OPEN BANKING

Mitigating the risks of financial crime

Framework for data collection on financial crime

October 2023

Contents

1. Executive Summary

One of the JROC actions is to design and implement a mechanism for collecting data that provides an informed view of the nature and extent of economic crime occurring in open banking payments. Participants have highlighted that fraud is already occurring in this context but there is limited available evidence to assess the impacts or respond by developing risk mitigation measures.

Availability of relevant and accurate data will help to resolve this. The need for this data will continue to increase as the volume of transactions grows and the ecosystem expands.

We have consulted widely on how best to achieve this objective and for the reasons set out in this report recommend that the key elements of the framework are as follows:

1.1 The framework has been specifically developed to build on existing data collection activities, incorporating used approaches, metrics and definitions so the additional requirements are incremental rather than completely new.

1.2 That the initial framework supports the gathering of data relevant to payment fraud with consideration of aggregation of data relating to broader financial crime to follow.

1.3 That data is provided exclusively by sending PSPs to avoid data duplication and reconciliation challenges.

1.4 That the metrics requested from contributors and the timing of data submission provide a statistical database of fraud, as well as relevant and timely intelligence for preventative purposes.

1.5 That metrics include fraud broken down by authorised push payment (APP) fraud, with the latter broken down into industry-used subcategories, consistent with how fraud is reported elsewhere by the industry.

1.6 A specific data component is included to establish how open banking fraud rates vary across Payment Initiation Services Providers (PISPs) which initiate payments.

1.7 Monthly transactional data is obtained in the collection process to allow a ratio of **fraud: successful payment** to be calculated (this is vital for making cross-comparisons between firms and between channels).

1.8 Although it is useful and necessary to make comparisons on fraud performance between the open banking and ASPSP's own channel, existing UK Finance data can be effectively used for computation, rather than asking firms to duplicate reporting.

Feedback from 10 ASPSPs, accounting for over 85% of Faster Payments Service (FPS) payments, indicates that they are likely to provide the required data from the start of Q4 2023. This would enable us to produce an initial report by the end of 2023. Most firms also indicate that they will be able to provide historical data for the 18-month period to end June 2023, which will enhance the ability to see trend data from the outset.

2. Background and Objectives

On 17 April 2023 the Joint Regulatory Oversight Committee (JROC) published its Recommendations for the next phase of open banking in the UK (referred to as "the JROC report").

In this report, the committee identified and set out a roadmap of 29 actions. This document focuses on one of these actions: "*Design a data collection framework for financial crime and submit to the FCA and PSR for approval*." This is "*the Financial Crime Framework*".

This action rests under the theme of "Mitigating the risks of financial crime" (paragraphs 4.16 - 4.30), and paragraph 4.16 sets out the overall objective:

> *4.16 "All those involved in open banking need to effectively mitigate risks and ensure consumers are safe. When we better understand the level of financial crime in open banking, including fraud and money laundering, we can improve the tools used and information exchanged between open banking participants so that fraud and financial crime risks are mitigated. This will enable the ecosystem to scale and evolve safely."*

Paragraph 4.22 of the JROC report states that: "*The Committee asks the OBIE, with the support from relevant industry stakeholders and in close coordination with other ecosystem participants, to design a financial crime data collection and reporting template for open banking. This should be submitted to the FCA and PSR for review and comment by the end of Q2 2023. This should include metrics, benchmarks, frequency of collection, use cases, reporting method and approach for disseminating the information gathered. It should also consider existing financial crime data collection through FCA reporting and in Faster Payments*."

We have based our proposals for the elements of the Financial Crime Framework on paragraph 4.22, together with other key evaluation issues in the agreed Terms of Reference for this particular workstream, that is:

1. Determining the scope of data collection
2. The metrics to be collected (including fraud types)
3. The metrics to be excluded (aligned to scope)
4. Frequency of collection
5. The mechanism for reporting data
6. Approach to dissemination of the information gathered.

To that end, OBL established an Expert Advisory Group (EAG) with a range of stakeholders to ensure the framework reflects the views of the entire ecosystem. In addition, we held several workshops with ASPSPs and UK Finance to consider potential alignment with existing financial crime collection activities. This document is the outcome of that work.

3. Determining the scope of data collection

3.1 We note that a key JROC objective is to obtain improved data around the level of financial crime in open banking, including both fraud and money laundering. The feedback received from our consultation activity suggests that very different approaches to data collection would be required for each of these distinct categories of financial crime. Collation of fraud data across various payment mechanisms by fraud type is well established and extending this to obtain similar data in relation to the open banking channel seems readily achievable.

3.2 In contrast, data relating to financial crime beyond fraud is less readily available from either ASPSPs or TPPs and is not being reported to any extent at industry level. It is also clear that fraud and financial crime are typically dealt with independently in most ASPSPs. This has limited the progress that we have been able to make to-date on developing a useful industry data framework for broader financial crime within the challenging timeframes set out in the JROC report.

3.3 We note that some firms have, or are providing, some relevant financial crime data to the FCA for monitoring and supervisory purposes. Annual Financial Crime Reports are required to be submitted to the FCA under the FCA's Dispute Resolution: Complaints Sourcebook (DISP), and Suspicious Activity Reports (SARs) may also have been submitted on an ad hoc basis, under the Proceeds of Crime Act 2002 (POCA) or the Terrorism Act 2000. It would be useful to have a better understanding of the nature and extent of the data that JROC currently has at its disposal. Also, to understand where there are gaps that could be usefully filled either by obtaining new data or by extending reporting across a wider pool of firms.

3.4 Our proposed approach is to decouple the development of the fraud component of the financial crime data collection from other types of financial crime. The latter is likely to require a different reporting mechanism across a broader constituency and is therefore likely to be very different from what we are proposing in relation to fraud. It is also important for JROC, OBL and the industry to have a clear and detailed view of the objectives of this requirement and well-defined measures of success. This may take some time. In our view it would be detrimental to delay progress of delivery of an essential component of the framework that will be of value to JROC and the wider ecosystem.

3.5 Careful consideration has been given to which ecosystem participants should provide data. The report references that it might be useful to collect and combine data from ASPSPs and TPPs to provide a holistic view of the nature and extent of the occurrence of fraud across the

open banking ecosystem. However, our evaluation has concluded that an alternative approach where only sending PSPsprovide data would be preferable on the basis that it efficiently provides a comprehensive view and removes complex reconciliation issues. Where multiple parties involved in a fraudulent transaction report that event separately, it is onerous and impractical to reconcile this data without having specific details of every fraudulent transaction, including personally identifiable data to enable accurate matching to take place. This is neither feasible nor desirable.

3.6 Our evaluation has concluded that the sending PSP is usually best placed to identify occurrences of fraud since it has the principal customer interface with the victim and, in most cases, has responsibility for reimbursement of customer losses and currently bears the liability for any loss. These factors result in sending PSPs having well-established practices to collate comprehensive information on the level of overall fraud that is responsive to the objective set out in the JROC report. This is also widely available. These two factors have influenced our proposed approach.

3.7 The primary objective of this activity, as noted in the report, is to improve the availability of empirical data relating to the nature and extent of fraud and other financial crime occurring in open banking payments. This is to address a gap clearly identified in the SWG process. The proposed framework has been developed with this aim in mind.

3.8 Nevertheless, the consultation process has demonstrated that open banking participants agree that a secondary objective should be to develop the framework, so it has the potential to provide timely intelligence on emerging fraud threats. For example, where fraudsters are probing fraud opportunities via attacks on individual firms and the identification of potentially weaker controls that result in higher fraud losses.

3.9 Providing ancillary benefits to contributing firms is likely to incentivise those firms to support this initiative voluntarily and deliver benefits that help offset the time and costs associated with participation. Consequently, we recommend the inclusion of certain components of the framework e.g., data splits by initiating PISP, monthly submission of data to identify issues or patterns and to draw conclusions for a rapid response, and the provision of anonymised benchmarking data to participating firms. In addition we are happy to provide similar benchmarking data to any PISP identified as initiating fraudulent payments.

3.10 We recommend that the framework accommodates this secondary objective to provide actionable intelligence that can potentially be used

by participants to identify necessary improvements in controls, and provides early warning of possible changes in fraud vectors.

3.11 The proposed approach where data is obtained exclusively from sending ASPSPs does have certain limitations in relation to use case, given that those firms will not have any contextual information to enable them to identify a particular use case that the payment supports.

3.12 However, we anticipate engaging with ecosystem participants once we have the data to draw insights that informs understanding of the current OB payment fraud vectors, any incremental risks introduced by OB payments, which OB payments use cases are susceptible and which are low risk as well as particular features of OB payment journeys that fraudsters are exploiting. We envisage including this interpretation of the data in reports provided to JROC.

4. The metrics to be collected (including fraud types)

4.1 The JROC report sets out in paragraph 4.22 that in designing the framework, the starting point should consider both existing financial crime data collection through FCA reporting and in Faster Payments. We undertook comparative analysis of the FCA's REP017 Payment Fraud Reports, the PSR Measure 1 requirements, as well as established UK Finance fraud reporting.

4.2 We set out the comparisons below and the definitions of the terms used are set out in Appendix 3.

4.2.1 Unauthorised fraud

	Rep 017	UK Finance	PSR Measure 1
Key metrics	• Issuance of a payment order by the fraudster • Modification of a payment order by the fraudster	• Fraudster gaining access to an individual's bank account to make an unauthorised transfer of money from the account	• Not included
Data breakdowns	• By geography (domestic, inside European Economic Area (EEA), outside EEA)	• Personal • Non-personal • Mobile • Telephone • Internet	
Suitability for data specification	• Provides the required open banking payment split • No mobile/ internet split	• No open banking channel split • No mobile/ internet split	• No data

4.2.2 Authorised Push Payment Fraud

	Rep 017	UK Finance	PSR Measure 1
Key metrics	• Manipulation of the payer by the fraudster to issue a payment order *Note: DISP states: "The category of 'payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order' covers a broader range of payment types than what is known in the UK as 'authorised push payment fraud'. The latter is restricted to credit transfers authorised by the payer to a fraudster."*	**Across eight defined scam types** **Volumes** • Confirmed case volume • No. of individual victims • No. of vulnerable victims • Total no. of payments • Total cases refunded • Cases refunded to vulnerable victims • Cases partially refunded • Cases partially refunded to vulnerable victims **Values** • Total case value • Value reimbursed • Value recovered • Bank loss • Customer loss	**Across eight defined scam types** • Total cases volume • No. of payments • Cases fully reimbursed • Cases not reimbursed • Cases partially reimbursed • Case value • Value reimbursed • Value not reimbursed • Value recovered

Data breakdowns	• By geography (domestic, inside EEA, outside EEA)	• Personal • Non-personal • Payment type	• Mobile • Telephone • Internet	• Consumer only
Suitability for data specification	• Provides the required open banking payment split • No mobile/ internet split	• No open banking channel split • No mobile/ internet split		• No open banking channel split • Only includes consumer payments so partial • No mobile/ internet split

4.3 The proposed metrics represent a combination of elements of each of these three fraud reporting mechanisms, in addition to existing data, in providing more granular data on fraud within the open banking channel.

4.4 The data splits are intended to give insight into the type of fraud that is commonly being perpetrated, features of open banking payment transactions that fraudsters may be exploiting, and use cases that may be particularly vulnerable. The chosen data points will also support cross-comparison between fraud occurring in the open banking channel with comparable fraud within banks' own channels. It also provides insights as to the extent to which fraud may be migrating between the two.

4.5 As noted in paragraph 4.3 it is not considered necessary or efficient to collect direct channel fraud data as this would duplicate existing UK Finance fraud reporting. This existing data can be used for comparative purposes.

4.6 The previous work that OBL has undertaken on fraud has concluded that all the current examples of fraud perpetrated in open banking map to these existing sub-types. No new classifications are currently required.

4.7 Inevitably aggregate data like this may not provide all the information as to how fraud is occurring and where there are weaknesses in any controls. However, the data should inform where further exploratory work is needed to understand threats and trends.

4.8 It was unanimously agreed that it would be valuable to incorporate and collect a key metric to establish if open banking fraud rates are consistent across PISPs which initiate payments. Most ASPSPs which are prospective data contributors have this data available and agree that it should be incorporated from the start of reporting. However, development will be required by a few prospective data contributors so this data will be incomplete in the first report. Despite this, the sample size will be sufficiently large to draw some initial valuable insights. Consequently, we recommend the inclusion of this metric from the outset, with providers having flexibility to provide the metric when they can.

4.9 However, to make reporting achievable for the broad cohort of ASPSPs which will provide data we are keen not to overcomplicate reporting requirements. For this reason, we have not proposed this metric as another data split. Instead, we propose that reporting of this metric is by fraud type (unauthorised/APP) and, in the case of the latter, by scam type.

4.10 The proposed metrics are as follows:

Metric	Fraud type	Data splits				
Total open banking **fraud volume and value** by month across half year reporting period (new cases identified during reporting month i.e., by case closed date). Reporting both cases and underlying payments.	Unauthorised fraud	Consumer Business	Browser App	Single Immediate Payment (SiP) Variable Recurring Payment (VRP)		PISP initiating the payment
	APP fraud	Consumer Business	Browser App	SiP VRP	Eight defined UK Finance scam types	

4.11 A critical element for making cross-comparisons in fraud both between firms and between channels is the ratio of **fraud: successful payment**. To provide this metric we propose to collect monthly data on the total number of successful PIS initiated that have been accepted and which resulted in a completed payment. To allow for comparison with the comparable fraud data the proposed metrics are as follows:

Metric	Purpose	Split by		
Total open banking payment volume – by month	Provides the denominator for calculation of the ratio of **fraud: successful payment** (volume)	Consumer Business	Browser App	SiP VRP
Total open banking payment value – by month	Provides the denominator for calculation of the ration of **fraud: successful payment** (value)			

4.12 Because the fraud data is reported in the month that it is identified rather than by the transaction date, the ratio of **fraud: successful payments** is unlikely to be absolutely accurate. However, reporting fraud by transaction date is more complex; reporting would be required on a rolling monthly basis with previously reported data being updated retrospectively when fraud is identified. We believe that the proposed

approach to report metrics on a six-monthly basis will eradicate the risk of inaccuracy, without overcomplicating the reporting process.

5. Metrics to be excluded

5.1 In determining what data should be collected we have also evaluated specific metrics that should be excluded. The primary aim is to achieve an appropriate consistency with existing fraud collection initiatives, while minimising the burden on prospective data contributors by not requiring duplication of reporting of data that they provide elsewhere. It is also important to ensure that data is relevant to open banking payments.

5.2 These proposed exclusions, set out in the table below, are supported by most respondents with which we have consulted.

Proposed Data Exclusions	Rationale
Non-FPS fraudulent transactions	Given the predominance of Faster Payments as the payment mechanism to execute open banking payments, and as most fraud takes place across Faster Payments, we consider restricting reporting exclusively to FPS transactions is proportionate. While this does impose some limitations on the ability to see fraud in totality and potentially on detection of any migration of fraud between payment schemes, we do not consider this a material deficiency. We will keep this under review and our approach will evolve if there is evidence that it needs to.
Net fraud losses	**Gross losses** are a primary metric that is indicative of the threat of fraud and how effective controls are. **Net losses** primarily indicate how well the receiving banks' controls are working from a recovery perspective, so from a fraud perspective 'gross losses' are usually more relevant. Although UK Finance does collect net loss data, this is only for some fraud types. We understand from conversations with several banks that inclusion of this metric increases reporting complexity as recovery can take place several months after a case is opened. This requires ongoing revision to reported figures. In addition, the PSR's proposals for reimbursement are not only likely to have an impact on what is reported, but it is also anticipated that future reporting obligations that the PSR is introducing will provide insights into recovery. This will avoid duplication.
Customer reimbursement	Customer reimbursement is a key focus of the metrics that the PSR recently introduced in relation to Measure 1 and is currently a key consideration in the development of Measure 3. The metric is only relevant to APP fraud and its inclusion would be duplication.

Fraud prevented	UK Finance provides a metric on fraud prevented for some fraud types, but this measure is not included within the organisation's APP scam reporting. Some respondents to our consultation expressed the view that it was an important metric, without which it was impossible to evaluate the totality of attempted fraud. However, the majority view was that it was a challenging metric to include as several assumptions need to be taken on both point of payment preventions (easier to quantify) as well as pre-payment preventions (more difficult to quantify) which are in place to prevent fraud. The risk is that the effectiveness of these measures is overstated in a way that overestimates the level of attempted fraud in the open banking channel. Consequently, we do not recommend including this metric although it will be kept under review for future reporting.
Friends and family (multi-step fraud cases)	Some APP fraud cases involve more than one payment. For example, the fraudster may 'socially engineer' a victim to transfer money from their bank account to an account outside the victim's control e.g., a trusted family member or friend prior to transmission to the fraudster. The first leg of these transactions should be excluded to prevent duplicate reporting. This is consistent with the approach taken in relation to PSR measure 1. There are many more types of multi-step fraud, and further guidance is being developed to support implementation of PSR Measure 1. We will monitor the development of guidance in this area and revise reporting definitions accordingly where relevant.

6. Frequency of collection

6.1 There is unanimous support for monthly collection of data. This has the benefit of enabling any preliminary observations from the data to be shared across the ecosystem providing insights and intelligence set out in 1.8. ASPSPs will provide a monthly submission to OBL, which will allow early interrogation of the data and the ability to provide some aggregated feedback on any new trends emerging on a timely basis.

6.2 OBL will provide a six-monthly report to JROC, which will be based on the aggregated monthly data/metrics received from the individual ASPSPs. The six-monthly reporting for the half years ending in June and December is aligned with other financial crime data collection initiatives. These are noted below.

	Rep 017	UK Finance	PSR Measure 1
Frequency	• Half-year • Jan - June • July - Dec	• Half-year • Jan - June • July - Dec	• Half-year • Jan - June • July - Dec
Publication	No – for internal FCA purposes only.	Yes – *Fraud the Facts* published May and Nov	Yes – covering the 14 directed PSPs and the largest recipients of APP scam payments from the directed PSPs.

6.3 It is not proposed to collect fraud data specific to fraud losses arising in ASPSP's own online channels, as this would duplicate existing UK Finance fraud reporting. Alignment to UK Finance's reporting periods will enable us to disaggregate its data, and efficiently compare fraud between the open banking and own channel for data providers. A different approach will be necessary to accommodate any data provider not among those firms providing data to UK Finance.

6.4 We recommend the monthly collection of data, which is the preferred approach of all the potential data providers, but propose to report data over a six-month period to align with other existing industry data collection initiatives. This will allow us to accurately compare these various datasets.

7. The mechanism for reporting data

7.1 Most identified prospective data contributors currently submit fraud data to UK Finance via Pay.UK's CAMIS system. Some potential data contributors have expressed a preference for using this existing process to submit new data. This option is contingent on agreement with both Pay.UK and UK Finance and is under consideration. This option may lend itself to a solution in which UK Finance assumes a role to collating this new data alongside its existing fraud data collection activities. Most, although not all, respondents to the consultation agreed that it was sensible for OBL to collect and analyse data in the initial phases of this exercise, recognising that it is likely that anomalies, potential errors, and misinterpretations are likely to require investigation and resolution. This may require further refinement of requirements before they are finalised.

7.2 Some CMA9 respondents suggested that the submission process should be aligned to the existing process used for OBL management information (MI) submissions.

7.3 We recommend that OBL undertakes the initial data collection and analysis exercise, in line with the JROC recommendation. After this, decisions regarding the long-term responsibility for this exercise can be discussed with the industry and JROC. It is likely that OBL will have to support more than one reporting mechanism in the initial phase of this project. These options will be discussed with potential data contributors once the framework, including the required data elements, have been approved by JROC.

8. The analysis and dissemination of the findings

8.1 The JROC report states that: "OBL should conduct a first data collection and reporting exercise in Q3 2023 and share the outputs with the FCA and the PSR."

8.2 All data shared with ecosystem will be fully anonymised so that no individual ASPSP or TPP can be identified. Non-anonymised data will be shared with the FCA and PSR for monitoring purposes.

8.3 Assuming a sufficient sample size, this will be made available to allow ASPSPs to benchmark themselves against industry-wide averages.

8.4 OBL will initially share aggregated data with data contributors as part of the quality assurance process. This will highlight any anomalies or potential errors/misinterpretations, which can be investigated and addressed prior to sharing findings more broadly.

8.5 An example of the potential output available is set out in Appendix 2.

9. Participation and next steps

9.1 As part of the consultation process, we received feedback from 10 ASPSPs accounting for over 85% of FPS payments, which indicated they supported this initiative and would be willing and able to contribute data. Several firms have the proposed data readily available. Others indicate that some development work will be required to extract specific data elements.

9.2 Understandably, it is difficult for firms to fully scope their ability to provide data until all elements of the framework are agreed, and the baseline requirements are known. However, from the feedback received, most firms can commence data provision in Q4 2023 which provides a good prospect of being able to produce a credible report by the end of 2023/ Jan 2024. Encouragingly, most firms indicate that they will be able to provide historical data for the 18-month period to end June 2023.

9.3 Once the framework is approved by JROC, we intend to discuss residual issues e.g., final reporting definitions, reporting mechanisms, data sharing agreements (which may replicate agreements in place for other data collection initiatives) and timelines for data provision bilaterally and collectively with the relevant firms. This will enable us to finalise first indications of when data will be available.

9.4 OBL (or the Future Entity) will continue to convene additional workshops with firms to ensure collective understanding of what is requested and provide useful FAQs to ensure data is produced in a standardised way. From our previous experience in collecting MI, we assume it will take time, effort, and extensive discussion with firms to ensure that the data initially provided is accurate, comparable, and high quality. Expected delivery timelines are set out in Appendix 1.

OPEN BANKING

Appendix1: Expected delivery timelines

Responsibility	Description	Jul	Aug	Sep	Oct	Nov	Dec	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	H2- 24
OBL / JROC	Finalise framework and data metrics													
OBL/ participants	Agree data collection mechanism / templates													
OBL/ participants	Agree data sharing legal agreement													
participants	Set up resource to provide data submission													
OBL	Set up resource to analyse data													
Participants	1st data submission													
OBL	Data analysis													
OBL/ participants	Final first report circulated													
OBL / JROC /participants	Review Framework / data requirements													
OBL/ participants	Ongoing data collection													

Appendix 2: Reporting Outputs

Half-year values PISP-initiated fraudulent payments			Volume Total Cases	Volume No. of Payments	Value (£) Gross Loss (£)
Browser	Single Immediate Payment	Consumer			
		Business			
	Variable Recurring Payment	Consumer			
		Business			
Mobile/Application	Single Immediate Payment	Consumer			
		Business			
	Variable Recurring Payment	Consumer			
		Business			

Half-year values PISP-initiated fraudulent payments		Volume Consumer		Volume Business		Value (£) Consumer	Value (£) Business
		Total Cases	No. of Payments	Total Cases	No. of Payments	Gross Loss	Gross Loss
Browser	Single Immediate Payment						
	Variable Recurring Payment						
Mobile/Application	Single Immediate Payment						
	Variable Recurring Payment						

OPEN BANKING

UNAUTHORISED FRAUD

Half-year values PISP-initiated fraudulent payments	Volume Consumer		Volume Business		Value (£) Consumer	Value (£) Business
	Total cases	No. of payments	Total cases	No. of payments	Gross loss	Gross loss
Browser						
App						
Total						
Single Immediate Payments (SIPs)						
Variable Recurring Payments (VRPs)						
Total						
Consumer						
Business						
Total						
Share of open banking fraud (volume)						
Share of open banking fraud (value)						

APP FRAUD

Half-year values PISP initiated fraudulent payments	Volume Consumer		Volume Business		Value (£) Consumer	Value (£) Business
APP scams - by scam type	Total cases	No. of payments	Total cases	No. of payments	Gross loss	Gross loss
Invoice and mandate						
CEO fraud						
Impersonation: police/bank staff						
Impersonation: Other						
Purchase						
Investment						
Romance						
Advance fee						
Unknown scam type						
Total						
Single Immediate Payments						
Variable Recurring Payments						
Total						
Browser						
App						
Total						
Share of open banking fraud (volume)						
Share of open banking fraud (value)						

Appendix 3: Definitions

Term	Definition
APP fraud	A payment order initiated by the PSU subsequent to fraud or dishonesty where the PSU makes a payment to an account they believe to be legitimate or a correctly identified payee for what they believe are legitimate purposes but is a scam.
App	Mobile banking app ASPSP authentication channel
Browser	Web-based ASPSP authentication channel
Case closed date	Date on which firms have investigated the fraudulent activity and cases are closed.
Consumer	PISP initiated FPS payment from personal current account
Business	PISP initiated FPS payment from business / corporate current account
Gross open banking fraud value	Total value open banking executed payments identified as fraudulent at the case closed date prior to any loss recovery.
Open banking payment value	Total value of successful FPS single domestic payment / VRP orders that have been accepted which resulted in a completed payment.
Open banking payment volume	Total number of successful FPS single domestic payment / VRP payment orders that have been accepted which resulted in a completed payment.
Reporting period	Half year Jan – June or July – Dec
SIP	PISP initiated FPS single domestic payments authorised by PSUs
Total open banking fraud volume	Total number of open banking-executed payments identified as fraudulent at the case closed date.
Unauthorised fraud	The PSU has not given consent for the payment and/or authentication of a payment is by a third-party other than the PSU.
UK Finance scam types	As per Authorised Push Payment – Monthly Reporting Definitions & Reporting Metrics: Form completion guidelines v2.0
VRP	PISP initiated FPS payments made using a long-held consent (“VRP Consent”) and which are subject to strong customer authentication (SCA) by the ASPSP as part of the VRP consent set-up.

OPEN BANKING

www.openbanking.org.uk