking consents • Consent dashboard • Revoking Open Banking consent

Research was undertaken between March and August 2017 by Ipsos Mori. For further information please contact Open Banking.