CMA Market Investigation into Retail Banking: HSBC response to the CMA's Provisional Decision on Remedies (PDR)

Response to CMA's foundational remedy proposal regarding implementation of an open API banking standard

This document supplements and completes our separate response to the rest of the CMA's remedy proposals.

Executive summary

1. HSBC welcomes the CMA's recognition that an open API banking standard has the potential to transform competition in retail banking markets. We agree with each of the steps the CMA is proposing, and the sequence in which the CMA proposes those steps. However, we do not consider it possible to meet time frames the CMA has provisionally set out in the PDR. We set out some indicative times in paragraph 18 below.

2. HSBC is going through a period of unprecedented change to its IT infrastructure, with a number of large scale projects (both regulatory and commercial) already running in parallel. The most significant challenge for HSBC in the UK is the implementation of the Ring Fenced Bank: this is unique in is nature, and far reaching in its remit, as it requires the careful separation and emulation of systems to support both the retail and non-retail banks. The Ring Fenced Bank must be implemented alongside other material regulatory changes such as PSD2, cheque imaging and the recently confirmed EU General Data Protection Regulation.

3. While we agree with the CMA's proposed package of work in respect of APIs, it will be a challenge to schedule any significant change or testing to our core banking and payments systems whilst they are being adapted for the Ring Fenced Bank, without generating unacceptable levels of execution risk (which could crystallise in a range of forms, including payments system failures). On the basis of the level of detail set out in the PDR (and in the short time since its publication), we have not been able to assess accurately how much change will be required in respect of APIs. We are therefore keen to get a firmer grasp of the specific scope of work required, through engagement with other stakeholders on the technical standards for the APIs and security protocols. This will enable us to assess whether it is possible to integrate changes with existing projects, in a way which does not adversely affect those projects. We believe change can be most effectively managed by ensuring that the APIs and security protocols are closely aligned with the PSD2 Regulatory Technical Standards (RTS).

4. Once we have more detail, we will be better placed to make further submissions on achievable timescales and levels of execution risk; our comments in this submission on timescales should be viewed in this light. Given the uncertainties inherent in projects of this nature (not least the need to align with PSD2), we propose that the CMA should set target dates but provide the Implementation Trustee with discretion to change the delivery timetable as it sees fit.

Governance arrangements

5. The delivery timetable proposed by the Open Banking Working Group OBWG (at the start of 2016) was premised on the prompt formation of an appropriate governance body, which has not yet taken place. An Implementation Entity with an Implementation Trustee acting as chair therefore needs to be constituted and set up as soon as possible, in order to drive through the process of agreeing and finalising standards (which the OBWG has laid the groundwork for), according to realistic indicative time frames laid down by the CMA. We consider that Payments UK is best placed to coordinate initial discussions between the banks on how the entity should be constituted, and that a lawyer with experience in data protection law would be an appropriate choice as Implementation Trustee.

6. The Implementation Entity will need to be well resourced with independent technical experts. It may need to retain a role after the implementation phase (for example in relation to maintaining the standards, and managing any the recovery of costs).

Recommended approach on implementation timeframe

7. We share the CMA's desire to implement open APIs as quickly as possible. We have recent experience of other large scale IT projects requiring coordination between multiple stakeholders (for example cheque imaging). That experience indicates that there are real challenges in setting fixed time frames and deadlines at the outset of such a project, as unanticipated challenges inevitably arise. It is not possible to commit to specific time frames in respect of each aspect until the scope of the requirements is finalised: a particular challenge will be around the agreement of common security protocols for APIs in respect of Closed Data. Implementation will also require co-ordination with other significant change projects which are already underway.

8. There will therefore be trade-offs between pace and risks that the Implementation Trustee will need to be allowed discretion to resolve. Three examples of the types of risk are:

   a. First, if open APIs are launched before security issues (such as white lists of approved third parties) have been robustly addressed, any ensuing security breaches could destroy consumer confidence in the use of applications that use APIs, setting back the whole process of market adoption.

   b. Secondly, the implementation of the CMA's remedy proposals in respect of personal account data ("Closed Data") ahead of PSD2 could generate unnecessary risks and costly complexities if the standards adopted for the implementation of the CMA remedies conflict with the Regulatory Technical Standards (RTS) decided upon by the European Banking Agency (EBA) for PSD2 (see section (ii) below).

   c. Thirdly, in light of the usual competition issues that arise when setting standards across markets, it will be important for the Implementation Trustee to manage the process transparently and in a way that delivers open API standards which smaller banks and third parties can utilise in a fair, reasonable and non-discriminatory manner. The need to involve smaller banks and third parties sufficiently within the governance arrangements and take into account any legitimate concerns could justify the Implementation Trustee exercising its discretion to extend the timeframe for implementation

9. We therefore propose that the CMA's order should require banks to use best endeavours (for example, by devoting sufficient resources), to achieve realistic indicative deadlines, which the CMA sets. The CMA should provide the Implementation Trustee with discretion to determine whether individual banks are fulfilling that obligation, and a discretion to amend the CMA's indicative timetable where it considers it appropriate to do so.

10. In particular, a delivery time frame which dovetails more closely with PSD2 time frames (in particular the adoption of RTS) would be likely to generate less risk. The Implementation Trustee should be empowered to weigh up – at a later date - the extent to which it is feasible to push implementation of the CMA's remedies ahead of PSD2 implementation, once the interlocking nature of the issues becomes clearer.[1]

[1] Subject as well to the outcome of the referendum on membership of the EU: a leave vote could generate further complexities around implementation.

Implementation timeframe for different data types

11. There is a major distinction between "Closed Data" (confidential personal and business account data) and "Open Data" (non-personally identifiable / non-confidential bank data).

12. **Work can commence on building Open Data APIs as soon as the common technical standards and definitions have been finalised**. A prerequisite of agreeing standards is that the Implementation Entity (with Implementation Trustee acting as chair) is constituted. It should be feasible to implement APIs in respect of Open Data within 9-12 months of the finalisation of common technical standards (or, in the case of service quality data, as soon as it is available). This indicates that a Q1 2017 deadline is not realistic, and points to a deadline in Q4 2017. We propose that the deadline is set by the Implementation Trustee once common technical standards have been agreed: the implementation timescales will depend on the specific requirements set by the Implementation Trustee.

13. For Closed Data APIs to be implemented, a common and single solution to a range of interlocking security-related issues needs to be delivered, which will take more time. The main security-related issues are (i) authorisation and authentication standards; (ii) standardised permissions frameworks (i.e. the need to ensure and manage explicit customer consents); (iii) whitelists (i.e. lists of third parties with the necessary security clearances); and (iv) customer redress mechanisms. The OBWG has provided a significant amount of guidance in relation to each of these aspects, which are also prominent considerations for PSD2. As the CMA notes, the deadline for transposition of PSD2 into UK law is January 2018. However, actual implementation of PSD2 is likely to take place during the course of 2018, as regulatory technical standards (RTS) are finalised.

14. The CMA proposes that APIs for read-only PCA Midata data sets should be made available by the end of Q1 2017, with adoption of full read and write APIs for PCAs and BCAs by the start of 2018.

15. **As regards Midata data sets**, the Q1 2017 deadline was proposed by the OBWG at the start of 2016 on the premise that a governance framework would be put in place (which has not yet happened – and is why it is imperative that an Implementation Entity with an independent Implementation Trustee is constituted as soon as possible). It may be possible to implement APIs for the Midata data sets within 12 months of the finalisation of common technical standards, provided that prompt agreement can also be reached in respect of key aspects of the security protocols. We consider that (in line with the thinking of the OBWG) the Midata data set APIs will require a whitelist process,[2] and will also require a clear redress framework, to address the risk of data security breaches (for example identity theft) in respect of read only customer data. These two issues will also be addressed through the PSD2 implementation process; it will be important to ensure that there is consistency between the Midata implementation and the broader PSD2 implementation.

16. **As regards full read and write functionality for PCAs and BCAs**, it may be possible to adopt open API standards with full read and write functionality by January 2018. However, significant risks will be generated if Closed (read and write) Data is made available via Open APIs without the adoption of common permissions management frameworks, robust whitelists of third parties, and redress mechanisms. These issues require a substantial additional amount of work to resolve and will interlock with, and may be dependent on, the PSD2 RTS process, which may continue through to the start of 2019. It therefore makes sense for the Implementation Trustee to have the discretion to align the implementation of open API standards with PSD2, if it considers that implementation

[2] The CMA indicates at 3.42 of the PDR that it has considered HSBC's proposal (in a paper prepared by Alix Partners and submitted to the CMA in January 2016) for a closed API as an interim measure. HSBC's proposal in that paper relates to the need for a prescribed list of third parties who can gain access to the Midata data sets – i.e. a Whitelist. The CMA considers that data protection risks have been satisfactorily considered by the OBWG. However the OBWG considers that a whitelist process is necessary for the development of APIs which involve the transfer of customer level data (see page 50 of the OBWG report).

prior to PSD2 generates significant risks or inefficiencies (for example, of misalignment between the UK and the EU on security standards such as permissions management frameworks).

17. In summary, and with the caveats expressed in this submission, we set out below our current high level view on a potentially feasible implementation timeframe, based on the premise that the Implementation Entity and Trustee are established and operational very quickly after the CMA's Final Report and that they are then able to determine common technical standards for APIs by the end of 2016.

    a. **Open Data** (non-personally identifiable / non-confidential bank data): we expect to be able to deliver this within nine months of the agreement of common technical standards. This could potentially be **Q4 2017**.

    b. **Closed Data (Midata data sets):** we expect to be able to deliver this within 12 months of the agreement of common technical standards. This could potentially be late **Q4 2017**.

    c. **Closed Data (read and write access to PCA and BCA account data):** This could potentially be delivered by the end of **Q1 2018**.

18. In respect of both categories of Closed Data, these dates will only be achievable if it is possible to agree promptly on common security protocols which are consistent with those proposed as part of the RTS programme for PSD2. We do not currently know when the EBA will finalise the relevant aspects of the RTS.

19. We explain our views and the underlying issues in more detail in the remainder of this paper.

The Order the CMA is minded to impose on the biggest banks

20. The CMA is minded to set the following requirements and deadlines for the biggest banks:

    a. Adopt and maintain common API standards through which they will share data with other providers and [any] third parties.

    b. Propose to the CMA for the CMA's approval an Implementation Entity (in terms of governance, arrangements, funding and budget) which will be responsible for implementing and maintaining open banking standards to a CMA-approved timetable. Also propose an Implementation Trustee to act as chair of the Implementation Entity. Agree to be bound by the decisions of the Implementation Entity and Trustee.

    c. Make available the following by an open API by end Q117:

        i. Prices, charges, terms and conditions, eligibility criteria for all PCA and SME products within scope of the Investigation. The "reference data" (as described by OBWG) – branch/ATM locations, opening hours etc.

        ii. Midata data sets (i.e. redacted PCA data sets).

    d. Make full PCA and BCA data sets available, with full read and write functionality, no later than the transposition deadlines for PSD2.

    e. Make data on service quality indicators available via APIs as soon as available in line with the remedy on service quality.

HSBC's response to the CMA's proposals on Open APIs

(i) Governance arrangements

21. The initial OBWG delivery timetable was premised on the prompt formation of an appropriate governance body to drive forward the further development and implementation of common standards and definitions in respect of both the technical aspects of APIs (needed for all data), and the security aspects (needed for any customer data). This has not happened yet, which is inevitably lengthening the timeframe for implementation. As such we welcome the CMA's proposal to set up an Implementation Entity, to be chaired by an Implementation Trustee. In our experience, it will be challenging to make any significant progress in the development of the appropriate common API definitions and standards without the presence of an effective governance body. The formation and activation of an Implementation Entity should therefore be a priority.

22. In the light of the expedited timeframe which the CMA has indicated it wishes to pursue, we are engaging with other banks, via Payments UK,[3] over how the Implementation Entity should be set up and constituted, prior to the publication of the CMA's final report. We agree with the CMA that the Implementation Entity should provide a forum for discussion of the implementation options, and also have the means to impose a solution where consensus does not emerge, to ensure timely delivery. Payments UK is best placed to coordinate initial discussions between the banks on how the entity should be constituted. Payments UK has considerable experience in a range of similar initiatives, including CASS and the Agency Bank code of conduct.

23. We consider that initial funding for the Implementation Entity, up to the point at which APIs are operational, should come from the larger banks (as named by the CMA), in proportions based on market shares. As regards ongoing costs of the Implementation Entity (for example updating the standard and regulating who can access providers' data), we propose that a cost recovery model is

[3] Payments UK contains representatives from smaller banks as well as larger ones.

developed. Under this model, providers should be entitled to charge heavy users of their API interfaces a small fee which enables them to recover the costs of supplying access to their data via APIs. This is a common model in respect of APIs, and is what has been envisaged by the OBWG (see page 32 of its report, published in February 2016).

24. A decision will need to be made as to whether the Implementation Entity should continue to play a role after the initial implementation phase, for example in relation to the maintenance of a white list of approved third parties (see further below), the recovery of costs or charges, or the updating of relevant standards and definitions. Where an ongoing role is envisaged, HSBC considers that the Implementation Entity should be set up as a company, or potentially converted to a company at a later date.

25. We consider that the Implementation Trustee should be a lawyer with a specialisation in privacy and data protection. The Implementation Trustee will require a significant amount of support from technical architects, who are independent of the banks. Independent technical architects will need to have (or be supported by) good project management capability, as well as experience of aligning different stakeholders with potentially divergent interests and views. The Government Digital Services office (GDS) may be well placed to assist in this regard, as it has a strong track record in coordinating multiple government departments behind single sets of data standards.

26. We anticipate that each large bank will have a technical architect seconded to the Implementation Entity on a full time basis (with smaller banks and the FinTech sector also represented). The independent technical architects should chair discussions between the banks' representatives on technical definitions and standards, and have the authority (subject to the ultimate adjudication of the Independent Trustee) to impose solutions once each stakeholder has been properly consulted.

27. One challenge for the Implementation Trustee and all independent support staff will be to ensure that the API standard and definition setting process complies with competition law, but does so in a way that does not cause undue delay to the standard setting process. It is important that all stakeholders have a fair opportunity to participate in the development of the standard, and that the adopted standard is unrestricted, transparent and accessible on FRAND (fair, reasonable and non-discriminatory) terms. However, the Implementation Trustee will need to decide when sufficient consultation with different stakeholders has taken place, and ultimately decide on the standard.

28. The CMA envisages that smaller banks should have the opportunity to participate in the Implementation Entity on the same terms as larger banks, and that FinTech companies should be represented. The CMA may need to clarify whether this means that smaller banks would be expected to commit to the same costs and obligations as the larger banks: if this is the case, smaller banks are unlikely to wish to participate. We think it may work better for smaller banks and FinTech companies to be grouped together, perhaps with representatives and voting rights within the Implementation Entity structure and/or with a requirement for the Implementation Entity/Trustee to consult them throughout the process.

(ii) The time frame for implementation and coordination with PSD2

29. It is always difficult accurately to predict timescales for the development of IT infrastructure and the coordination of stakeholders in standard setting processes (we have recent experience from cheque imaging. The Gov.uk programme of work is another example). It is not possible to commit to specific time frames in respect of each aspect until the scope of the requirements is finalised: a particular challenge will be around the agreement of common security protocols for APIs in respect

of Closed Data. Implementation will also require co-ordination with other significant change projects which are already underway.

30. Given the fundamental importance of getting certain aspects of this remedy right first time (in particular as regards security), we do not think it would be appropriate for the CMA to seek to force the pace artificially by setting hard deadlines. This could lead to poor outcomes and the loss of consumer confidence in the use of APIs in banking, if, for example, security standards are not effective. It may also be difficult for the CMA to identify who is at fault for any particular delays.

31. Nonetheless, we appreciate that the CMA is keen – as is HSBC – to expedite the development of APIs. We propose that the CMA should set target completion dates for the various stages, but then leave the Implementation Trustee with a wide discretion to amend the delivery timetable. The CMA's order could require banks to use best endeavours to achieve the deadlines which the CMA sets (for example, by devoting sufficient resources). The CMA could then leave it to the Implementation Trustee to advise the CMA as to whether individual banks have behaved reasonably or not, at any stage in the implementation process.

32. The implementation of APIs for Closed Data (including Midata) will require careful coordination with the development of Regulatory Technical Standards (RTS) by the European Banking Authority as part of the PSD2 implementation programme. There are a number of actual or potential differences between the proposed CMA programme and the implementation of PSD2:

    a. First, the Midata data sets which form the central element of the CMA's remedy proposals are much wider than the data sets which form the basis of PSD2. Midata involves comprehensive 12 month transaction history data sets. PSD2 requires only that basic account balances and certain recent transaction data are shared with Account Information Service Providers ("AISPs") and Payment Initiation Service Providers ("PISPs").

    b. Secondly, the CMA anticipates that Price Comparison Websites (PCWs) will be the principal users of Midata data sets. In our view there is considerable doubt as to whether a PCW (which may apply a year's worth of account data on a one-off comparison basis) will qualify as an AISP. However, it is also possible that other third parties who may wish to access the Midata data sets may qualify as AISPs.

    c. Thirdly, it is not yet clear what standards will be adopted for authorisation and authentication, and other security protocols, under PSD2.

33. HSBC will be required to provide data to third parties under the auspices of PSD2, and also under the auspices of the CMA remedy proposals. There may be circumstances where the CMA's measures and the provisions of PSD2 overlap, and other occasions where they may not. It will be imperative for the Implementation Entity and Implementation Trustee to ensure that there is no regulatory clash between the implementation of the CMA remedies, and the RTS. The two implementation programmes are likely to cover the same issues: we cover four principal areas below (authentication and authorisation, permissions management and customer consents, whitelists, and customer redress). It is vital that the Implementation Entity adopts solutions which dovetail with those pursued by the EBA through the RTS.

34. We expect the RTS implementation programme to continue for 12 months beyond the January 2018 date for transposition of PSD2 into national law. A delivery time frame which corresponds more closely with PSD2 time frames (in particular the adoption of Regulatory Technical Standards (RTS) at the EU level) would be likely to generate less implementation risk. The degree to which this is the case will become clearer over time. The Implementation Trustee should therefore be empowered to weigh up – at a later date - the extent to which it is feasible to push implementation of the CMA's remedies ahead of PSD2 implementation, once the interlocking nature of the issues becomes clearer

(iii) The nature of the standard that should be developed

35. We endorse the OBWG's recommendations in respect of the appropriate API standards (see pages 22 to 30 of the OBWG report). The next step will be to agree on the appropriate definitions for the APIs (i.e. how the APIs will appear to third parties who need to interface with them). This will likely require a significant coordination effort from independent technical experts.

(iv) Delivery of an open API for publicly available data, reference data, and service standards (Open Data)

36. The development of an API for Open Data does not generate issues around security. It should be feasible to implement APIs in respect of Open Data within 9 months of the finalisation of common technical standards (or, in the case of service quality data, as soon as it is available). This indicates that a Q1 2017 deadline is not realistic, and points to a deadline in Q3 2017. We propose that the deadline is set by the Implementation Trustee once common technical standards have been agreed.

(v) Security in respect of all customer data APIs (Closed Data): the interaction between authorisation and authentication procedures, permissions management, whitelisting criteria, and customer redress mechanisms

37. The CMA notes that the OBWG has already given consideration to data protection risks. The view of the OBWG is that if personal data is to be included within the Open API (i.e. looking to introduce "Closed Data") data protection considerations will need to be revisited. Consent of the data subject addresses a number of general concerns as to the lawfulness of disclosure and processing. However there are also broader security and liability considerations, which HSBC, & OBWG members were concerned with during the drafting of the OBWG recommendations. We address these broader issues below.

38. The process of using APIs in respect of Closed Data involves three actors: the user, the bank and the third party. Wherever APIs are used as a mechanism for the sharing of users' data, all three actors have an interest in four inter-related security requirements. These requirements are also under consideration by the EBA through its work on the RTS for PSD2, and will require harmonisation, as far as possible. We summarise these below and provide more detail in an annex.

39. **First: Authorisation and authentication**: data must be transferred in a manner which is both secure, and minimises friction in the user experience. This requires robust authentication and authorisation procedures, as well as secure data transfer protocols.

40. **Second: User Consent (fair processing notices) and permissions management**: users should be provided with clear, transparent information about how their data will be used and processed by the bank and the third party (this requires clarity of data controller / processor roles of the bank and third party). Users must be able to control the scope of the data which is transferred between their bank and a third party. This requires there to be a clear permissions management framework in place.

41. The Implementation Entity may need to give consideration to the extent to which it is practicable and/or desirable to require banks to harmonize permission categories, and the need for banks to adopt a single set of criteria in respect of each permission category. For example: whether access to Midata data sets should be provided on a 15 minute one-off time limited basis, or whether third parties should be given permission to access the data for a longer period of time.

42. **Third: the use of whitelists**: Only third parties who achieve a minimum level of security standard should be provided with access to customer data via an API. This requires an independent body to maintain a form of whitelist of approved third parties. We consider that, in line with the OBWG Report, there should be a "whitelisting process" for any third party which seeks access to customer data via the use of APIs (see pages 50 to 53 of the OBWG report). A requirement to share customer

level data with any third party which presents a valid customer authorisation would generate significant and unacceptable levels of fraud and data security risk.

43. The Implementation Entity will need to consider how best to reach an industry consensus on the types of security standard that third parties (principally, AISPs, PISPs and PCWs) will need to meet in respect of different categories of data, and whether such standards are consistent with the provisions of PSD2, and with the other use cases which fall outside the scope of the CMA remedies. In our view, such discussions will need balanced representation from banks and from third parties, who are likely to have - to some extent - divergent interests.

44. **Fourth: customer redress mechanisms**: There needs to be clarity around who is liable in the event of data security breaches. Customer redress forms part of the implementation programme for PSD2.

45. The Implementation Entity will need to take a view on which types of interaction envisaged by the CMA may fall within the scope of PSD2 and/or whether it will be necessary to specify that the PSD2 rules will apply in all cases in any event.

46. **These four elements are inter-related**: for example, where there are no security standards requirements placed on third parties, and banks have liability for security breaches, they are likely to apply very strict permission regimes. A balance is required between these four elements. This is best illustrated through two scenarios:

    a. At one end of the spectrum: any third party can access a user's account data, even on a read only basis (and the bank considers itself potentially liable for any data security breach and misuse of data). In this scenario, the bank is likely to insist on the use of authorisation windows on a request by request basis, and is likely to limit the permission it grants to a short time period of a few minutes. This will obviously have a negative impact on the user experience, and will undermine the commercial viability of the third party's offering to the user.

    b. At the other end of the spectrum: the whitelist of approved third parties is very restrictive, and only approved providers with the highest levels of security are approved; the third parties take on liability for data security breaches and any misuse / unlawful usage of data. In this scenario, banks would be more comfortable enabling third parties to seek authorisation on behalf of customers, and may allow for more relaxed permission regimes (for example allowing third parties to reuse authorisation tokens, rather than request a new one each time). This would generate a much more positive user experience, but may limit innovation as only third parties with the most robust security standards, and insurance for customer redress, would be enabled to provide users with access to their bank data.

47. Further, the rules and standards to be adopted in respect of each of the above four elements will need to be agreed in parallel between all banks, including with input from smaller banks and FinTech companies, in respect of both read only Midata functionality and read and write functionality. While the development of common rules and standards will take longer, it will ensure that the user experience is as frictionless as possible.

48. The CMA does not address issues around permissions management or the process of whitelisting in the PDR. It also does not give sufficient consideration to the customer redress issue in respect of the transfer of Midata data sets. We explain each of these four elements, and how they interact with PSD2, in more detail in the annex. We set out below our assessment of the feasibility of delivering the different APIs to the CMA's current proposed timetables.

(vi) The release of redacted PCA "Midata" data sets

49. The OBWG report envisaged that it would be possible to implement APIs for Midata by the end of Q1 2017. We consider the application of the four elements discussed above in respect of the release of the existing Midata sets.

50. **Authorisation and authentication**: it will be necessary for the Implementation Entity to establish detailed standards and rules which all banks will be required to adopt. Authorisation and authentication could be conducted through a calling out platform, whereby the third party directs the user to the bank's log in page, and the user logs in and provides a one-off time limited permission for the third party to access their Midata data set on a read only basis.

51. **User Consent (fair processing notices) and permissions management**: the use of a one-off permission, provided at the point in time at which the user interacts with the third party, may mean that it is not necessary for banks to develop a detailed and commonly agreed permissions framework or infrastructure.

52. **Whitelists**: the CMA indicates at 3.42 of the PDR that it has considered HSBC's proposal (in a paper prepared by Alix Partners and submitted to the CMA in January 2016) for a closed API as an interim measure. HSBC's proposal in that paper relates to the need for a prescribed list of third parties who can gain access to the Midata data sets – i.e. a Whitelist. The CMA considers that data protection risks have been satisfactorily considered by the OBWG. However, as explained above, the OBWG considers that a whitelist process is necessary for the development of APIs which involve the transfer of customer level data (see page 50 of the OBWG report).

53. While the risk of fraud will be lower in respect of read only Midata sets (compared to permissions to process payments for example), significant risks will remain – for example in relation to identity theft. A third party could obtain personal customer data through the use of appropriate authorisation and authentication procedures, but then use that data for fraudulent purposes. As such, we would not be comfortable providing customer data to third parties, without some minimum security checks being conducted on the third party by a body responsible for whitelisting (either the FCA through an authorisation process in line with PSD2, or another independent body). This is an important point: if there is a significant number of frauds reported in the initial stages of the implementation of API standards, this could have very adverse effects on consumer perceptions of the benefits of APIs.

54. **Customer redress**: while it is not clear whether banks would be liable for misuse of customers' Midata data sets, banks may consider themselves obliged to offer customers redress, in the event that they are victims of fraud. This militates further towards a need for a whitelist process, even in respect of read only Midata data sets.

55. Taking account of the above, in order to implement Midata data set APIs, it will be necessary to:

    a. Set up the implementation entity and agree on governance processes.

    b. Agree on API standards and definitions. Banks will then need to implement these.

    c. Agree on the details of authorisation and authentication.

    d. Agree on the principles for the development and maintenance of security standards for FCA authorisation, and/or a separate whitelist. The absence of any whitelist would in our view generate unacceptable levels of risk, which could undermine the whole API programme.

    e. Agree on an appropriate redress mechanism.

    f. Banks will then need to implement.

56. It is difficult to determine the length of time it will take to implement each of these steps, but it is clear that this is not achievable by end of Q1 2017. Much will depend on the interaction between stakeholders, the quality of the independent technical experts, and the approach adopted to the whitelist (it may be more expedient to identify named PCWs in the first instance, before then setting standards and criteria for any third party). Much of these considerations will overlap with issues being considered as part of the implementation of PSD2. We consider that once steps (a) and (b) above have been completed, it may take a period of 12 months for steps (c) to (f) to be completed.

(vii) Making full PCA and BCA data sets available, with full read and write functionality, no later than the transposition deadlines for PSD2

57. The development of APIs for full read and write access presents a more significant range of challenges. All of the stages envisaged above in respect of the Midata data sets would need to be completed. It will also be necessary to come up with a comprehensive permissions management framework, a comprehensive whitelisting process, and a clearer and more detailed customer redress mechanism. These elements will involve very considerable additional amounts of work which will need to be aligned with equivalent PSD2 work streams. We provide additional detail in respect of each type of work in the annex below. Further, as indicated above, these elements will each interact with the other (for example, a more robust whitelist process will affect the nature of the permissions regime). The agreement of common rules and standards in respect of these elements will require excellent oversight from the Implementation Trustee and the independent technical experts.

58. Significant risks will be generated if Closed (read and write) Data is made available via Open APIs without the adoption of common permissions management frameworks, robust whitelists of third parties, and redress mechanisms. These issues will interlock with, and may be dependent on, the PSD2 RTS process, which may continue through to the start of 2019. It therefore makes sense for the Implementation Trustee to have the discretion to align the implementation of open API standards with PSD2, if it considers that implementation prior to PSD2 generates significant risks (for example, of misalignment between the UK and the EU on security standards such as permissions management frameworks).

(viii) Other Remedy Design Consideration

59. As regards the types of SME in scope, if banks do apply a limit to SMEs in respect of the provision of transaction data, the upper limit should not be set below £6.5m. This aligns with CASS, and covers 99 per cent of SMEs.

Annex – the four relevant security issues for all Closed Data

Authorisation and authentication procedures

60. The CMA notes that the OBWG has considered and proposed standards for authentication and authorisation. We summarise the OBWG's recommendations (see pages 38 and 39 of the OBWG report):

    a. Informed consent: the consumer should clearly understand the authorisation they are being asked to provide: who to, what for (i.e. what the authorisation will permit the third party to do), and how long the authorisation will last.

    b. As regards authentication of the consumer request, the OBWG recommends OAuth 2.0 and OpenID Connect, although further work is required to specify the precise model. Banks should be required to notify customers directly (through an Out Of Band (OOB) process) when they receive an authentication submission.

    c. As regards Authorisation, once a consumer has authenticated with their bank, tokens should be provided by the bank to the third party, which the third party can present to the bank in order to collect data. Tokens can be scoped both in terms of type of access and time frame.

    d. In terms of security, data in transit should be encrypted using TLS v1.2 as a minimum, and a security accreditation model based on ISO27001 should be employed.

61. HSBC endorses these recommendations, which should form a solid basis from which the Implementation Entity can develop a common set of more detailed specifications, which all banks will need to adhere to.

User Consent (fair processing notices) and permissions management

62. It is vital that customers are asked to provide their explicit and informed consent to the use of their data (i.e. having been provided with clear, transparent and plain English understandable explanation as to how their data will be used).

63. Permissions are the customer's informed consent (following disclosure by the third party of its privacy notice setting out the proposed uses to be made of the customer data), communicated to their bank, for the bank to provide a specified third party with a certain type of access to the customer's data, for a specified period of time. The OBWG recommends that permissions should be assigned risk levels, which reflect the potential impact of malicious misuse of the permission. This relates both to the type of information (for example sensitive personal data or banking transaction data) and the nature of function (for example read only versus setting up new account beneficiaries).

64. Permissions should only be granted where the third party has sought access to the customer's data via the appropriate authorisation and authentication procedures. Permission will also require the third party to have provided the customer with informed outline (privacy notice) of what they will be using the customer data for. Permissions may also be sensitive to the channel by which data is transferred (for example, consideration may need to be given to the security of the end user's electronic device).

65. Banks will wish to develop a range of different permission categories to take account of the above considerations. The Implementation Entity may need to give consideration to the extent to which it is practicable and/or desirable to require banks to harmonize permission categories, and the need for banks to adopt a single set of criteria in respect of each permission category. For example: whether access to Midata data sets should be provided on a 15 minute one-off time limited basis, or whether third parties should be given permission to access the data for a longer period of time.

66. Further, it will be necessary for banks to build user interfaces for permissions management. The OBWG envisages that banks will need to allow customers to review: (i) pertinent information about third parties they have provided permissions to; (ii) permissions being requested by third parties; and (iii) the duration and validity for which the permissions will be granted. Banks will need to provide users with the ability to revoke permissions. The development of these user interfaces may take a significant amount of time.

67. Banks may be reluctant to go too far in the development of permissions management interfaces before the Implementation Entity has set down what the permissions management framework will be.

68. Some concerns raised by the OBWG as to permissions for joint account holders (i.e. joint signatories) and accounts with different access permissions (i.e. corporate accounts), will require further consideration.

The use of whitelists

69. The CMA appears to suggest that banks' API data should be capable of being used or accessed by anyone. While it may be possible to make publicly available data and bank reference data open to anybody to access, we consider that third parties who wish to access customer data should be vetted to assess whether they meet a minimum required set of security standards and reviewed to ensure a good practice of usage of customer data (i.e. not repeated privacy offenders).

70. We consider that, in line with the OBWG Report, there should be a "whitelisting process" for any third party which seeks access to customer data via the use of APIs (see pages 50 to 53 of the OBWG report). A requirement to share customer level data with any third party which presents a valid customer authorisation would generate significant and unacceptable levels of fraud, data privacy and data security risk. We agree with the OBWG that different levels of vetting will be necessary in respect of different risk categories. Minimal or no vetting will be required for access to publicly available information via an API. Vigorous vetting should be expected by third parties who wish to be able to transfer funds between a consumer's accounts.

71. Under the provisions of PSD2, in order to obtain access to a Payment Service Provider's (PSP's) individual account level data – i.e. to be white listed - an Account Information Service Provider (AISP) or a Payment Initiation Service Providers (PISP) will need to be registered with and authorised by the FCA, and meet the requirements set down by PSD2 (see Article 5 in particular).

72. There are two issues which the CMA and/or the Implementation entity need to consider in relation to the PSD2 registration and authorisation process:

    a. First, the implementation of PSD2 post-dates the implementation of the Midata data set APIs. It will be necessary to have some form of whitelisting process in place as a pre-requisite to the implementation of these APIs, which will require the Implementation Entity to define that process before it has been defined for the purposes of PSD2.

    b. Secondly, it appears unlikely that Price Comparison Websites will qualify as AISPs under PSD2. This may mean that PCWs need a whitelist which is separate from the FCA register.

73. We endorse the recommendations of the OBWG around the appropriate whitelisting process that should be adopted, through the use of digital certificates. We consider that the FCA should adopt this process when authorising AISPs and PISPs.

74. Entitlement tokens provided to third parties as part of the authorisation process are the equivalent of credit card details. The Payment Card Industry Data Security Standard (PCI DSS) sets down a rigorous vetting process for any company or organisation which seeks permission to process card

payments. In our view, there is likely to be significant read-across between the PCI DSS certification process, and the types of vetting procedures necessary for the handling of users' personal banking data.

75. The Implementation Entity will need to consider how best to reach an industry consensus on the types of security standard that third parties (principally, AISPs, PISPs and PCWs) will need to meet in respect of different categories of data, and whether such standards are consistent with the minimum harmonising provisions of PSD2, and with the other use cases which fall outside the scope of the CMA remedies. In our view, such discussions will need balanced representation from banks and from third parties, who are likely to have – to some extent – divergent interests.

76. If PCWs and other entities wishing to access customer account information do not qualify as AISPs or PISPs, it may be necessary to consider how to manage a separate whitelist on an ongoing basis, which is not more onerous than the FCA authorisation requirements.

77. Any entity responsible for the ongoing maintenance of a whitelist which sits outside of the FCA authorisation framework for AISPs and PISPs would need to be independent of the Implementation Entity.

Customer redress mechanisms

78. At present there is a lack of clarity around the way in which the customer redress mechanisms envisaged by PSD2 will be implemented. PSD2 anticipates that customers will be able to seek immediate redress from their bank, with the bank then having the right to pursue the third party for compensation, where the latter is liable (for example, for an unauthorised transaction). However, it is not clear how the process of deciding when third parties should provide compensation will be set up, or whether the treatment by third parties of compensation requests may have an impact on their whitelist status. For example, it may be reasonable for banks to expect that third parties who do not honour valid compensation claims are struck off the whitelist.

79. The principle of immediate compensation only applies to interactions between banks and third parties which take place within the scope of PSD2. The Implementation Entity will need to take a view on which types of interaction envisaged by the CMA will all unequivocally fall within the scope of PSD2 and/or whether it will be necessary to specify that PSD2 rules will apply in all cases in any event.

80. As indicated above, the nature of the customer redress mechanism, combined with the process adopted in respect of whitelists, will have a significant impact on the approach of the banks to permissions, authorisation and authentication.