OPEN BANKING

How to Guide: Consent Model

Part 1: Implementation

Open Banking Read/Write API
December 2017
Version 1.1

Contents

1 Introduction

In response to the Competition and Markets Authority's (CMA) Order, the Open Banking Implementation Entity (OBIE) has developed Application Programming Interfaces (APIs) to support services that will be offered by Account Servicing Payment Service Providers (ASPSPs) and Third Party Providers (TPPs). These APIs underpin the Open Banking Consent Model, the process by which a Payment Service User (PSU) (also referred to as the customer) gives their consent to a TPP to initiate payments or access account information and transaction data.

This document is the OBIE view on how Participants (ASPSPs and TPPs) should implement the Open Banking Consent Model within the OBIE interpretation of the relevant legislation. This legislation includes the Payment Services Directive (PSD2), General Data Protection Regulation (GDPR) and the CMA's Retail Banking Market Investigation Order. This document does not provide a definitive guide to regulatory compliance. It is the sole responsibility of the individual Participants to ensure that they are compliant with their regulatory and legal responsibilities.

Implementation of the consent model must also be in line with the Open Banking Read/Write API specifications. These specifications define the underlying information exchanges between Participants but not the way in which that information is presented to the PSU.

OBIE has also carried out an extensive program of customer research around the consent experience. This research has informed the language and design of the examples of the user experience contained in this document. This research has also informed 'How to Guide: Consent Model, Part 2 - User Experience' which provides additional guidance on how Participants can optimise the user experience.

This document should be read in conjunction with:

- How to Guide: Consent Model, Part 2 - User Experience
- Open Banking Read/Write API specifications

Participants should also refer to:

- Open Banking Interim Guidelines for Read/Write Participants
- OBIE Consent Journey Mock-ups

Links to these documents are available at the end of this document.

2 Open Banking Consent Model - Consent, Authentication and Authorisation

In order to engage in Open Banking through the use the Open Banking Read/Write APIs, Participants are required to follow a common three step process of consent, authentication and authorisation known as the **Open Banking Consent Model.** This model was created through extensive research on preferences of the PSU, relevant regulation and existing practices between PSUs and payment services providers.

The three step Consent Model 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 the service to the PSU.

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 following section gives an overview how the steps of the Consent Model link to each other to support the overall process. The details of each individual step follow the overview.

2.1 Three Step Consent Model Overview

Consent:

The TPP will request explicit consent from the PSU in order to initiate payments or access information from the PSU's account (see Figure 1.1 for an example of the consent step to access account information). There could be a number of elements associated with this consent request depending on the service being offered. At this stage the PSU will be required to identify their ASPSP that they want to use for the service offered by the TPP (see Figure 1.2).

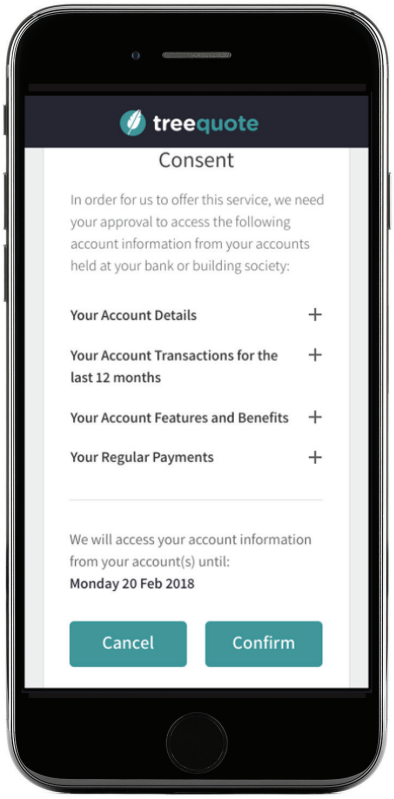


Figure 1.1 Consent step

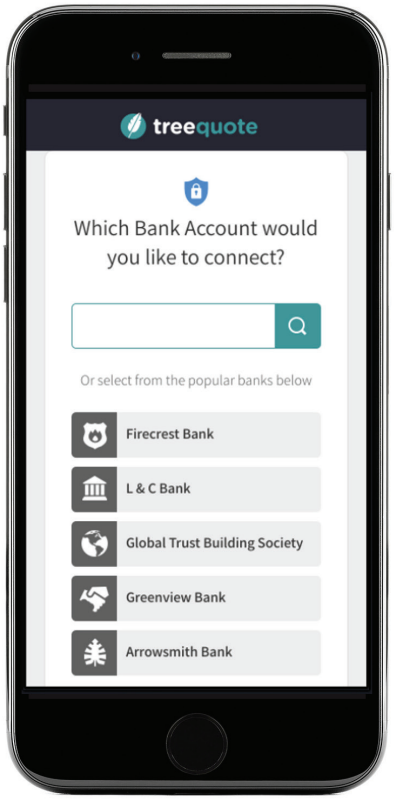


Figure 1.2 Choosing ASPSP

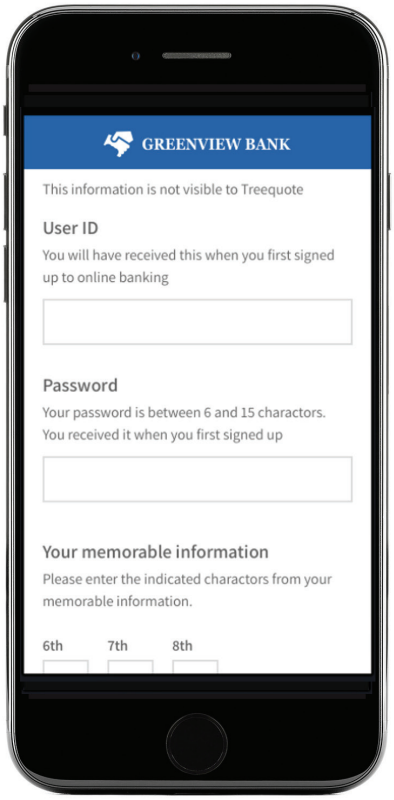


Figure 1.3 Authentication step

Once the TPP has gained the PSU's consent, the TPP will send a message to the ASPSP confirming the elements of the consent that has been obtained from the PSU and requesting access to the PSU's account. The PSU will then be re-directed to the ASPSP for the authentication step.

Authentication:

The authentication step takes place in the ASPSP's domain and allows them to verify the identity of the PSU (as in Figure 1.3) so that the TPP's request can be serviced appropriately. The ASPSP will choose the method by which they authenticate the PSU.

Authorisation:

Once the PSU has verified their identity via authentication, the ASPSP will then present the PSU with a description of the access request confirming all elements of the consent that the PSU previously provided to the TPP. The PSU will then authorise the ASPSP to fulfil the request from the TPP (see Figure 1.4)

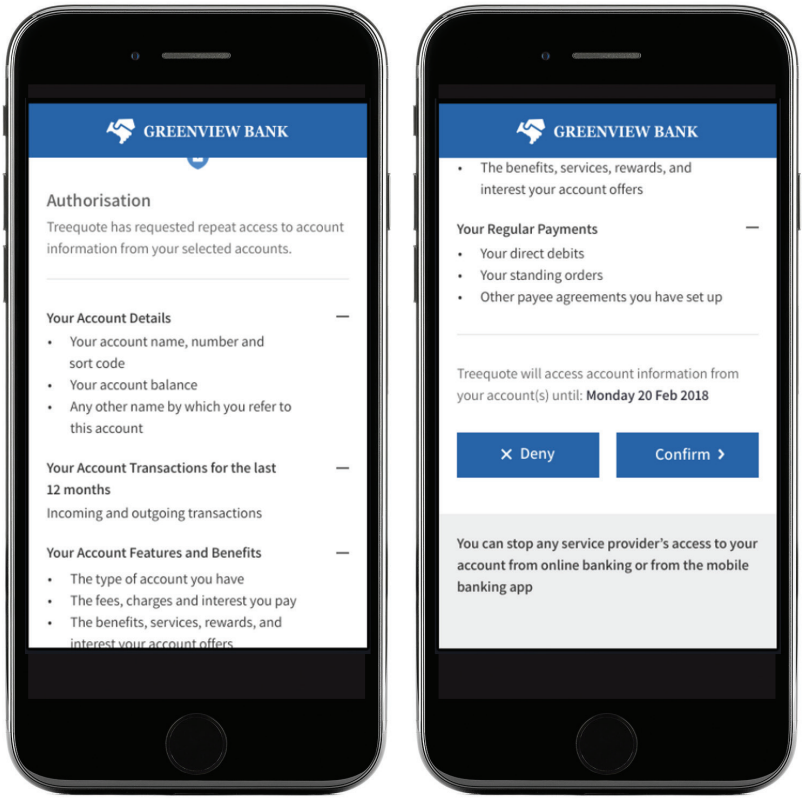


Figure 1.4 Authorisation step - Authorise the ASPSP

Once the PSU has authorised the ASPSP, the PSU will be re-directed back to the TPP's domain and their connection to the ASPSP will be closed. Once back in the TPP's domain, the PSU will continue with the service the TPP is offering.

Depending on the products or services provided by the TPP, they may need access to a number of the PSU's accounts. In the event the PSU has accounts at multiple ASPSPs, the Authentication and Authorisation steps will be repeated for each ASPSP.

The following sections look at each of the three steps in more detail.

2.2 Consent Step

The consent step is where the TPP requests explicit consent from the PSU to access their account for account information or payment initiation. The consent request should be clear, specific and informed. Clarity and specificity will be helped by ensuring that when consent is sought it is distinguishable from other matters (e.g. not hidden in terms and conditions) and written in clear, plain language.

In this step, the TPP has to gather all the elements that are required by the Read/Write API and use them to populate the relevant payloads. Some of these elements will be presented directly to the PSU for confirmation (e.g. the amount of a payment and the payee). Others will be generated by business rules put in place by the TPP access request. Consequently, not all of the elements listed in the following sections will be applicable to the consent request for every service offering.

Account Information Consent Request:

For account information, the consent request to the PSU could include, but not be limited to, the following elements (see Figure 1.5):

1. Name of the TPP that is requesting the consent
2. The data (see section 3) that has been requested
3. The purpose of the data request and how the data will be used
4. The period over which the transaction data has been requested
5. When the TPP's access to the data will expire
6. Whether the request is one-off or recurring

The information that the TPP provides to the PSU will be dependent on the specific service being offered. However, the minimum requirement in all instances is that the TPP meets its obligations in terms of requesting explicit consent as defined by the regulations and conforms to the Read/Write API specifications.

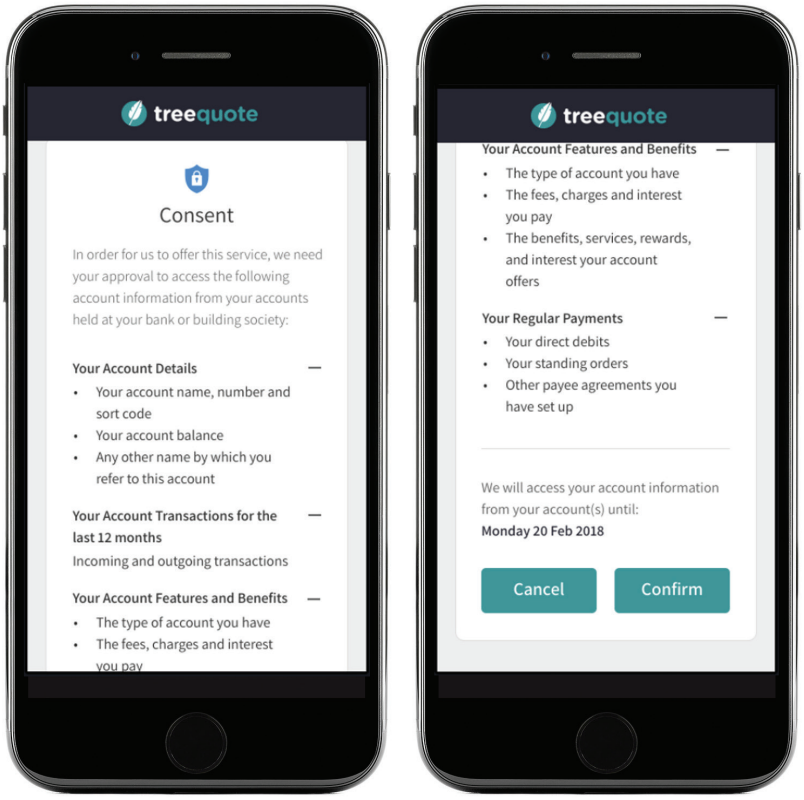


Figure 1.5 Consent Step - Account Information

Payment Initiation Consent Request:

For payment initiation, the consent request to the PSU could include, but not be limited to, the following (see Figures 1.6a and 1.6b):

1. The TPP requesting the payment
2. The amount of the payment
3. What the payment is for
4. The beneficiary of the payment
5. The reference of the payment
6. The payer's account details, if they have been provided by the PSU to the initiating TPP
7. Any additional charges

All the components that apply to the TPP's business model should be catered for in the consent request. There should be no implicit opt-ins and the PSU should not be requested to explicitly opt out.

The information that the TPP provides to the PSU will be dependent on the specific service being offered. However, the minimum requirement in all instances is that the TPP meets its obligations in terms of requesting explicit consent as defined by the regulations and conforms to the Read/Write API specifications.

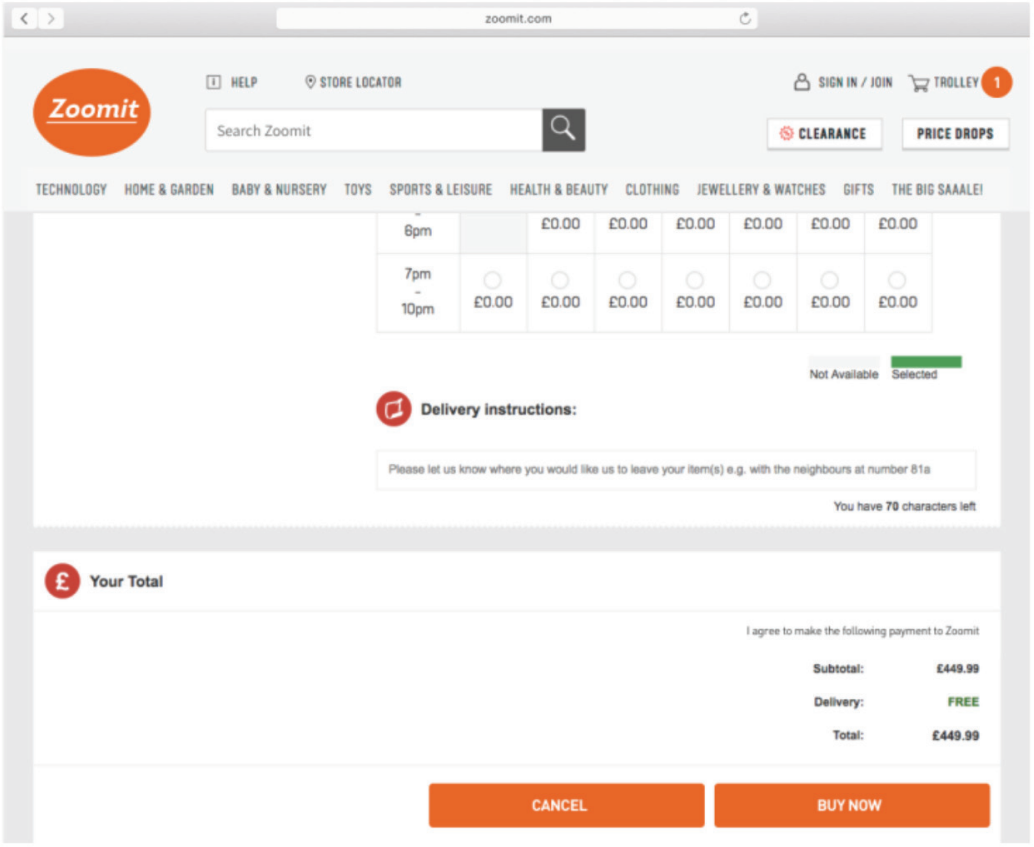


Figure 1.6a Consent Step - Payment Initiation

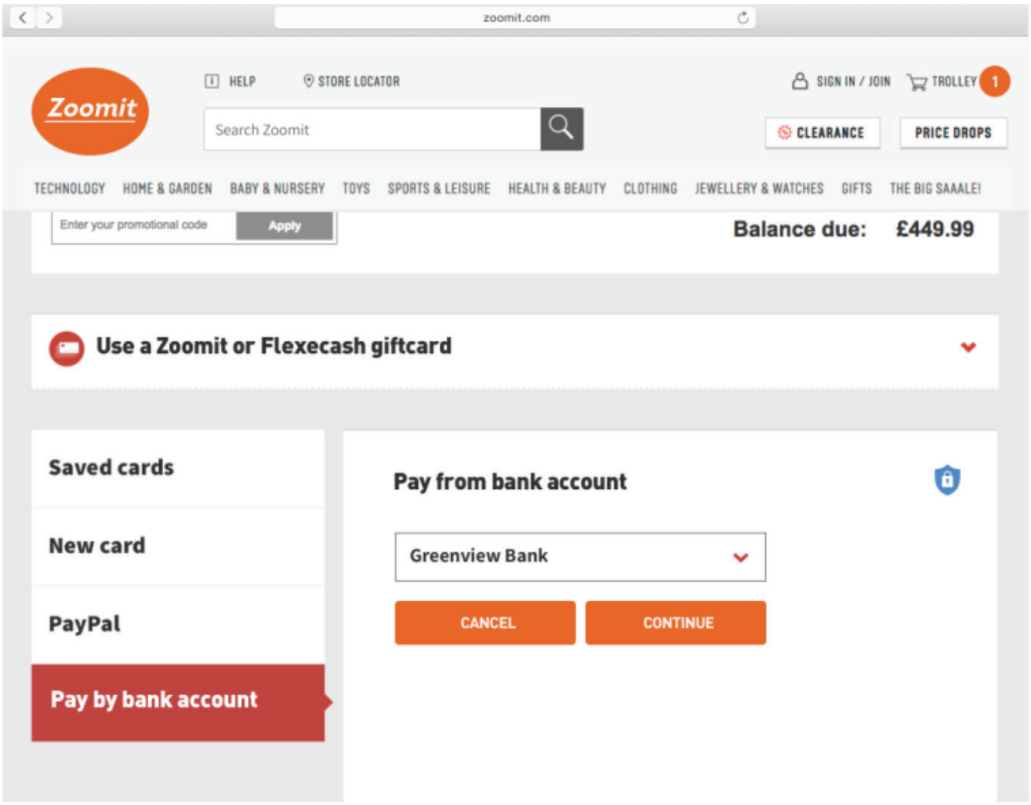


Figure 1.6b Consent Step - Payment Initiation

2.3 Authentication Step

The authentication step takes place within the domain of the ASPSP and is where the ASPSP requests the PSU to identify themself so that the TPP's request can be serviced appropriately.

It is the competitive space and for the ASPSP to determine which methods of authentication it wishes to use to validate the identity of the PSU. The minimum requirement is that the ASPSP meets any regulatory obligation and that the authentication process they deploy can be integrated into the Open Banking Consent Model. An example of the authentication step in the context of the Open Banking Consent Model is shown in figure 1.3.

2.4 Authorisation Step

The authorisation step is where the PSU confirms, in the domain of the ASPSP, that the ASPSP may process the TPP's request, based on the consent previously provided by the PSU.

Account Information Authorisation Request:

Choosing Accounts (Figure 1.7):

Once in the domain of the ASPSP and prior to giving authorisation, the PSU will be asked to select the required account(s) from a list provided by the ASPSP. If the PSU only has one account, this could be presented as a default.

Authorising the ASPSP (Figure 1.8):

When seeking authorisation from the PSU, the ASPSP will present the PSU with the details of the request it received from the TPP. This could include the following:

1. The name of the TPP that requested the consent
2. The data that has been requested
3. The period over which the transaction data has been requested
4. When the TTP's access to the data will expire
5. The details of the account(s) to which access will be authorised
6. For transaction data, the period over which transaction history has been requested

All the elements of the TPP's access request that are available to the ASPSP should be shown on the authorisation request. The PSU should not be able to de-select any of the data elements presented on the authorisation request. However, they should be able to accept or reject the authorisation request in its entirety.

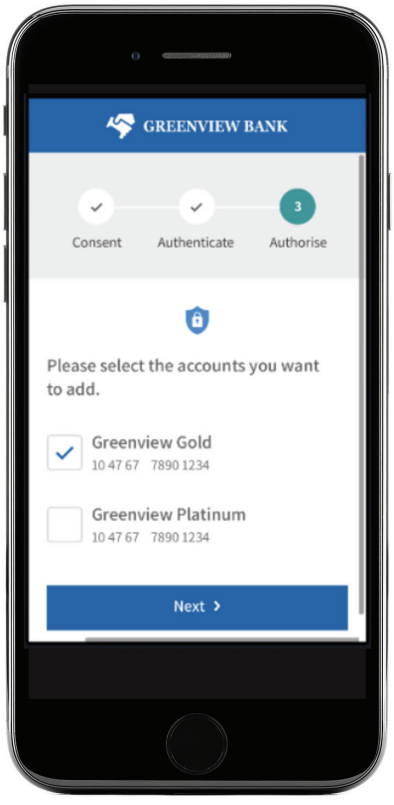


Figure 1.7
Authorisation step - Choose account

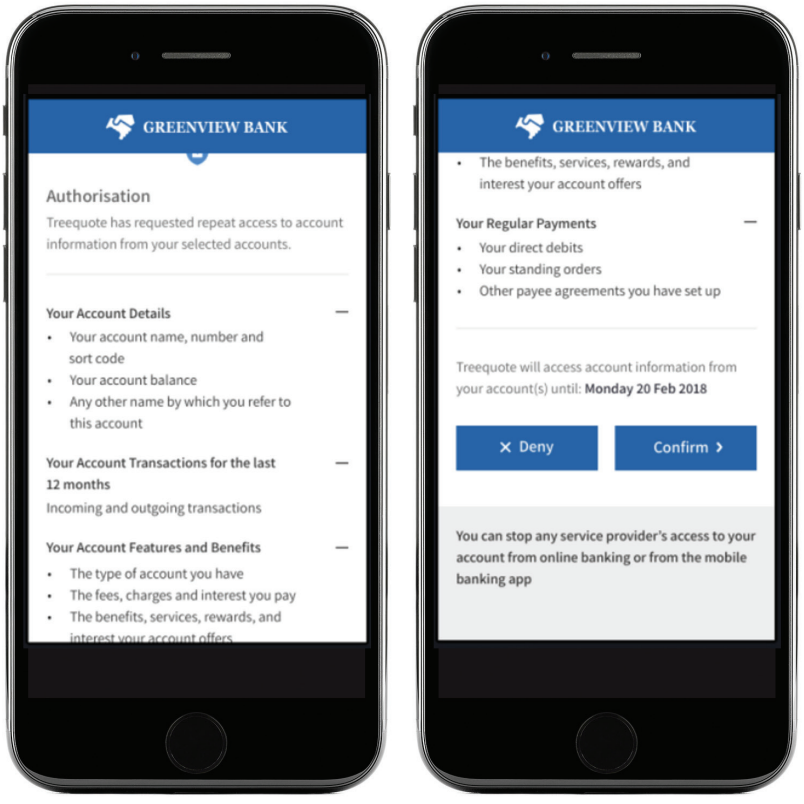


Figure 1.8 Authorisation step - Authorise the ASPSP

Payment Initiation Authorisation Request:

Choosing Accounts:

At some point in the consent process the account from which the PSU wants to make the payment needs to be selected by the PSU.

The Open Banking APIs provides two ways in which the PSU can provide their for their account details (account number and sort code):

- The TPP can ask the PSU for their account details at the consent step and these details are then passed to the ASPSP.
- The PSU can be asked to select the required account from a list provided by the ASPSP as part of the authorisation step. See Figure 1.9 (if the PSU only has one account, this could be presented as a default).

At account selection the PSU could be shown their account balances. There is no obligation for the ASPSP to do this but customer research has shown that PSUs would find this helpful and that it is a feature that could differentiate this payment mechanism from others that might be available.

Authorising the ASPSP:

For payment initiation the authorisation request to the PSU could include the following (see Figure 1.10):

1. **The name of the TPP that requested consent to make the payment**
2. **The amount of the payment request**
3. **The beneficiary of the payment**
4. **The reference of the payment**
5. **The payer's account details**

All the components that apply to the TPP's access request should be shown on the authorisation request.

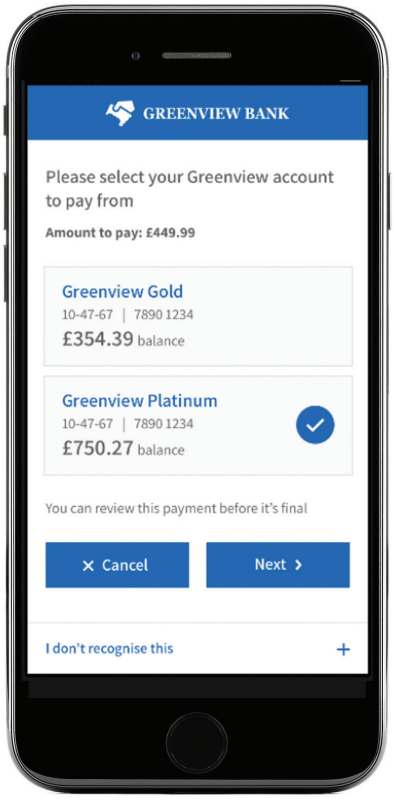


Figure 1.9 Account Selection

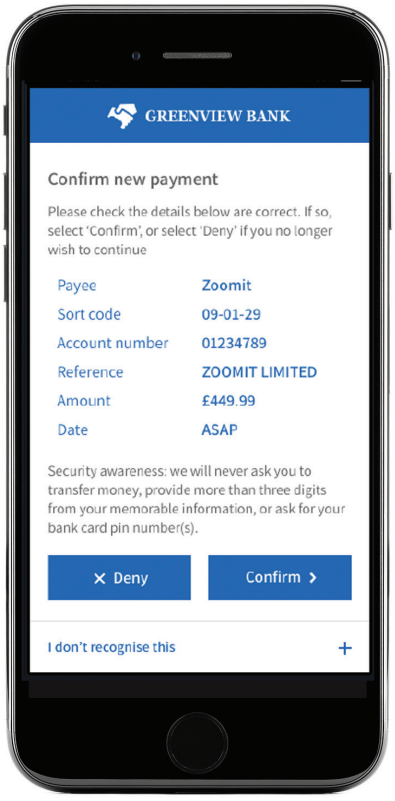


Figure 1.10 Authorisation

ASPSPs should be aware that there is a risk that messaging used in the authorisation step could be viewed as the ASPSP challenging the PSU's intentions. The authorisation step is a replay of the customer's choice, it must not be used to influence their behaviour.

2.5 Redirection

Two redirections happen in the Open Banking Consent Model:

- The PSU is redirected from the TPP to the ASPSP to allow authentication and authorisation
- The PSU is redirected from the ASPSP to the TPP once authorisation has been given by the PSU.

The customer research carried out by OBIE looked at the opportunities to improve the overall experience that are provided by these redirections. Examples are shown in Figures 1.11 and 1.12. Further detail is included in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links).

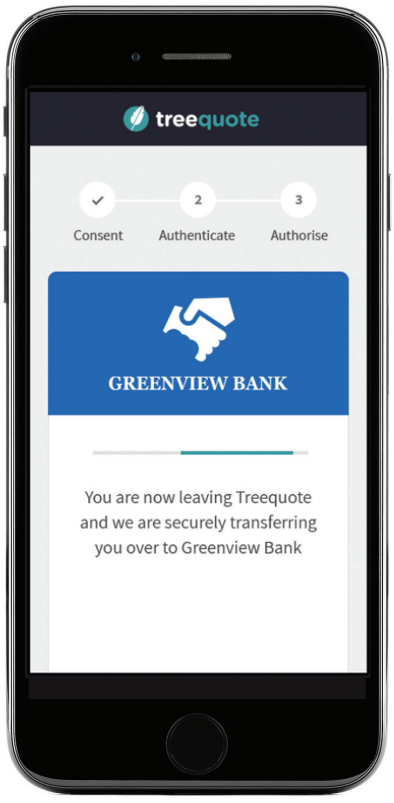


Figure 1.11
TPP to ASPSP redirection

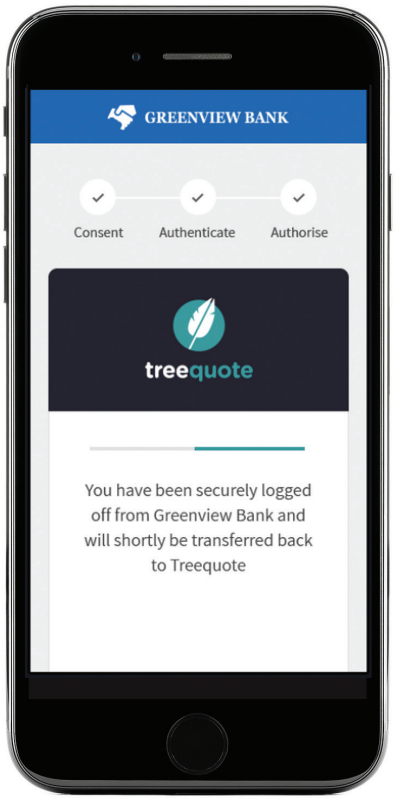


Figure 1.12
ASPSP to TPP redirection

2.6 Ongoing Authentication and Authorisation

When a PSU gives consent to a TPP, who is an Account Information Service Provider (AISP), so that the AISP can access their account information on an ongoing basis:

- The PSU will be required to authenticate themselves and authorise the ASPSP (as described above) in order for the ASPSP to fulfil the AISP's first access request
- Subsequently, the PSU will have to authenticate themselves and authorise the ASPSP at least every 90 days, provided that the AISP only requests up to the last 90 days' transactions at any time, during the 90 day period
- However, if after the first access request, the AISP requests more than the last 90 days' transactions, even if it has been less than 90 days since the last time the PSU authenticated themselves and authorised the ASPSP, the PSU will have to authenticate and authorise again
- Although, the ASPSP could at any time request that the PSU authenticates themselves and authorises the ASPSP

For example, let's say the PSU (on 14 January 2018) consents to Treequote accessing the last three years' of account information (i.e. from 15 January 2015 -14 January 2018) from L&C Bank with a validity lasting until December 2018. L&C Bank offers Treequote three years of account information in the first access request after the PSU has authenticated themselves and authorised the ASPSP. After this, Treequote can continue to access the last 90 days' account information up to four times a day without the PSU having to authenticate themselves and authorise the ASPSP. Therefore, on the 15 March 2018, if Treequote requests 90 days' worth of account information, the PSU will not have to authenticate themselves and authorise the ASPSP as it hasn't been 90 days since the PSU last did this and the Treequote is not requesting more than 90 days' account information. However, the PSU will have to authenticate themselves and authorise the ASPSP:

- If Treequote requests more than 90 days' worth of account information
- If Treequote requests account information on 15 June 2018 as more than 90 days have passed since the PSU authenticated themselves and authorised the ASPSP
- At any time the ASPSP requests the PSU to do so

Example customer experiences on how an AISP may request the PSU to authenticate themselves with the ASPSP and authorise the ASPSP are shown in Figure 1.13. Further detail is included in 'How to Guide: Consent Model, Part 2 – User Experience' (see Links)

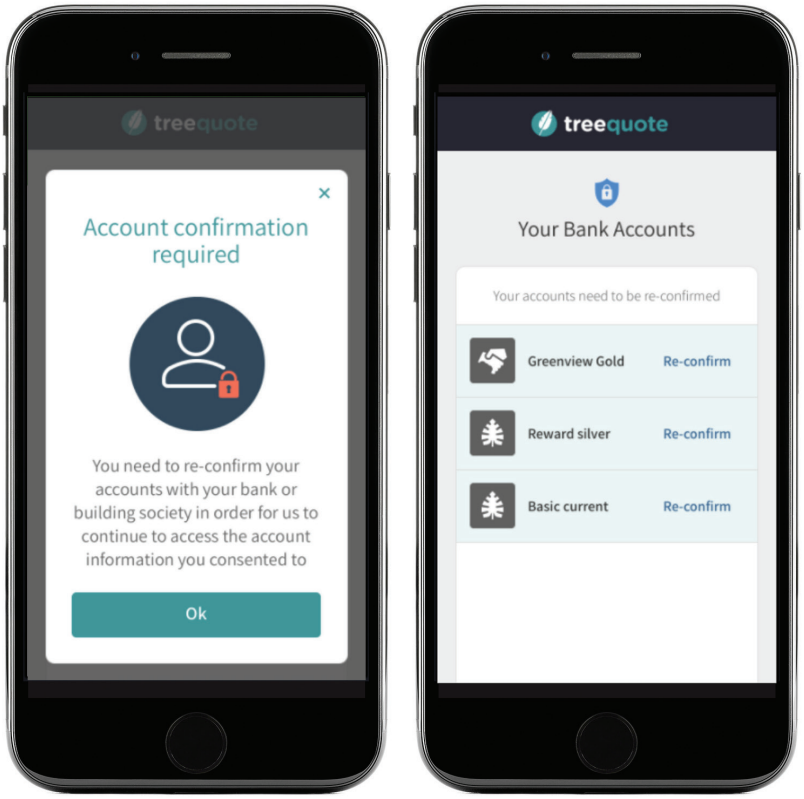


Figure 1.13 Authentication and authorisation request

3 Data Minimisation

TPPs need to follow a data minimisation approach whereby they only request access to the PSU data that they need to deliver the specific service that they are offering.

In the Open Banking API design data elements are logically grouped together into 'permissions' (as described in section 4). It is at this level that TPPs will request data access. If they request access to a specific permission they will have access to all the data elements in the permission. This provides a pragmatic approach, allowing TPPs to be selective but at the same time creating a consent process that is at an acceptable level of granularity for the PSU.

4 Permissions

The following table describes the Permissions that are supported by the Open Banking Read/Write API.

Permissions supported	Description of the PSU's account attributes contained in the permissions set
Account Basic	Currency of the account, Nickname of account (E.g. 'Jakes Household account').
Account Detailed	'Account Basic' permission set plus: Account Name, Sort Code, Account Number, IBAN, Roll Number.
Balances	Amount, Currency, Credit/Debit, Type of Balance, Date/Time, Credit Line.
Beneficiaries Basic	List of Beneficiaries.
Beneficiaries Detailed	'Beneficiaries Basic' permission set plus: Details of Beneficiaries account information (Name, Sort Code, Account).
Standing Orders Basic	SO Info, Frequency, Creditor Reference Info, First/Next/Final Payment info.
Standing Orders Detailed	'Standing Order Basic' permission set plus: Details of Creditor account Information (Name, Sort Code, Account).
Direct Debits	Mandate info, Status, Name, Previous payment information.
Transactions Basic Credits	Transaction Information on payments made into the PSU'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	Transaction Information on payments made from the PSU's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Does not include information about the entity to whom the payment was made.
Transactions Detailed Credits	Transaction Information on payments made into the PSU'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	Transaction Information on payments made from the PSU's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Includes information about the entity to whom the payment was made.
Product (1.0)	PCA/BCA Product information relating to the account (v1.x contains a pointer to the product in Open Data when the PSU has a on sale PCA/BCA product).

(NB - some permissions have basic and detailed options. In these cases, the detailed version contains all the data included in the basic version plus some additional data elements).

4.1 Using Permissions

The structuring of data elements into Permissions is a core part of the Read/Write API design and influences how participants should approach the implementation of the Consent Model.

As part of the consent step (see section 2.2) the TPP will have to describe the data that they are requesting access to. As part of the authorisation step the ASPSP will have to play back the data that the PSU has consented to provide access to. It is critical that the language used by both parties to describe the data is consistent so that the PSU can be sure that they are authorising the ASPSP to provide the access to the TPP that they consented to. The ASPSP will have no sight of the language used by the TPP in the consent step. The ASPSP will only know which permissions have been included in the access request from the contents of the message delivered by the API.

The OBIE program of customer research looked at the language that best describes the data elements of each permission. The output is included below:

Permission	Description
Account Basic	*Any other name by which you refer to this account*
Account Details	*Your account name, number and sort code*
Balances	*Your account balance*
Beneficiaries Basic	*Payee agreements you have set up*
Beneficiaries Details	*Details of Payee agreements you have set up*
Standing Orders Basic	*Your Standing Orders*
Standing Order Details	*Details of your Standing Orders*
Direct Debits	*Your Direct Debits*
Transaction Basic Credits	*Your incoming transactions*
Transaction Basic Debits	*Your Outgoing transactions*
Transaction Detailed Credits	*Details of your incoming transactions*
Transaction Detailed Debits	*Details of your outgoing transactions*

Participants are under no obligation to implement this language but it has been recognised that failing to do so could lead to customer confusion and potentially reduce take-up. Please refer to the 'How to Guide: Consent Model, Part 2 - User Experience' for further information.

4.2 Data Clusters

The OBIE customer research also found that grouping permissions together and adding another layer of description aided the PSU's understanding of the connection between data described in the consent step and that described in the authorisation step. These groups of permissions are known as Data Clusters. Details of how Data Clusters can be implemented by Participants to enhance the User Experience are contained in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links).

5 Advanced TPP Propositions

The Open Banking ecosystem will see the introduction of new players, offering different and innovative services. These players will offer an extensive range of propositions beyond the simple scenarios outlined in this document.

For example:

- A TPP may want to offer a number of services based on Open Banking APIs and may want to design a consent customer journey that avoids repetition for each service
- A TPP may want to offer services that require the PSU to give consent to share data from other sources (e.g. Companies House, accounting software packages) and may want to offer a consent process to optimise the journey.
- A TPP may want to offer a consent revocation process that includes all the consents it holds from the PSU for Open Banking and other unrelated services. Within this the TPP may want to offer selective revocation across a range of consents.

The design of these user experiences is entirely in the domain of the TPP and the range of possible solutions cannot be addressed in this document.

However, if a TPP chooses to combine elements of the consent process across different Open Banking services and/or other unrelated services, they must ensure that the resulting user journey complies with the relevant regulatory requirements.

The program of customer research conducted by OBIE included reference to this type of scenario. This is explored in more detail in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links)

6 When multiple TPPs are involved ('onward provisioning')

This section describes how multiple parties can be catered for in the context of the Open Banking three step consent model.

The customer facing TPP may use other providers in servicing the end customer. Therefore, it is possible that the customer facing TPP may use another provider (ASPSP facing TPP) to connect to the ASPSP to actually make the data or payment initiation request.

Here is an example of this scenario within the Account Information Service context:

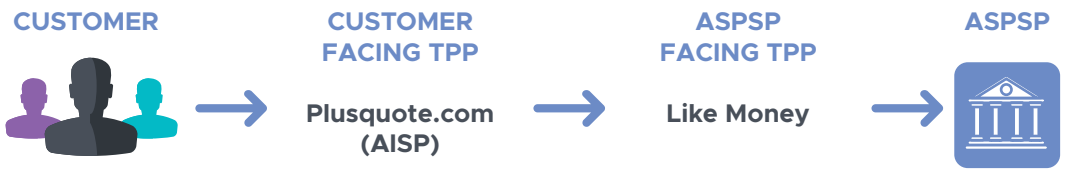


Figure 1.14 Multiple TPP model

In the example above 'Plusquote.com' (a price comparison website provider) is the customer facing TPP and is regulated. 'Like Money' is the ASPSP facing TPP and may not be regulated. However, other scenarios with different combinations of regulatory statuses may also be possible. There should be at least one regulated TPP in the chain and it should be made clear to the customer who in the chain is regulated.

It is the customer-facing TPP's responsibility to obtain explicit consent from the PSU and also to comply with data protection legislation in respect of the permission or transparency required in respect of other third parties.

Find below an example of multi-party consent, here 'PlusQuote' the customer facing TPP is requesting explicit consent for both the 'PlusQuote' and 'LikeMoney'.

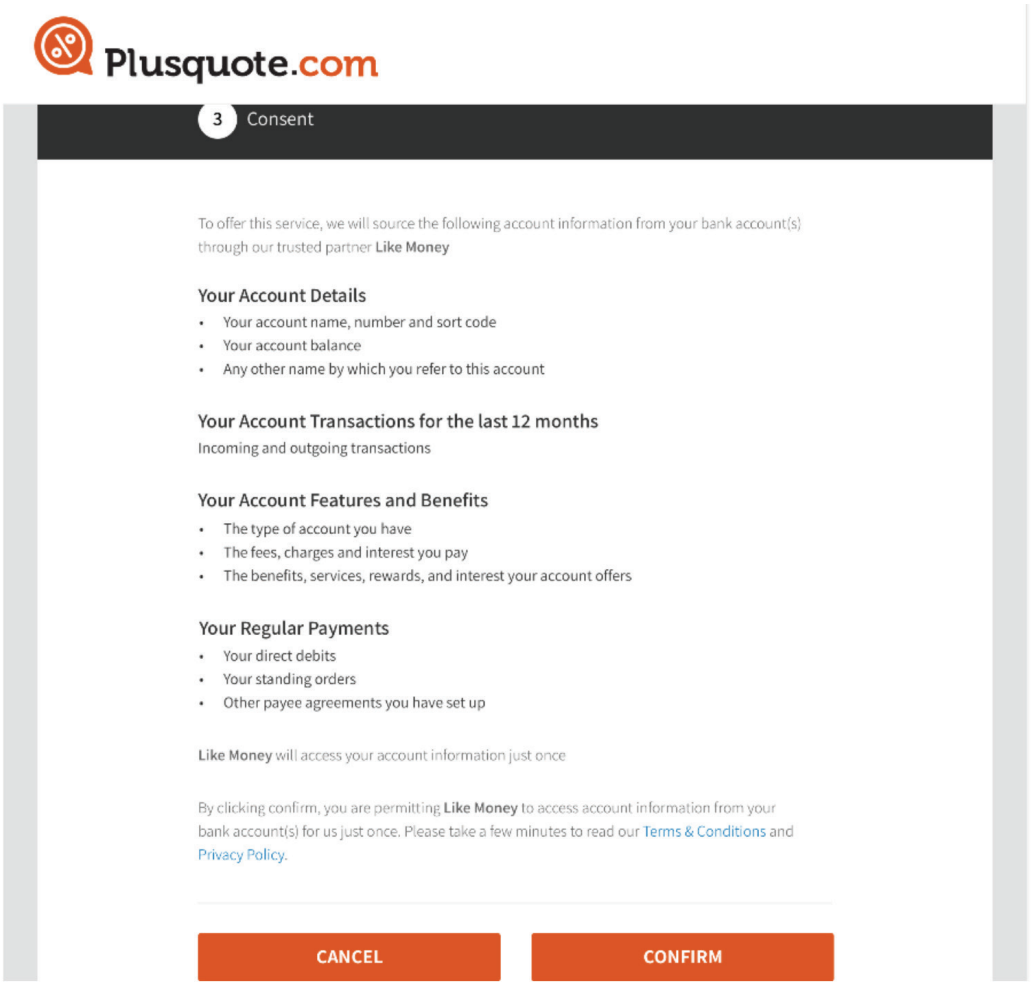


Figure 1.15 Multi-party TPP consent

After the customer has authenticated themselves with the ASPSP, the ASPSP should as part of the authorisation step, request authorisation from the customer for the regulated TPP making the account information request and the other TPP in the chain.

Find below an example of multi-party authorisation, here the ASPSP is requesting the customer to authorise the customer facing TPP 'Plusquote.com' and the ASPSP facing TPP 'Like Money', to access their account.

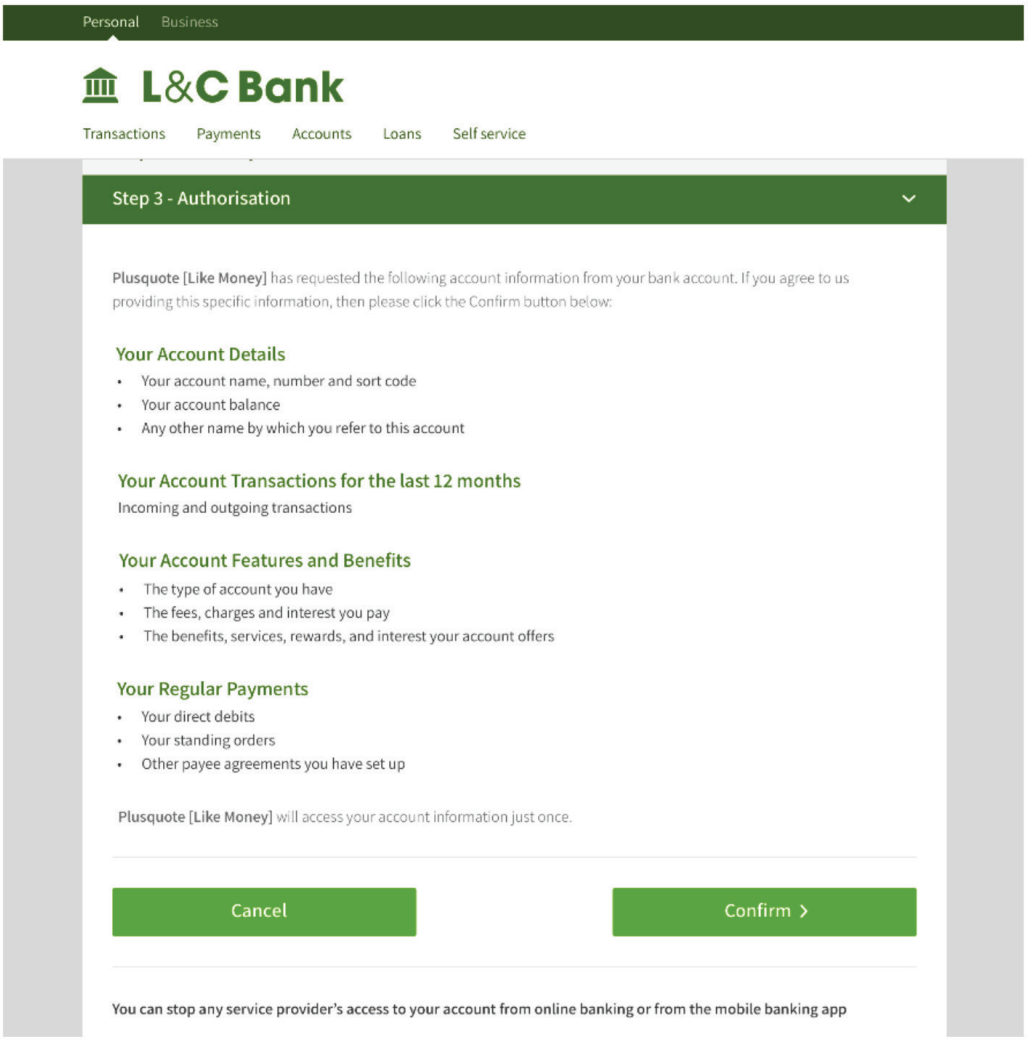


Figure 1.16 ASPSP displaying name of the customer facing TPP and ASPSP facing TPP

Both the regulated TPP making the account information request and the other TPP in the chain should be displayed within the Authorisation dashboard for each authorisation where multiple TPPs are involved in the chain. More detail is provided in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links).

7 Incremental Consent

It is possible that, after obtaining the PSU's consent, a TPP could enhance their offering and as a consequence require additional data to provide the enhanced service. There is currently no mechanism by which consent can be amended (e.g. add in the extra data elements required to provide the enhanced service). Therefore a TPP must issue a new consent request for all the elements required even if some of those elements were included in the previous consent.

Although this is effectively a new consent request, the TPP can present it to the PSU as an update (as shown in Figure 1.1) in line with how they have positioned their new service offering.

Figure 1.17 illustrates how a TPP can update consent. (The PSU can also see what they previously consented to).

It is important that the TPP shows all the elements of this new consent request to ensure consistency with the elements that are played back by the ASPSP in the authorisation step.

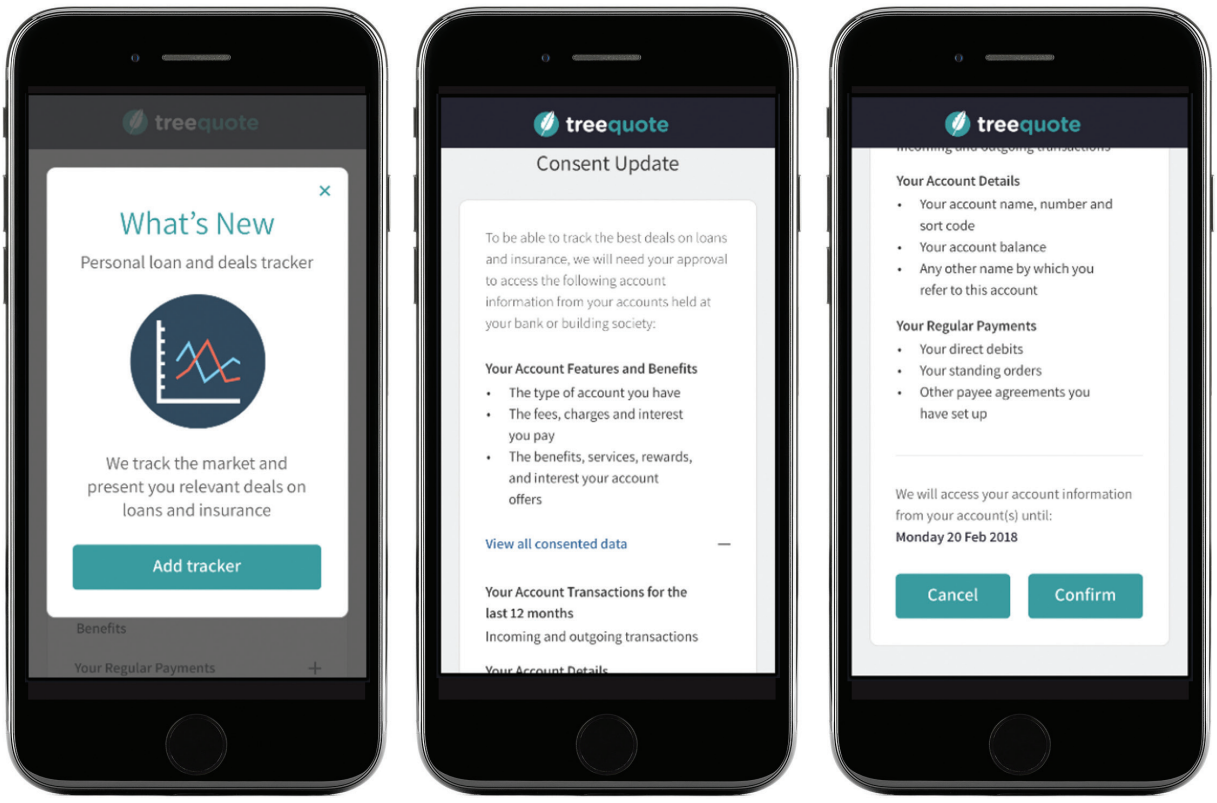


Figure 1.17 Incremental Consent

8 Revocation of Consent

A TPP that requests consent from a PSU should also make it as easy for the PSU to withdraw consent as it is to give it. The TPP should also inform the PSU how they can withdraw the consent.

PSUs should be able to revoke the consent at the TPP or the authorisation at the ASPSP with the same end result that the TPP is no longer able to provide the service.

The following sections look at how consent and authorisation can be managed by the PSU at the TPP and ASPSP respectively.

9 Management of consent at the TPP - Consent Dashboard

The OBIE research program found that the PSU preference for managing the consent previously given to a TPP was to do so via some form of dashboard.

This would be provided by the TPP and the PSU would see a list of ASPSPs that had been authorised to give access to that TPP. The PSU would then be able to 'drill down' into the detail of the consent the TPP originally requested. The PSU should then have the option to revoke that consent.

Figure 1.18 Shows how a PSU might view a consent dashboard and then revoke a specific consent (Figure 1.19).

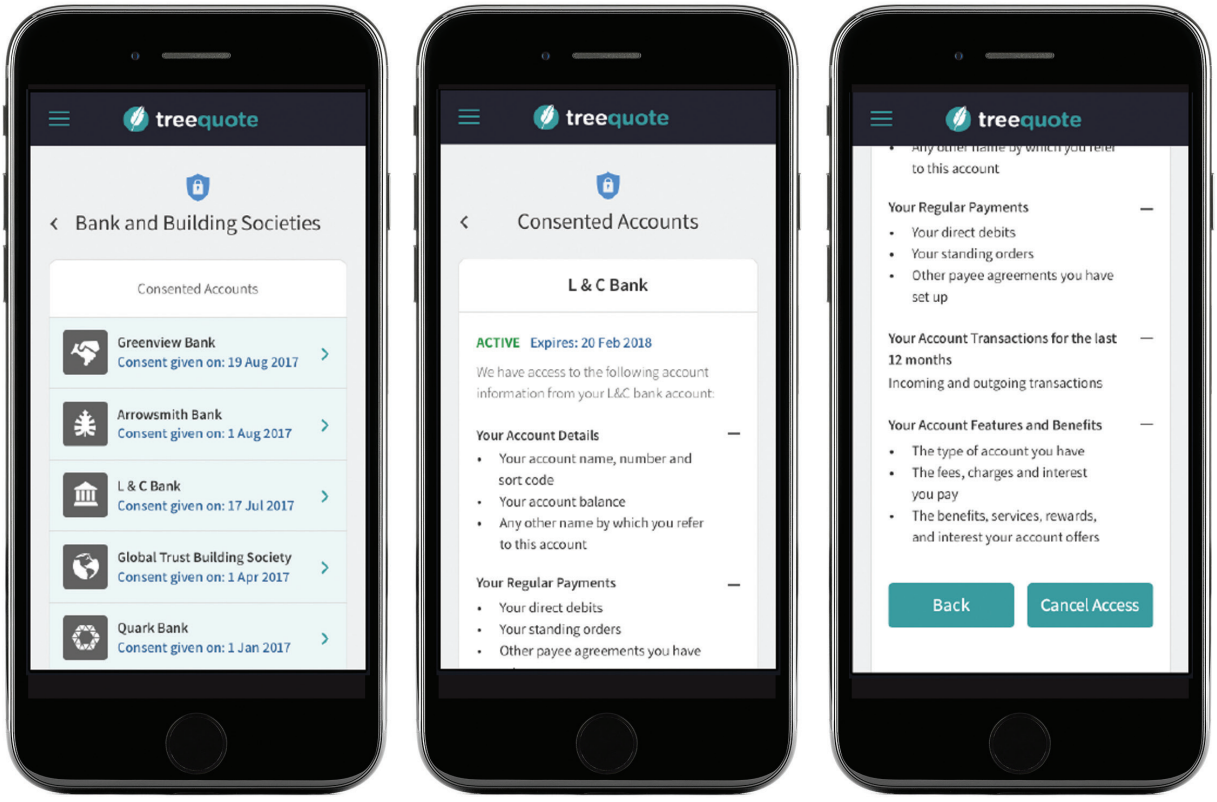


Figure 1.18 View Consent

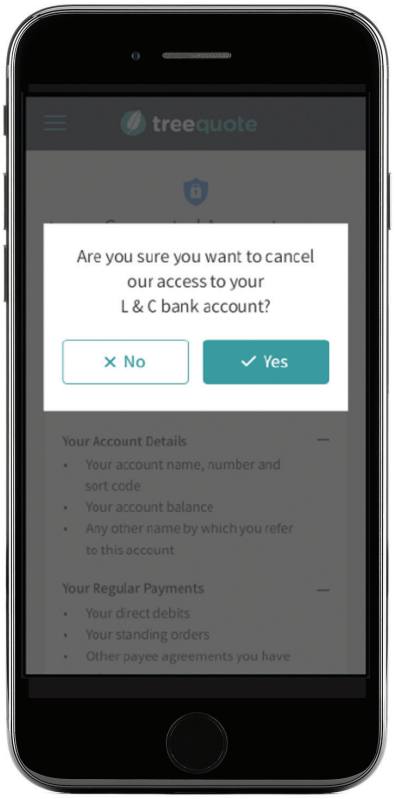


Figure 1.19 Revoke Consent

The Open Banking design only allows the full revocation of the consent with the TPP. PSUs cannot modify these consents (e.g. a PSU cannot revoke consent to share a specific data element included in the original consent).

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

1. The name of the TPP that requested the consent
2. The data requested
3. The purpose of the data request and how will the data be used
4. The period of which the transaction data was requested
5. When the TPP's access to the data will expire
6. The date the consent was granted

It should be noted that consent for single immediate payments cannot be revoked and therefore will not be stored and will not feature on dashboards.

10 Management of authorisation at the ASPSP - Authorisation Dashboard

OBIE customer research has indicated a preference on the part of PSUs to be able to view a list of authorisations on a dashboard provided by their ASPSP. The PSU should also have the ability to revoke those authorisations.

The Open Banking design only allows the full revocation of the authorisation with the ASPSP. PSUs cannot modify these authorisations (e.g. a PSU cannot revoke authorisation to share specific data elements included in the original consent). An example of an authorisation dashboard is shown in Figures 1.20 and 1.21

Revoking ASPSP authorisations could have unintended consequences at the TPP. Therefore, care should be taken with how this is presented to the PSU by the ASPSP. More detail is provided in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links).

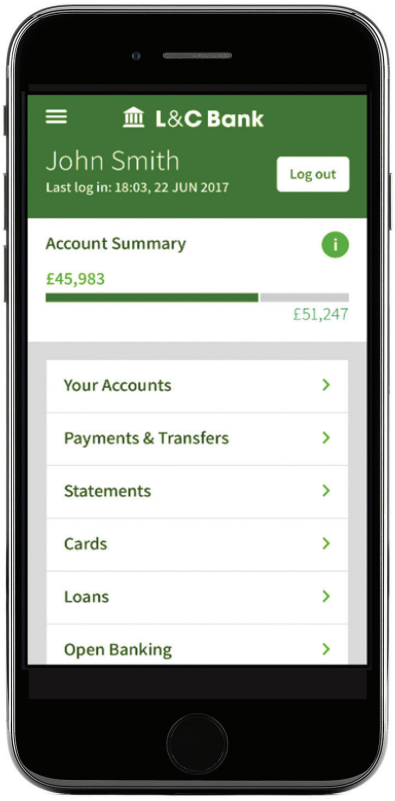


Figure 1.20
Bank account summary

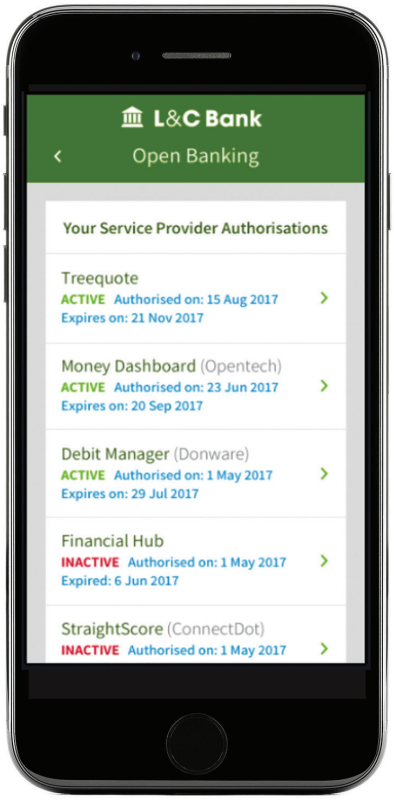
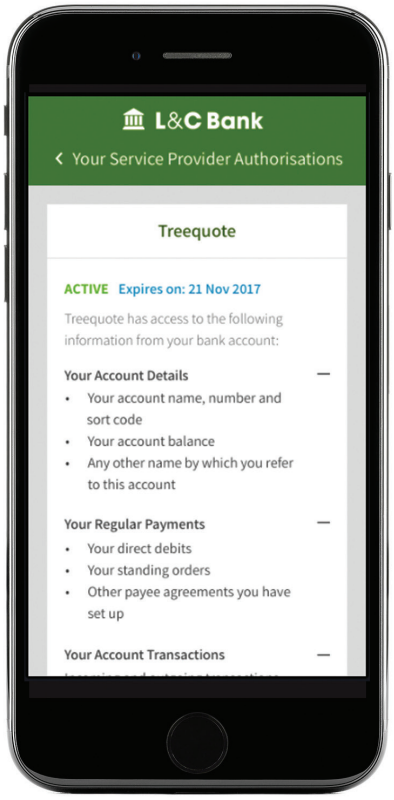


Figure 1.21
Open Banking Authorisation Dashboard

The PSU should be able to see the detail behind a specific authorisation (as in Figure 1.22) This detail should include:

1. The name of the TPP that requested the consent
2. The status of the authorisation e.g. Active/Inactive
3. The data that was requested
4. When the TPP's access to the data will expire
5. The date the authorisation was granted

The PSU should then have the option to revoke that authorisation (Figure 1.23)



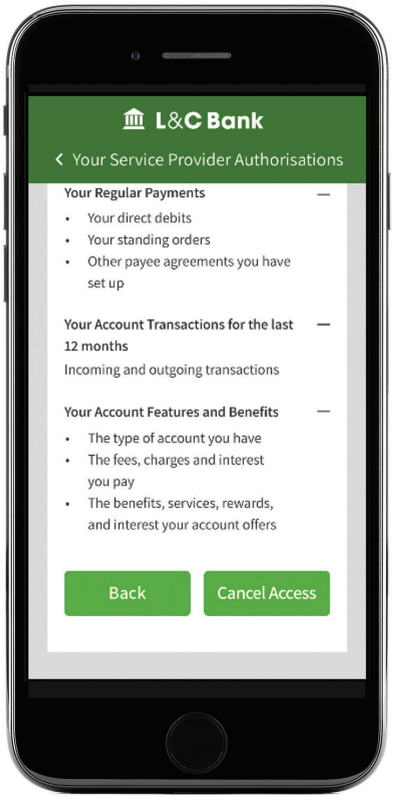


Figure 1.22 View Authorisation

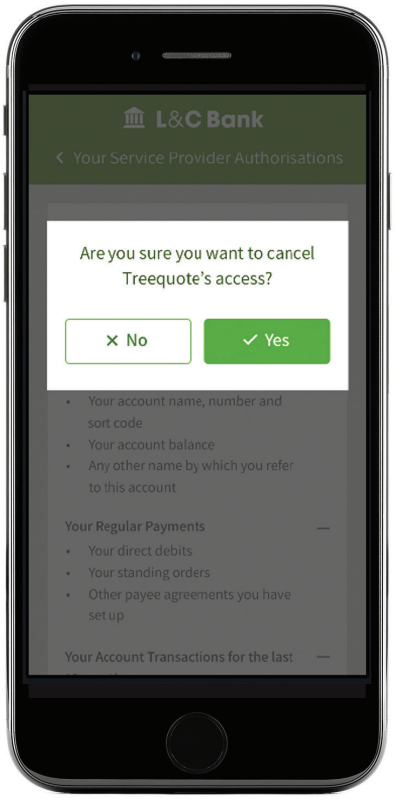


Figure 1.23
Revoke Authorisation

11 Consent communications and messaging

The choice of the language used in all of the example PSU journeys was informed by the OBIE program of customer research.

Use of this language by individual Participants would engender trust and encourage PSU take-up, an effect that would be reinforced if a consistent messaging framework is adopted across all participants.

Further details are provided in 'How to Guide: Consent Model, Part 2 - User Experience' (see Links).

12 Links

How to Guide: Consent Model, Part 2 - User Experience 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/KTD3lUJ3W#/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