The Information Commissioner's response to the Payments Strategy Forum's consultation on being responsive to user needs

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations 2004 ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

2. The Commissioner welcomes the opportunity to respond to the Payments Strategy Forum's consultation on future of the UK's payments system. She takes this opportunity to offer her assistance to the Payments Strategy Forum on the application of the DPA to any future model for the UK's payments system should it be required.

3. The Commissioner's response is restricted to those questions which fall within her regulatory remit. Therefore she has responded to the questions where data protection or privacy concerns have been raised, these being questions 3, 7 and 8. This response does not provide full answers to all the sub questions, but provide an overview of the data protection issues that have been raised by the related proposals. For this reason we have decided not to use the provided template.

4. The consultation puts forward a model for the future of the UK's payment system that makes use of enhanced levels of data both to assist the payer and the payee. It also proposes data sharing to help combat financial crime. We can see a benefit in both of these aims, however we are keen to stress any processing of personal data must be done in compliance with the DPA and would like to take this opportunity to highlight areas where further thought may be required from the Payments Strategy Forum.

5. Before moving on to specifically answer the relevant questions, it is worth providing a brief overview of the DPA, highlighting the relevant parts that will then be referred to in the specific responses below. The protections contained within the DPA are only engaged when personal data are being processed. Personal data is defined In Section 1 or the act, which states:

> ""personal data" means data which relate to a living individual who can be identified—
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;"

6. The DPA does not apply to data that do not relate to an identifiable living individual.

7. It is important to note that any processing of personal data must be compliant with the 8 data protection principles contained within the DPA. These can be found in Schedule 1 of the DPA and are included as an annex to this response.

8. To satisfy the first data protection principle the data controller must have a legal basis for carrying out the processing activity. These "conditions for processing" can be found in Schedule 2 of the DPA. If the activity includes the processing of sensitive personal data then it must also satisfy a Schedule 3 condition. The categories of sensitive personal data can be found in Section 2 of the DPA and are:

> "(a) the racial or ethnic origin of the data subject,
>
> (b) his political opinions,
>
> (c) his religious beliefs or other beliefs of a similar nature,
>
> (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
>
> (e) his physical or mental health or condition,
>
> (f) his sexual life,
>
> (g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

9. We strongly encourage the drafting of a privacy impact assessment (PIA) for any proposal that involves the processing of personal data. The ICO has produced guidance on how to complete a PIA, and this can be found at https://ico.org.uk/media/1595/pia-code-of-practice.pdf. We recommend the use of PIAs before embarking on a project that could have an impact on individuals' privacy as they can assist in mapping out data flows and enable organisations to identify any privacy risks. Once those privacy risks have been identified it is then possible to mitigate those risks in the design of the project.

Question 3: Enhanced Data Capabilities

10. We recognise the benefits on incorporating richer data capabilities into the UK payment system. We are pleased to see that the consultation document has highlighted that such enhanced data capabilities also bring with them a number of data protection risks that must be fully considered in designing such a system.

11. The Horizon for Payments document provides more detail on the proposed introduction of richer data.[1] This highlights that there is the potential for any data to be attached to a payment in the form of a URL that links to data of any size and in any format. To allow for this, this enhanced data could be provided through an "out-of-band" transmission, thus not interfering with the transmission of the critical data. The document goes on to suggest that an example of such enhanced data could be a utility company sending the "entire itemised invoice" with the payment to make it easier for the customer to understand the payment and the utility company to implement one click payments.[2]

12. With this in mind, we would like to draw attention to the need to treat this enhanced data in the same way as the critical data required for the payment. The Horizon document suggests that such data could be provided over a different network with the enhanced data being linked to the payment through the use of a URL. Care must be taken to ensure that if this approach were to be followed access to the enhanced data be afforded suitable security to ensure that only those who need to access it

[1] The Horizon for Payments, Payments Strategy Forum, https://www.paymentsforum.uk/sites/default/files/documents/HSWG%20Report.pdf
[2] The Horizon for Payments, at 51

are able to access the data. There will likely be interest in this data from a number of other sources, not least from the payment processor and the customer's bank. Allowing access to this data would need to be carefully considered, with those seeking access having a legitimate reason and legal basis to do so. As highlighted in the consultation document the information that maybe contained within the enhanced data could allow other parties, such as the customer's bank, to profile their customers in a way that they currently cannot. Some of these organisations will also offer other services to their customers such as insurance, loans and mortgages. There is therefore potential for the enhanced data to be used to make decisions on a customer's access to credit or their insurance risk. By way of example, if a user were to go to their own bank to apply for a mortgage, if that bank were to have access to the enhanced data they would be able to use this to piece together a much more granular profile of the applicant's lifestyle.

13. Of course it is possible that data subjects may want to make use of the enhanced data in exactly the way described above, or to provide a more complete picture of their finances to enable them to better plan for the future. It is important that data protection is not seen as a barrier to such services when the customer has full knowledge of how their data are to be used, there is a legitimate basis for the processing and suitable safeguards are put in place to protect the data. This feeds in well to the work done by the Open Banking Working Group and to the implementation of the second Payment Services Directive. The aims of both are to open up banking data to enable consumers to make better use of their data and introduce new financial products and services to the market. Returning to the hypothetical example given above about bank access to enhanced data for mortgage purposes, a customer may wish to make use of this data to compare and apply for mortgages across a number of banks and there is no reason why they should not be able to do so if appropriate safeguards are put in place.

14. It is also worth noting that it is possible that the enhanced data could be considered sensitive personal data. For instance, if itemised invoices are included in a payment, this could easily constitute data relating to the health of the data subject if the customer is buying medical supplies. As mentioned above, the processing of such sensitive personal data requires an additional condition for processing. These conditions can be found in Schedule 3 of the DPA.

Questions 7 and 8: Data Sharing and Central Data Repository

15. Questions 7 and 8 will be taken together as they both relate to the sharing and pooling of transaction data for the purpose of preventing and detecting financial crime. The main pillar of these proposals is a central data repository with centralised data analytics capabilities. The consultation document recognises that there are a number of legal issues that would need to be addressed, including the Data Protection Act. We welcome the fact that the Payments Strategy Forum has considered the privacy impact that a central data repository could have and would again like to take this opportunity to highlight some areas where serious thought is required.

16. As noted above, data on the commission or alleged commission of an offense are considered sensitive personal data, and as such are afforded extra protection by the DPA. To process such data a Schedule 3 condition will be required in addition to a Schedule 2 condition. The consultation brings up the prospect of sharing data on suspected fraud. This raises some significant issues that will need to be addressed. There is greater potential for causing detriment to individuals if this type of data is being shared and so care needs to be taken when considering whether the sharing of such data are necessary and appropriate. For instance, if the central data repository's data analytics capability suggests to a PSP that a payment may be related to financial crime there is potential for that individual to be unable to make payments for necessary purchases.

17. The July 2016 report from the Financial Crime, Data & Security Working Group[3] highlights two potential options for the creation of the central data repository. The first option being without the central data analytics capability and with the data being uploaded in a way that the document claims is anonymous. The report noted that the data would be sent into the central data repository with any identifying data replaced with a unique key. It is important to consider whether it will be possible to match the data held in the repository to a list of individuals and the unique identifiers assigned to them. If that is possible the data will not be considered anonymous and any processing will be subject to the DPA. Even if that were not possible, there is still the potential for the data held in the central repository to be linked to an identifiable individual. The more data that is held and the more granular that data, the more likely for identification to take place. The ICO has produced an Anonymisation

[3] Financial Crime, Data & Security Working Group report, Update for July 2016, https://www.paymentsforum.uk/sites/default/files/documents/PSF%20Fin%20Crime%20WG%20-%20All%20Solutions%20Description%20-%20July%202016.pdf

Code of Practice which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/. This page also provides links to the UK Anonymisation Network, which provides further information on anonymising data.

18. The second and favoured option provided in the working group paper is for a centralised data repository and a centralised analytics capability. The document makes it clear that in this option the data is not going to be held anonymously. This means that the DPA will be engaged.

19. Regardless of which option is taken, one of the issues that the working group report brings up is where this centralised database should be held. The favoured option is to be held by a public authority. This is considered the favoured option for governance and competition reasons. If this is chosen as the way forward, it is important for the Payments Strategy Forum to fully consider how to restrict any public authority's access to the database, to ensure that it is only used for purposes specified by the data controller. Many public authorities hold numerous data sets on UK citizens and it is of the utmost importance to ensure that the payments dataset that will be held in the central data repository does not get mixed in with the other datasets held.

20. The first data protection principle requires that data subjects are provided with fair processing information about any data processing activities. The working group report notes that it will be up to the individual payment service providers to provide the necessary information to the data subject. With regard to sharing data of suspected financial crime, thought needs to be given as to what will be considered as an instance of suspected financial crime. There would need to be a clear set of criteria as to what would be considered a suspected financial crime, with those criteria being communicated to individuals whose data are shared with the central data repository. In effect this would mean anyone using a PSP. It also needs to be clear what the effect of a payment being flagged as potentially fraudulent or linked with financial crime will be. Again, this will need to be communicated to individuals that are using a PSP.

21. The processing also needs to satisfy the "data quality" principles, those being principles 3, 4 and 5 of the DPA. These state that personal data must be adequate, relevant and not excessive (Principle 3), accurate and up to date (Principle 4), and only retained for as long as necessary (Principle 5). When deciding what data are to be stored in the central repository due thought must be given to these principles. If certain data points are not necessary for the financial crime prevention purposes then they should not be included in the data set. For instance, is the enhanced data necessary for the stated purposes, or will the basic payment data be

sufficient? Retention periods must be considered carefully as well. Once data is no longer needed for the stated purpose they must be deleted or made anonymous so as to no longer be considered personal data.

22. If the operator of the central data repository is to be considered a data controller for those data thought must be given to how individuals will be able to avail themselves of their rights contained in the DPA. The most notable of these being the right of subject access under Section 7 of the act, which states that a data subject has the right:

> "(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
>
> (b) if that is the case, to be given by the data controller a description of—
>
> (i) the personal data of which that individual is the data subject,
>
> (ii) the purposes for which they are being or are to be processed, and
>
> (iii) the recipients or classes of recipients to whom they are or may be disclosed,
>
> (c) to have communicated to him in an intelligible form—
>
> (i) the information constituting any personal data of which that individual is the data subject, and
>
> (ii) any information available to the data controller as to the source of those data, and
>
> (d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking."

23. Given the level of data that will be contained within the central data repository thought must be given to how a subject access request can be responded to. Tools should be built into the system to enable the retrieval of the relevant data in the event of such a request. The final part of section 7 could potentially be of interest if the data analytics capability

becomes fully automated as suggested in the working group report. If the centralised analytics capability is making decisions about individuals then thought must be given to algorithmic accountability. That is, if a decision is being made by an automated "black box" there should be a way for a human to analyse the decision that has been made to ascertain how the algorithm has come to that decision.[4]

24. It is also important to note that European data protection law is being updated, with the General Data Protection Regulation due to come into force in May 2018. It is therefore important that the Payments Strategy Forum take any change in the law into account when moving forward with the project.

25. Once again, we would like to thank the Payments Strategy Forum for the opportunity to respond to this consultation and are keen to provide any advice and assistance in the future. Rebuilding the UK's payment system from the ground up is an important and ambitious project, and we are keen to ensure that data protection concerns are considered from the outset.

Annex 1

The data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
   (a) at least one of the conditions in Schedule 2 is met, and.
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for

[4] See generally Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard UP, 2015)

longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.