OPEN BANKING

Dispute Management System (DMS)

Code of Good Practice

For Account Servicing Payment Service Providers (ASPSPs) and Third Party Providers (TPPs)

Date: October 2019
Version: DMS 2.0 v0.11
Classification: PUBLIC

Contents

1 Introduction

Open banking is revolutionising the financial services industry. One effect of this revolution is an increasing number of transactions – and that could mean more customer enquiries, complaints and disputes. Open Banking Limited's (OBL) Dispute Management System (DMS) provides a communication tool for a member which aims to facilitate the speedy resolution of customer related issues in order to deliver better customer experiences. As a platform, DMS is designed specifically for open banking and connects players in the ecosystem, allowing them to communicate securely and solve customers' problems quickly, efficiently, and fairly.

This code of practice, created collaboratively through workshops, review, consultation and user acceptance testing, sets out the expectations and recommended good practice for members.

The contents of this Code do not constitute legal advice. Although intended to be consistent with regulations and laws it is the sole responsibility of DMS members to ensure that they meet applicable regulatory obligations when engaging in DMS.

2 Principles

DMS members should always:

- **Put the customer first**
    - For Case Recipients and Case Respondents the customer will be mutual, so they should work together in addressing and supporting a customer case, and aim to provide a good customer outcome. It is important to take ownership of a case from start to finish, so the customer isn't sent from pillar to post. Working collaboratively, for a successful resolution, should minimise escalation.
- **Collaborate**
    - Members should be open, fair and support one another to maintain a self-regulating community. They should make every effort to be responsive to acknowledging, attending and collaborating on cases raised by mutual customers.
- **Keep customer data safe and secure**
    - Members should handle all customer data in line with the General Data Protection Regulation (GDPR) as detailed in the Data Protection Rules – *refer to link in page 8 of this document.*
    - This suggests that only appropriate information and evidence necessary to support a case is shared, and appropriate records for every case are maintained. Customer information within each case in the DMS platform is automatically deleted after 6 months of case closure.

3 DMS Good Practice

This section is a guide to good practice between members using the DMS platform.

- **User Access Management**

For the effective management of the DMS platform, all members are recommended to segregate roles with users, so that there is no single point of failure. This will also ensure that the roles are aligned to the risk and operational processes of the members.

- Super users and team leaders are responsible for setting up and maintaining the appropriate number of user licences for their organisation. Members should be aware of the number of licences they have been assigned before adding new users. More user licences can be acquired but there may be a cost associated.
- We recommend that super users and team leaders regularly review their organisation's users and amend or remove access rights as required.

- **Inputting case details**

Capturing detailed and accurate information within the case file will assist all members to better understand the enquiry, complaint or dispute being raised by the customer. This should facilitate effective case management and result in faster outcomes to the customer.

- **Case Type:** the DMS platform classifies complaints in line with the Financial Conduct Authority (FCA) *"DISP 1.3 – Complaints handling rules*".
- **Value of Case:** This is an optional field for the Case Recipient to fill in if they feel it necessary.
- **Transaction ID:** It's recommended that Case Recipients use the unique transaction ID, or API reference ID, to avoid using personal identifiable information.
- **Additional case information:** DMS members should only enter information that is relevant and necessary to enable effective case resolution either by the DMS members, the Financial Ombudsman Service, alternative dispute resolution or the courts. In submitting information, the DMS member must also remain compliant with GDPR requirement

Note: As Data Controllers the onus is on DMS members to ensure all employees are suitably trained in ensuring that the Controller is able to meet their GDPR requirements. Members should ensure only relevant and necessary data is uploaded onto the DMS platform in accordance with the Data Privacy Principles.

- ## Identifying case reason codes

Using the correct reason codes will help direct the enquiry, complaint or dispute to the right department to resolve the customer issue. Analysis of reason codes may assist in driving desired changes in operational behaviour that benefit the customer.

These codes are short descriptions aimed at classifying cases by cause or effect to the customer.

- **Primary reason code:** Case Recipients should choose the most appropriate classification for the case raised by the customer.
- **Secondary reason code(s):** Case Recipients should choose the most appropriate secondary (lower level) classification for the case raised by the customer.
- Both the primary and secondary reason codes should be reviewed and updated throughout the investigation and findings of the case. As a minimum, review the reason codes before logging an outcome and closing the case.

- ## Inputting Claimant details

This is the customer's information, visible to the Case Recipient(s) only and not to any Case Respondent(s).

- **Have you conducted customer identity and verification (ID&V)?** Case Recipients are expected to follow internal procedures on ID&V prior to or when populating this field.

- ## Uploading case evidence

- Case Recipient and Case Respondent(s) will share and upload all relevant documentation and evidence necessary to enable members to communicate with each other in order to reach an outcome for the customer.
- Members uploading documentation and evidence on the DMS platform should make sure that the files are relevant, appropriate, readable (not corrupted), and free from viruses.
- We recommend that members put in place internal procedures for peer reviews between its Case Handlers and conduct regular internal quality checks.

- ## Sharing case evidence

- Case Recipient(s) and Case Respondent(s) can use the DMS platform to share evidence to the appropriate members quickly and easily
- Case Recipient(s) and Case Respondent(s) can send messages to each other requesting additional information or confirming the provision of information as necessary.

- **Creating a message**
  - The messaging functionality within the DMS platform allows Case Recipient(s) and Case Respondent(s) to discuss matters relating to the case. When creating a message, it is good practice to be as clear, concise, and specific as possible to enable efficient and relevant responses.
- **Responding to a message**
  - Case Recipient(s) and Case Respondent(s) should make every effort to respond within a reasonable timeframe so the customer's case can be resolved quickly and efficiently.
- **Adding notes**
  - Use the internal notes function when you want messages to be visible only to users within your member organisation.
- **Logging an outcome**
  - Before logging an outcome, we recommend the Case Recipient(s) review the case in its entirety to ensure all information captured previously is still current, accurate and complete.
  - Outcomes should capture the following:
    - Definition of the problem
    - Root cause of the problem, if applicable and identified
    - Outcome for the customer
  - Subsequent actions to settle the case such as restitution of funds and repayments and issuance of the final response letter as outlined in the FCA DISP rules, will be conducted using existing internal member processes, and ideally noted in the case within the DMS platform for completeness and future reference.
- **Exporting cases**
  - We recommend Case Recipient(s) export and keep a copy of every case that has been closed, as all customer information contained within a case will be automatically deleted 6 months after it has been closed. Retaining a copy of the case may help if the case is escalated to an ADR or to the FOS.

4 Appendix 1 – Definition of terms

Term	Definition
Alternative Dispute Resolution (ADR)	A provider of a dispute resolution service which is voluntary and acts as a means for disagreeing members to come to an agreement short of litigation.
ASPSPs	Account Servicing Payment Service Provider (ASPSP) provides and maintains a payment account for a payer as defined by the Payment Services Regulations (PSRs). In the context of the Open Banking Ecosystem, ASPSPs are entities that publish Read/Write APIs to permit, with customer consent, payments initiated by third party providers and/or make their customers' account transaction data available to third party providers via their API end points.
AISP	Provides account information services as an online service to provide consolidated information on one or more payment accounts held by a payment service user with one or more payment service provider(s).
Case	An enquiry, complaint or dispute lodged in the context of the DMS platform.
Case Recipient	In the context of DMS, an ASPSP or TPP that receives a verbal or written expression of an in-scope complaint, dispute or enquiry.
Case Respondent	In the context of DMS, an ASPSP or TPP that is party to the in-scope complaint, dispute or enquiry that is neither the claimant nor the case recipient. The Case Recipient may ask the Case Respondent to provide information related to the case to assist in the resolution of the complaint, dispute or enquiry
CBPII	A payment services provider that issues card-based payment instruments that can be used to initiate a payment transaction from a payment account held with another payment service provider.
Claimant	In the context of DMS, a customer, ASPSP or TPP that makes a verbal or written expression of an in-scope complaint, dispute or enquiry.
Complaint	In the context of DMS, any oral or written expression of dissatisfaction, whether relating to a customer submitted by an ASPSP or TPP about the provision of, or failure to provide, payment initiation, account information or confirmation of funds service (a) alleges that the complainant has suffered (or may suffer) financial loss, distress or inconvenience; and

Term	Definition
	(b) Relates to an activity of the respondent, or of any other respondent with whom that respondent in relation to open banking products or services.
Data Protection Law	Means the Data Protection Act (1998), EU Data Protection Directive 95/46/EC and the EU Privacy & Electronic Communications Directive 2002/58/EC, any amendments and replacement legislation including the EU General Data Protection Regulation (EU) 2016/679, European Commission decisions, binding EU and national guidance and all national implementing legislation.
Data Protection Rules	https://www.openbanking.org.uk/wp-content/uploads/DMS-Data-Protection-Rules.pdf
Dispute	Any conflict in opinion between an ASPSP(s) and/or TPP(s) in relation to a case.
Enquiry	Any request for information or clarity from a customer, ASPSP or TPP about the provision of, or failure to provide a payment initiation or account information service.
Member	An ASPSP or TPP that has signed up to participate on the DMS platform and adhere to the Code of Good Practice.
Open Banking Ecosystem	The Open Banking ecosystem refers to all the elements that facilitate the operation of Open Banking. This includes the API Standards, the governance, systems, processes, security and procedures used to support members.
Dispute Management System (DMS)	DMS is a communication and information exchange process governed by good practice standards. It is intended to be used by ASPSPs and TPPs and support with the handling of payment initiation, account information service-related complaints, or confirmation of funds disputes or enquiries.
Payment Initiation Services Provider (PISP) Party	Provides an online service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider. An ASPSP or TPP acting as claimant, case recipient or case respondent involved in the case in question.
Payment Service User (PSU)	A natural or legal person making use of a payment service as a payee, payer or both.
Third Party Provider	Regulated entities that use APIs or other alternative means to access customer's online payment accounts held at ASPSPs, in order to provide account information

Term	Definition
(TPP)	services (AISPs) and/or to initiate payments (PISPs) or request confirmation of funds (CBPII).