

Considerations when using VRPs for Sweeping

The contents of this document do not constitute legal advice. Whilst this document has been drafted with regard to relevant regulatory provisions and best practice, it is not a complete list of the regulatory or legal obligations that apply to Participants. Participants are responsible for their own compliance with all regulations and laws that apply to them, including without limitation, PSRs, PSD2, GDPR, consumer protection laws and the FCA Handbook.

Date: 09 08 2021
Version: [3]
Classification: PUBLIC

Considerations when using VRPs for Sweeping Services

Contents

1.	Introduction	3
1.1.	Definition of sweeping	3
2.	Regulatory principles and consumer outcomes	4
2.1.	General considerations	4
2.2.	Vulnerable customers	6
2.3.	Summary	7
3.	Payment Services Regulations 2017	8
3.1.	Need to obtain customer consent	8
3.2.	The original payment order is not amended during the lifecycle of a VRP:	9
3.3.	Right to be refunded	10
3.4.	Right to withdraw consent	11
4.	Impact on proposition development	12
4.1.	Consideration of the end to end process	12
4.2.	Strong Customer Authentication	13
4.3.	Setting the appropriate consent parameters	13
4.4.	Visibility and Control	14
4.5.	Other considerations	15
4.5.1.	Insurance	15
4.5.2.	Complaints Process	15
4.5.3.	Redress Framework	18
5.	Examples of customer protections	19
6.	Appendix: Glossary	21

1. Introduction

In July 2021 the CMA announced that they had decided that implementing sweeping through VRPs is appropriate and proportionate and OBIE's proposed definition of sweeping is appropriate.

The purpose of this document is provide prospective sweeping service providers ("**SSPs**") with an overview of the key regulatory requirements they should take into account when designing any sweeping service offering and OBIE guidelines about what specifically SSPs might want to think about when considering those regulations in the context of sweeping.

1.1. Definition of sweeping

Sweeping is a generic term for the automatic movement of funds between accounts. For the purpose of the CMA Order, OBIE has proposed a specific definition, limited to the movement of a customer's own funds between accounts owned by them. Payments made to other individuals or other companies, e.g. paying for goods or services, would be excluded under this definition.

For a VRP transaction to be able to meet the definition of "Sweeping" it needs to meet the following criteria:

- i. The source account needs to be a PCA or BCA.
(PCAs or BCAs which require multi-authorisation are explicitly excluded from the definition. Joint accounts typically do not require multi-authorisation as both parties have full authority to make payments and so would be included in the definition.)
- ii. The destination account is any account into which a domestic payment can be made by the payer's bank's direct channel.¹
- iii. Both accounts are UK sterling accounts.
- iv. The payment can be an unattended payment, not requiring any interaction by or presence of the PSU at the time of making the payment²
- v. The transaction is between two accounts belonging to the same person or legal entity.³

¹ For example, savings accounts, building society savings accounts using a roll number, or personal credit card accounts are valid destination accounts.

² It should be noted that the customer will need to be present when the mandate for the payment service is set up.

³ For the avoidance of doubt, it should be noted that the destination account may not have a unique sort code and account number, for example e-money accounts, building society roll number accounts and head office collection accounts for loans and credit cards may have common sort code and account numbers but a unique reference in the transaction will ensure the payment is applied to the correct customer's account.

2.Regulatory principles and consumer outcomes

2.1. General considerations

All SSPs using VRPs would typically be conducting a combination of Account Information Services (“**AIS**”) and Payment Initiation Services (“**PIS**”) activities and so would be regulated by the FCA. For sweeping services the actors in the payment chain will be largely/wholly regulated by the FCA and/or the Prudential Regulation Authority. Therefore, firms offering sweeping services must conduct their business activities in a fit and proper manner, ensuring that their customers’ interests are adequately protected. This impacts not only the products and services offered by SSPs but also how those products and services are designed, managed and delivered. Consumer protection should demonstrably be at the forefront of an SSP’s product design process for any VRP-enabled sweeping proposition.

FCA regulated activity in the UK is underpinned by the FCA’s 11 Principles for Businesses. These are set out below.

The Principles for Businesses	
1. Integrity	A firm must conduct its business with integrity.
2. Skill, care and diligence	A firm must conduct its business with due skill, care and diligence.
3. Management and control	A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
4. Financial prudence	A firm must maintain adequate financial resources.
5. Market conduct	A firm must observe proper standards of market conduct.
6. Customers' interests	A firm must pay due regard to the interests of its customers and treat them fairly.
7. Communications with clients	A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.
8. Conflicts of interest	A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.
9. Customers: relationships of trust	A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment.
10. Clients' assets	A firm must arrange adequate protection for clients' assets when it is responsible for them.
11. Relations with regulators	A firm must deal with its regulators in an open and cooperative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice.

Table 1.– FCA’s Principles for Businesses

To support this, the FCA have provided clarity on the consumer outcomes they expect as a result of businesses adhering to Principle 6 and this will include providers of sweeping services. These are outlined below.⁴

TCF Consumer Outcomes	
Outcome 1	Consumers can be confident they are dealing with firms where the fair treatment of customers is central to the corporate culture.
Outcome 2	Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and are targeted accordingly.
Outcome 3	Consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale.
Outcome 4	Where consumers receive advice, the advice is suitable and takes account of their circumstances.
Outcome 5	Consumers are provided with products that perform as firms have led them to expect, and the associated service is of an acceptable standard and as they have been led to expect.
Outcome 6	Consumers do not face unreasonable post-sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint

Table 2. – Description of customer outcomes that are expected as part of the fair treatment of customers

⁴ See the FCA Handbook for more information

2.2. Vulnerable customers

Firms also need to ensure they consider the needs of their vulnerable customers, and the FCA have issued specific guidance⁵ on this to ensure vulnerable customers achieve good outcomes from the products and services provided.

The FCA recommend that firms should do the following:

- understand the needs of their target market / customer base;
- ensure their staff have the right skills and capability to recognise and respond to the needs of vulnerable customers;
- respond to customer needs throughout product design, flexible customer service provision and communications; and
- monitor and assess whether they are meeting and responding to the needs of customers with characteristics of vulnerability and make improvements where this is not happening.

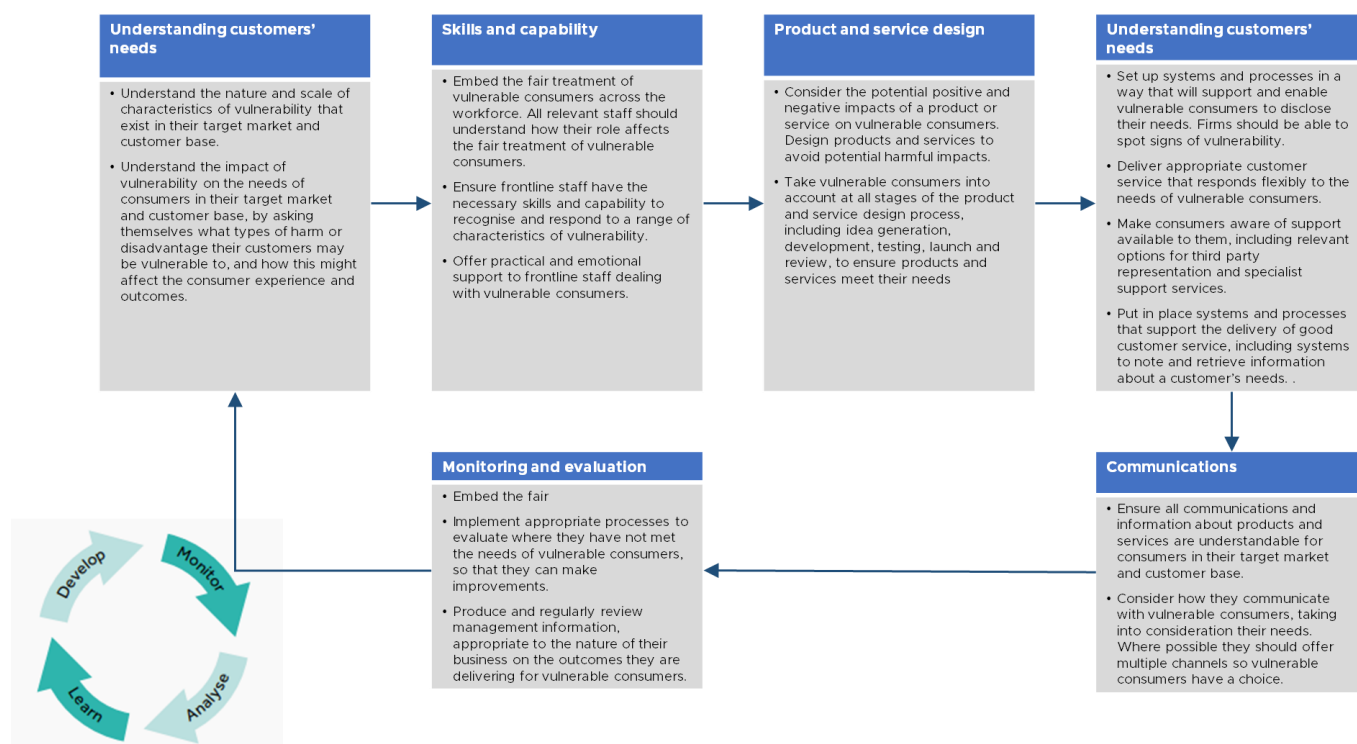


Figure 1. – Actions that firms should take to ensure they treat vulnerable consumers fairly, from FG21-1

⁵ See <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf>

2.3. Summary

In summary, the FCA expects regulated firms to put the wellbeing of customers at the very heart of how they run their business and how they design, manage and deliver their products and services (including products and services that use VRPs for sweeping purposes).

VRPs are a new product offering and SSPs who intend to provide this service to their customers should undertake a robust new product development process. SSPs must put their intended consumers at the heart of the decision making process when developing new products and services and consider issues such as:

- What is the target market, and why would the intended customers choose to use the services of the SSP?
- How will the SSP determine whether or not the needs of its intended and actual customers are met?
- What does the end to end customer journey look like (including the role of any other firms etc. that might play a role in proposition to the customer). What kinds of risks are posed, and how will the SSP keep this under regular review?
- Might the intended sweeping service use evolve or customer change? How will the SSP keep this under review to ensure protections etc. remain appropriate?
- How might the service impact vulnerable customers? Can protections be designed into the service offering?

Placing the needs of customers at the heart of new product development should enable SSPs to identify and consider the potential risks to customers when using sweeping-related products and services and what can be done to mitigate those risks.

An example of something that SSPs should consider and take into account when developing sweeping propositions is the nature of the destination account. Are transactions easily reversible? Are there risks associated with the destination account and will the intended customer be adequately informed of those risks? E.g. if the SSP is providing sweeping to an investment account, has the user been adequately informed that their capital might be at risk? Can the SSP demonstrate that it is sufficiently clear that e.g. investments might not be readily reversible and even if they are, that any sums returned might be less than the amount “swept” (or indeed be zero)?

This is just one example, and all SSPs should ensure they fully understand the legal and regulatory implications of providing sweeping services using VRPs and take appropriate advice.

SSPs should assess whether they need to seek individual guidance from the FCA when designing their sweeping propositions using VRPs.

3. Payment Services Regulations 2017

This section provides an overview of OBIE's understanding of key areas of regulation that are pertinent for use of VRPs for sweeping. However, ultimately interpretation of the regulations is a matter for the courts.

The Payment Services Regulations ("**PSRs**") do not prohibit the use of VRPs and expressly anticipate scenarios where multiple payments are made to the same payee(s), referencing "series of payment transactions"⁶, as well as, "recurring payments"⁷.

The PSRs place certain restrictions on payment service providers ("**PSPs**") that are relevant to VRPs and equally to other existing forms of recurring payments, such as standing orders, Direct Debit mandates and recurring transactions on a payment card.

In addition, the PSRs provide consumer protections, including: the need to obtain customer consent and the right to be refunded in the case of unauthorised payment transactions (regulations 67 and 76 respectively); redress in the case of defective payments initiated through PIS (regulation 93) and liability on PSPs for fees and charges incurred in connection with defective payments (regulation 94). These protections cover all forms of recurring payments, including VRPs.

In addition, PSPs are subject to various governance and prudential conditions, including the need to hold professional indemnity insurance to cover business activities in relation to payment services, including PIS and AIS. Again, this requirement applies to all PSP activities, including VRPs.

OBIE has outlined its view on the key regulatory considerations in more detail below. SSPs that are considering providing sweeping services should familiarise themselves with these statutory provisions and ensure that these are appropriately reflected in their service offering.

3.1. Need to obtain customer consent

The PSRs require a payment to be appropriately authorised by the payment service user ("**PSU**"). For the purposes of VRP payments, a PSU may provide their explicit consent to a PISP⁸ to initiate a series of payment transactions. For this consent to be valid, in the FCA's view it must be "clear, specific and informed"⁹. In the context of VRPs, the PSU can be treated as having given explicit consent for each VRP Payment under a VRP Consent, provided that the following consent parameters are met:

- i. the payee is fixed;
- ii. the number and/or frequency of payments is fixed (or capped); and
- iii. although the amount cannot be fixed in advance, there are clear parameters around the permitted value, such as maximum individual payment amount, maximum total value in a month or year etc.

Once the PISP has obtained the PSU's explicit consent, in order to set up the VRP it must successfully complete the VRP Consent Setup process. Practically this requires the PISP to

⁶ The PSRs definition of a "credit transfer" refers to a series of payment transactions, as does Regulation 67.

⁷ See Regulatory Technical Standards for Strong Customer Authentication UK-RTS

⁸ PSRs, Regulation 67(2)(c) read with regulation 69(2).

⁹ paragraph 8.151, FCA Approach Document

redirect the PSU to the domain of the ASPSP for the application of strong customer authentication (“**SCA**”). Following this, subsequent VRP payments can be made without the PSU being present by relying on the application of available exemptions by the ASPSP under the UK-RTS. For the majority of sweeping payments, OBIE believes that the UK- RTS Article 13 “trusted beneficiary exemption” is likely to be the most suitable (as the destination account will be established as a trusted beneficiary during VRP Consent Setup). There may be instances when payments are swept into accounts held at the same ASPSP and the account is in the name of the payer, in which instances UK – RTS Article 15 “payment to self” exemption may be more suitable.

The VRP Consent Parameters provide details around the parameters of a series of payments that the PSU is authorising the PISP to initiate on their behalf. It is the responsibility of the PISP to ensure that it obtains explicit consent from the PSU and any subsequent VRP payments are initiated within those consent parameters. Similarly, the ASPSP must ensure that it does not execute VRP payment orders outside of the payment parameters.

3.2. The original payment order is not amended during the lifecycle of a VRP:

When VRPs are used to support sweeping services they will by definition involve the PSU consenting to a series of payment transactions to the same payee where the exact amount of each payment transaction is unknown in advance, but within defined parameters. The fact that a PSU has consented to the VRP Consent Parameters as part of the VRP Consent Setup should in our view enable PISPs to adhere to the requirement under regulation 69(3)(h) of the PSRs not to change any feature of a transaction notified to it by the payer, provided that the payment order is within that range/subject to that limit. There is no requirement in the PSRs that a customer’s consent relates to an exact amount nor is there any prohibition against the use of a range, maximum payment amount or other similar limits. In the context of VRPs, the ‘amount’ referred to should be treated as the cap or range agreed to by the PSU in the original mandate. Once an individual payment order has been initiated under a VRP, the PISP must provide or make available certain information to the PSU, including confirmation of successful initiation, amount (including any charges) and a reference number.¹⁰

A PISP cannot change or exceed the VRP Consent Parameters, the payee and frequency (or maximum number) of transactions. These are fixed by the PSU in the VRP Consent Setup. Unauthorised changes by a SSP would make the resulting payments unauthorised. Please see section 4.3 for further considerations on consent parameters.

¹⁰ PSRs, Reg.44(1)

3.3. Right to be refunded

The PSU has the right to be refunded for:

i. Unauthorised Payments

These are transactions where the PSU did not agree to, or was not aware of, the transaction or its terms. A transaction that is not consistent with the customer's VRP Consent Parameters would be unauthorised. As referenced in section 3.1 the PISP must seek consent that is clear, specific and informed. The PISP must ensure that the VRP Consent Parameters are sufficiently narrow to support the service being offered to the customer, so that they can be confident they have received the customer's explicit consent, as without it the transactions would be considered unauthorised. See Section 4.3 for more details on appropriate consent parameters. Under regulation 76 of the PSRs, if a payment is unauthorised the customer is entitled to a refund "as soon as practicable, and in any event no later than the end of the business day following the day on which it becomes aware of the unauthorised transaction".

Customers that lose out as a result of unauthorised VRP payments will be entitled to a refund from their ASPSP without having to wait for the resolution of any dispute between the ASPSP and the PISP, in the same way that they would for any other unauthorised payment type within the scope of the PSRs. The ASPSP has a right to request compensation from the PISPs for the amount refunded to the customer if the PISP cannot prove that they were not at fault.

ii. Defective Transactions

These are transactions where the customer agreed to the transaction but there was an error in the way the payment was made, for example if the payment was made late or was not made at all. In this scenario, the customer could approach their ASPSP in the first instance for a refund. If the ASPSP does refund the customer, the ASPSP would then have a right of recourse against the PISP. The PISP would need to prove that they were not at fault, failing which they would have to compensate the ASPSP for the amount refunded to the customer. This is set out in more detail under PSRs, Regulation 93. It is possible that there are some instances where neither the PISP nor the ASPSP have all the required information to resolve the issue as to who is responsible. ASPSPs and PISPs are encouraged to develop arrangements that support both the exchange of information and issue resolution¹¹.

A PSU may also approach a PISP directly in the case of unauthorised or defective payments. In the case of sweeping OBIE believes that PSUs will probably approach the SSP in the first instance, as they hold the customer relationship for the sweeping service.

There is also a liability on PSPs for fees and charges incurred as a result of the actions of a PSP (Regulation 94), so PSUs are protected not just for the funds transferred but also additional fees or charges incurred.

¹¹ All of the CMA9 and many other ASPSPs and TPPs use the OBIE's Dispute Management System (DMS) platform for information sharing but there is no requirement to use this system and other options are available.

3.4. Right to withdraw consent

Payment service providers offering sweeping services using VRPs should notify their customers of the procedure for withdrawing their VRP Consent, which can be achieved by including clear provisions within their contract with the PSU. It is expected that this will include a simple mechanism to revoke consent if the customer no longer wishes to use their service. Under regulation 67(4) of the PSRs, a customer has the right to withdraw their consent to the execution of a series of payment transactions at any time, enabling all future payments to be stopped once consent has been withdrawn. Once the customer has withdrawn their consent, then any payment transactions executed after the time of withdrawal will be unauthorised payment transactions and so subject to the above protections.

4. Impact on proposition development

There are a number of considerations SSPs need to bear in mind when developing sweeping propositions using VRPs:

4.1. Consideration of the end to end process

All regulated firms are expected to consider the full end to end customer journey as part of their product development and management processes (See section 2). When developing sweeping services using VRPs, SSPs need to ensure that they pay due care and attention to ensuring that their products and services are designed with customer protection at their heart and in accordance with all applicable regulations. Two examples of such considerations are provided below (we have taken these from risks cases highlighted to OBIE in the course of its consultation):

Example 1:

If an SSP is enabling a lending company to use VRPs as part of a revolving credit proposition (such as an alternative to an overdraft), then the VRP would be subject to the same restrictions as other Continuous Payment Authorities (CPA's) under CONC¹². The SSP would be expected to conduct a risk assessment of the firms they are contracting with in provision of this provide service to customers, including whether they are confident that the firm will not misuse the VRP capability. For example, are the VRP Consent Parameters appropriate based on the specific credit permission in terms of frequency, duration and absolute amounts? This provides an additional level of protection in addition to the obligations on the regulated credit provider.

Example 2:

If a sweeping service involves the use of AIS permissions to establish when payments should be made, there is a risk that a lender could misuse this information. Under regulation 70(3)(f) of the PSRs, an AISP cannot *"use, access or store any information for any purpose except for the provision of the account information service explicitly requested by the payment service user"*. An attempt to access account information for other purposes (such as attempting to identify when to seek repayment of a credit facility) would be considered a breach of the PSRs.

Note - this risk exists independently of whether an SSP uses VRPs for sweeping or uses an alternative funds transfer mechanism.

SSPs proposing to offer these types of services will need to assess how the services will be used and what controls it needs to put in place. The SSP will need to be clear what the customer has authorised AIS to be used for, and the VRP Parameters must also be designed to provide appropriate protections.

¹² See CONC 4.6 and CONC 7.6

4.2. Strong Customer Authentication

The design of the VRP functionality in OBIE Standard 3.1.9 (“**VRP Standard**”) requires the application of strong customer authentication by the ASPSP in setting up the VRP Consent Parameters. This is in contrast to Direct Debits where no transaction is subject to SCA or continuous payment authority on debit cards where the initial transaction may be subject to SCA but future transactions are not. For sweeping, the OBIE VRP Standard requires the VRP Consent Parameters to include:

- Payee Account Name
- Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN)
- Maximum amount per payment
- Maximum amount per frequency (Day/Week/Fortnight/Month/Half Year/Year) and Currency
- Expiry Date

As the initial VRP Consent Setup will be subject to SCA, the ASPSP will have the relevant customer-approved VRP Consent Parameters and will be required to execute payment transactions within those parameters. If the ASPSP executes a payment transaction outside the VRP Consent Parameters, then this will be an unauthorised payment. Similarly, if a PISP initiates a payment transaction outside the VRP Consent Parameters, then it will not have done so in accordance with the customer’s consent. Customers that lose out as a result of unauthorised VRP payments will be entitled to a refund from the ASPSP without having to wait for the resolution of any dispute between the ASPSP and the PISP, in the same way that they would for any other unauthorised payment type within the scope of the PSRs (See section 3.3).

4.3. Setting the appropriate consent parameters

Prospective SSPs should bear in mind that where a customer is permitted to specify inappropriately broad VRP Consent Parameters (e.g. a relatively high maximum payment value per payment), then it may be more likely that a question could arise as to whether or not the consent is sufficient for the purposes of the PSRs, even if a payment transaction is executed within those VRP Consent Parameters. In this respect, the PSRs refer to the payer having given “explicit consent” or “explicitly requested” (under regulation 69) and so if the consent parameters are not sufficiently narrow it may be reasonable to conclude in the event of a dispute/regulatory action that the customer has not given explicit consent. If the transaction was deemed unauthorised because the VRP Consent Parameters were not sufficiently narrow, the PISP may need to compensate the ASPSP, if they have refunded the customer in these circumstances.

SSP’s may wish to monitor the VRP Consent Parameters and regularly review the “headroom” between actual transactions and the parameters, resetting parameters as they deem appropriate in order to attempt to mitigate these risks. This is likely to be very fact specific and to depend on the context, including the customer’s experience of the service in practice. The customer is protected if any payment transaction is executed without appropriate consent having been given in accordance with the PSRs because the transaction will be considered unauthorised. This provides a clear incentive for PISPs to ensure that the range that is specified in the VRP Consent Parameters is such that any payment within that range would be reasonably expected by the customer. Clearly, increased specificity and narrowness in terms of the VRP Consent Parameters will give increased certainty that explicit consent has been obtained and this protects both PISPs and customers.

The appropriate level of parameters will be unique to the different use cases and firms also need to consider the customers' individual circumstances when setting up consent parameters. Some examples of considerations that firms might want to consider are included in the table below.

Use Case	Potential Parameter Considerations
Subscribing to a fixed term savings plan (e.g. Christmas savings club)	The duration of the consent parameters should not exceed the duration of the plan and the maximum level should be reasonable in light of the customer's financial position (e.g. ensuring they have sufficient funds to cover living expenses)
Sweeping round up transactions into a savings account	The parameters governing frequency of sweeping should align to the agreement in the sweeping service. (e.g. if the service specifies weekly sweeping, then the VRP parameters should reflect that), and the maximum amount per transaction should reflect that these will be a combination of a number of individual transactions that are each less than £1 each (if proposition is to round up to the nearest £1).
Sweeping excess cash into a savings account	The parameters governing the maximum amount that can be swept into savings should be lower than the customer's income less "essential outgoings".
Repaying a loan	The frequency and quantity of the repayment schedule should align to repayment schedule in the loan agreement. If the borrower falls into arrears and the lender wishes to make use of a VRP to conduct additional collections of funds this would have to be specifically agreed with the customer.
A savings plan that has not been used for a period of time	A customer may have set up an enduring savings plan and so the VRP Consent Parameters had an open ended expiry date. If the customer's circumstances are such that the plan has not been used for a number of months the PISP needs to consider whether they still have the customer's explicit consent to conduct that transaction. This will be dependent on the specific proposition and the communications between the PISP and the customer. PISP's may be aware that a Direct Debit mandate expires if it has not been used for 13 months but the PISP may choose a shorter period of time to reconfirm explicit consent with the customer.

Table 3. – VRP Consent Parameter Guidance

4.4. Visibility and Control

As mentioned in section 3.4, the PSRs require the PISP to provide a clear and transparent way for the customer to be able to withdraw their consent. Even though the PSU can revoke VRP access at the ASPSP, this does not negate the obligations on the SSP to provide their customers with the means to revoke the VRP consent provided. Furthermore, under the obligations of Treating Customers Fairly, (TCF Outcome 3), the SSP has obligations to provide its customers with appropriate levels of visibility and control over the services offered.

The SSP will determine exactly how it provides visibility and control to its customers. See Figure 2. for an example from the Customer Experience Guidelines on how a user might revoke consent for a VRP they had set up.

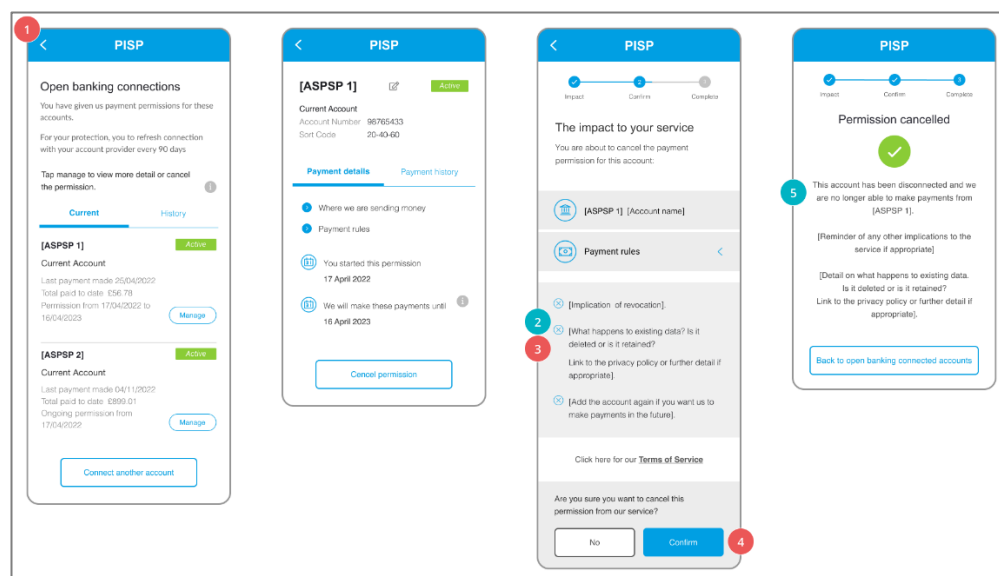


Figure 2. – Examples from the Customer Experience Guidelines

The Customer Experience Guidelines¹³ provide further guidance on OBIE's expectations on ASPSPs (Access Dashboards) and TPPs (Consent Dashboards).

4.5. Other considerations

4.5.1. Insurance

In addition, PSPs are subject to various governance and prudential conditions, including the need to hold professional indemnity insurance to cover business activities in relation to payment services, including PIS and AIS. Again, this requirement applies to all PSP activities and would include VRPs.

4.5.2. Complaints Process

An SSP must have an appropriate complaints process for all their services, including provision of VRPs. This section highlights some of the elements firms will want to consider to ensure they have suitable processes and procedures for handling customer complaints.

The rules for handling complaints from eligible complainants are set out in DISP¹⁴ (the Dispute Resolution: Complaints sourcebook in the FCA handbook) and differ depending on whether the complaint is a PSD/EMD complaint or not.

The rules for handling PSD/EMD complaints from non-eligible complainants are set out in PSRs, Regulation 101.

¹³ <https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/>

¹⁴ <https://www.handbook.fca.org.uk/handbook/DISP.pdf>

The decision tree set out below (See Figure 3.) indicates which complaint handling rules apply in different circumstances.

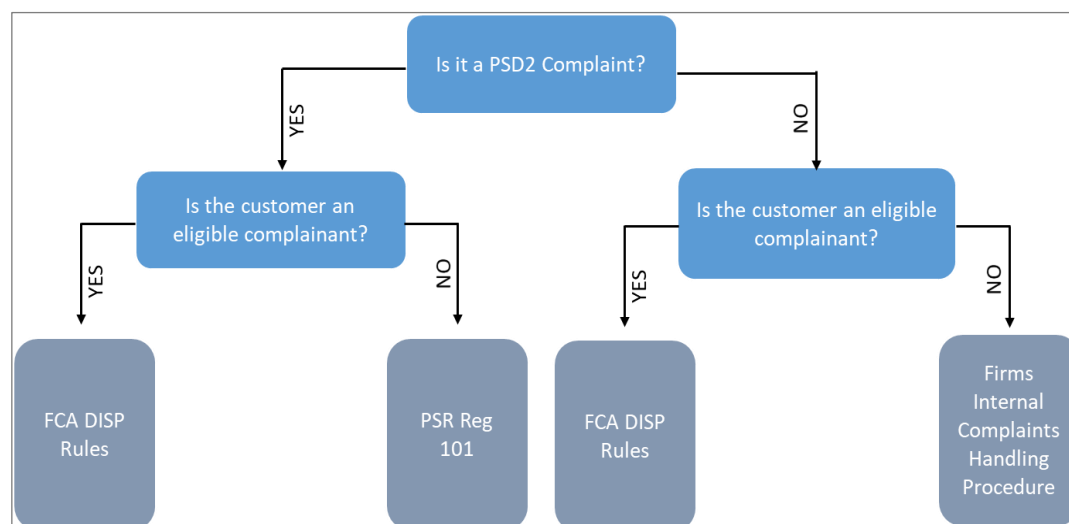


Figure 3. - Complaint handling rules decision tree

An eligible complainant is anyone who is eligible to bring a complaint to the Financial Ombudsman Service (FOS).

Access to the FOS is available to consumers, micro-enterprises, small charities and small trusts. You can find the definitions of these at 11.36 of The FCA's Approach Document¹⁵. In addition, the Financial Ombudsman Service host an eligibility checker for SMEs on their website¹⁶.

Summary of Complaints sourcebook (DISP) Rules

The rules on handling complaints from eligible complainants are set out in DISP¹⁷. These cover a range of issues, including:

- a. Consumer awareness:
PSPs must provide information concerning their internal procedures for complaints handling. This should provide adequate information on how customers can access the complaints process. PSPs must maintain complaints procedures and policies, which are easily accessible and transparent. PSPs also need to make information about the FOS and customer's rights of redress through FOS easily accessible. The customer should be able to complain by 'any reasonable means'. PSPs must ensure that freephone or standard charge numbers only are used, rather than premium rate lines.
- b. Internal complaint-handling procedures:
PSPs must investigate complaints "competently, diligently and impartially, and assess the complaint fairly, consistently and promptly". Organisations should have internal

¹⁵ <https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf>

¹⁶ <https://sme.financial-ombudsman.org.uk/complain/can-help/our-eligibility-checker>

¹⁷ <https://www.handbook.fca.org.uk/handbook/DISP/>

complaints handling policies and procedures and the complaints handling literature they provide to customers must reflect the DISP requirements and PSPs must take reasonable steps to ensure that in handling complaints it identifies and remedies any recurring or systemic problems, for example, by root cause analysis. The PSP should also analyse any patterns in determinations by the Ombudsman and reflect this in future approaches to compliant handling.

- c. Co-operation with the Financial Ombudsman Service:
PSPs must fully co-operate with the Financial Ombudsman Service and comply promptly with any settlements or awards made by it.

Summary of complaint handling timeframes as outlined in the FCA Approach Document

When dealing with a complaint, PSP must provide a full written response within 15 business days, or 35 business days in exceptional circumstances. (For non-PSD2 complaints this is 8 weeks). Payment service providers must inform a customer within 15 business days if their complaint is considered to involve exceptional circumstances and indicate the reasons for the delayed response.

The three business day rule¹⁸ allows organisations to handle complaints less formally, without sending a final response letter, so long as the complaint is resolved to the complainant's satisfaction within three business days after the organisation receives the complaint. In these circumstances the organisation will not have to send a final response letter, tailored to the specific complaint and individual concerned. Instead, organisations have to send a written, 'summary resolution communication', which is a simpler, template message.

Complaint Recording & FCA Reporting

Organisations must maintain a record of all complaints for at least three years. Organisations must submit a report to the FCA annually, including the number of complaints received, the root cause, how many were closed or upheld, and the total amount of redress paid. If the organisation has received over 500 complaints in a report period, it must publish a summary of the complaints data it has submitted in the report to the FCA, usually on its website. Payment service providers must complete the new Payment Services Complaint Return on an annual basis.

¹⁸ See DISP 1.5

4.5.3. Redress Framework

If a PSU is not satisfied with how their complaint was dealt with they may be able to refer their complaint to the Financial Ombudsman Service (FOS). The FOS operates the alternative dispute resolution (ADR) procedure for payment service users required by PSD2. FOS is a statutory, informal dispute-resolution service, established under FSMA. It provides an accessible alternative to the civil courts. Its role is to resolve disputes between eligible customers and financial services organisations quickly, impartially with minimum formality, on the basis of what is fair and reasonable in the circumstances of each case. In adjudication, FOS will consider the relevant laws and regulations, the regulator's rules, guidance and standards, as well as codes of practice, and what is considered to be good industry practice at the relevant time.

The FOS can consider complaints which relate to acts or omissions of regulated firms in carrying on one of the specified list of activities.¹⁹ Those activities include 'payment services' which includes both account information services and payment initiation services so the activities of SSPs clearly fall under FOS jurisdiction

¹⁹ See DISP 2.3

5.Examples of customer protections

During the Sweeping and VRP consultation process a number of respondents raised questions about the protections afforded to customers when VRPs were used to support sweeping. Key questions are considered in the table below:

Questions Raised	Response
Are VRPs offered the same protections as CPAs in CONC regulation?	When used to collect funds as part of a credit agreement VRPs would meet the definition of CPAs in CONC regulation and so VRPs cannot be used by lenders to avoid the rules on CPAs in CONC.
Customer disputes the amount of a sweeping transaction.	<p>If transaction is outside of the VRP Consent Parameters, then it is an unauthorised transaction and customer entitled to a full refund. (See section 3.3)</p> <p>If transaction is within the VRP Consent Parameters but these were not set sufficiently narrow then the transaction may be unauthorised and the PSU could be entitled to a full refund. (See section 4.3)</p> <p>If the transaction is within appropriately defined VRP Consent Parameters but the SSP should not have initiated the transaction then the PSU could complain to the SSP. (See section 4.5.2). If the PSU was not satisfied with how the complaint was dealt with, they could seek refer the complaint to the FOS for independent consideration. (See section 4.5.3)</p>
Customer disputes the number of sweeping transactions (SPP has been moving 2 transactions per month but in 1 month makes 4 transactions).	The customer could complain to the SSP that the service was not as expected. (See section 4.5.2). If the PSU was not satisfied with how the complaint was dealt with, they could seek refer the complaint to the FOS for independent consideration. (See section 4.5.3)
Customer complains that the Saving sweeping service caused them to move into overdraft causing them to incur fees as funds were moved before they made a one off purchase.	<p>The customer could complain to the SSP that the service received was not as expected. (See section 4.5.2).</p> <p>Customer could complain to their ASPSP who could refer the customer to the SSP (see above). If the ASPSP chose to refund the customer, the ASPSP could seek redress from the PISP (see section 3.3). whether the ASPSP was entitled to the refund will be determined by the specifics of the individual case.</p> <p>If the PSU was not satisfied with how the complaint was dealt with, they could seek refer the complaint to the FOS for independent consideration. (See section 4.5.3)</p>
Funds not received at the beneficiary account due to an error at the ASPSP or the PISP	<p>The customer could complain to either the ASPSP or the PISP who would need to investigate the complaint and take appropriate action based on who was at fault for the defective transaction. (See section 3.3 and section 4.5.2).</p> <p>If the PSU was not satisfied with how the complaint was dealt with, they could seek refer the complaint to the FOS for independent consideration. (See section 4.5.3)</p>
Customer cancels the VRP at the SSP but a transaction takes place after cancelation.	<p>Customer can complain to the SSP. As this is an unauthorised transaction the SSP has to refund the PSU (Section 3.3).</p> <p>Customer can complain to the ASPSP. If the customer provides evidence of cancelation the ASPSP can determine that this is an unauthorised transaction and provide a refund to the PSU and seek redress from the SSP. (Section 3.3). If the ASPSP is unable to determine</p>

	<p>that the transaction is unauthorised then they may choose to refer the PSU to the SSP, or to follow their usual complaints procedure.</p> <p>If the PSU was not satisfied with how the complaint was dealt with, they could seek refer the complaint to the FOS for independent consideration. (See section 4.5.3)</p>
Customer advises that the payee account is not in their name (as they input incorrect destination account details when setting up the sweeping service).	<p>Customer can complain to the ASPSP. If the account is not in the customer's name then the transaction will be unauthorised (it cannot be an authorised sweeping transaction), so the ASPSP will refund the customer and seek redress from the SSP. (Section 3.3).</p> <p>Customer can complain to the SSP. As the destination account is not in their name is it not a Sweeping transaction and so the consumer could claim that that this is an unauthorised transaction and the SSP must refund the customer.</p> <p>If the PSU was not satisfied with how the complaint was dealt with, they could refer the complaint to the FOS for independent consideration. (See section 4.5.3)</p>

Table 4. – Examples of Customer Protections

6. Appendix: Glossary

AIS	Account Information Service, the provision of account information service carries out by an Account Information Service Provider (AISP), which is authorised and regulated by the FCA.
ASPSP	Account Servicing Payment Service Provider (ASPSP) is any financial institution that offers a payment account with online access. This includes banks and building societies.
Payer	Payer means—: (a) a person who holds a payment account and initiates, or consents to the initiation of, a payment order from that payment account; or (b) where there is no payment account, a person who gives a payment order;
Payment Order	“Payment order” means any instruction by a payer or a payee to their respective payment service provider requesting the execution of a payment transaction
PIS	Payment Initiation Service, the initiation of a payment from a customer’s account carried out by a Payment Initiation Service Provider (PISP), which is authorised and regulated by the FCA.
Sweeping	Sweeping is a generic term the movement of funds between a customer’s own accounts, a “me to me” transaction. For the purpose of the Order and following the consultation process OBIE recommends the following definition of Sweeping: <ul style="list-style-type: none"> • The source account needs to a PCA or BCA. • The destination account is any account into which a domestic payment can be made by the debtor bank’s direct channel. • Both accounts are UK sterling accounts. • The payment can be an unattended payment, not requiring any interaction by or presence of the PSU at the time of making the payment • The transaction is between two accounts belonging to the same PSU.
Sweeping Access	Provision of access to the VRP APIs, for the purpose of delivering Sweeping. OBIE is currently assessing whether to recommend to the Trustee whether mandating Sweeping Access on the CMA9 would be an effective and proportionate remedy.
Sweeping Services Provider (SSP)	This is a firm which provides Sweeping services to its customers. The firm is likely to hold an AIS permission, to enable the interrogation of the PSUs account to determine if it is appropriate to initiate a sweep of funds, and also a PIS permission so it can use of VRPs to enable Sweeping. For clarity, an SSP is not a separate permission but is a term that OBIE uses to refer to this business model, rather than a term used by the FCA or in the PSRs.
UK-RTS	UK-RTS are the technical standards included in the FCA Handbook to meet the requirements for Secure Customer Authentication
VRP Consent	VRP Consent is the consent provided by the PSU for a PISP to initiate a series of payments that fall within the agreed VRP Consent Parameters. The VRP Consent includes the specific values of the VRP Consent Parameters and must be authorised by the Payment Service User (“PSU”) via Strong Customer Authentication (“SCA”) at their ASPSP
VRP Payments	VRP Payments are one or several payments made using a long -held consent (“VRP Consent”) the VRP Consent Parameters are included within the VRP Consent and are therefore subject to SCA of the PSU by the ASPSP as part of the VRP Consent Setup.
VRP Consent Parameters	The VRP Consent Parameters are the parameters that are recorded in the VRP Consent, in a sweeping transaction they consist of: <ul style="list-style-type: none"> • Payee Account Name • Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN) • Maximum amount per payment and Currency • Maximum amount per frequency (Day/Week/Fortnight/Month/HalfYear/Year) and Currency • Expiry Date (Ongoing or a Specific Date) • Consent Reference

	See standard v 3.1.9 for more details
VRP Consent Set Up	VRP Consent Set Up is the activity of providing the VRP Consent and authorising it via Strong Customer Authentication (“SCA”) at their ASPSP