The Information Commissioner's response to the Competition & Markets Authority's 'Retail banking market investigation: notice of possible remedies'

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR). He 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 he can, and taking appropriate action where the law is broken.

2. The Information Commissioner welcomes the opportunity to respond to the Competition & Market Authority's (CMA) notice of possible remedies arising from its retail banking market investigation. The Information Commissioner recognises there may be benefits to consumers, businesses and other organisations brought about by the measures proposed in the notice. There are, however, a number of important concerns to be considered from a data protection and privacy perspective.

3. The CMA may wish to note that in February 2015 the Information Commissioner responded to HM Treasury's call for evidence on data sharing and open data in banking. [1] The Information Commissioner takes this opportunity to repeat some of the submissions made in that response as they are relevant to some of the proposed remedies contained in the notice.

4. The CMA may also wish to consider that the relevant laws the Information Commissioner is responsible for enforcing are derived from European legislation, namely Directive 95/45/EC ('the Data Protection Directive') and Directive 2002/58/EC (as amended) ('the ePrivacy Directive'). It should be noted that the respect for private and family life, and the protection of personal data are fundamental

[1] https://ico.org.uk/about-the-ico/consultations/hm-treasury-consultation-on-data-sharing-and-open-data-in-banking/

rights accorded to European citizens under articles 7 and 8 of the Charter of Fundamental Rights of the European Union. We have observed that recent decisions on data protection matters - both from the CJEU and domestic courts - have placed increasing reliance on the protection of these rights. On 25 January 2012 the European Commission proposed a comprehensive reform of data protection rules in the EU, the so-called General Data Protection Regulation (GDPR). It should therefore be noted that UK data protection law is expected to change once the GDPR comes into force. The texts of the draft Regulation are currently being negotiated, and we expect negotiations to be near to conclusion by the end of 2015.

5. Organisations processing personal data will need to comply with the eight data protection principles set out below.

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 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.

Remedy 1 – Prompt customers to review their PCA or BCA provider when they may have a higher propensity to consider a change.

6. We note this remedy would require PCA or BCA providers to prompt customers to consider making changes to their banking arrangements and explain to them how to do so. This may be as a result of a 'trigger point' event, or potentially as a result of account usage analysis. We understand that the remedy is intended to provide customers with information about the ease and potential rewards of switching.

7. It is likely that such prompts will constitute 'direct marketing' for the purposes of the DPA and PECR. In our direct marketing guidance we explain that the definition of direct marketing includes **any** advertising or marketing material, not just commercial marketing[2]. All promotional material falls within this definition,

[2] https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf p.10

including material promoting the aims of not-for-profit organisations. Any marketing must comply with the requirements of DPA and PECR, and the CMA should ensure that any requirements placed upon organisations do not conflict with existing legal obligations.

8. An individual is entitled to give notice under s 11 of the DPA requiring an organisation not to process their personal data for the purposes of direct marketing. Any such notice should be respected and complied with.

9. In respect of electronic marketing (telephone, fax, SMS, email) there are additional restrictions to consider if the prompts ('direct marketing') are to be delivered in this way. Electronic direct marketing is a source of great public concern, and it is of the utmost importance that organisations comply fully with the rules as set out in the law and our published guidance. Organisations that do not comply can expect to receive heavy fines from the Information Commissioner up to £500,000 and the ICO is actively enforcing in this area. It should be further noted the threshold at which the Information Commissioner may issue a fine has recently been lowered following removal of the "substantial damage or substantial distress" requirement in relation to the breaches of PECR. This change in the law reflects the significant concerns associated with non-compliant direct marketing.

10. We note the considerations around 'circumvention risk' set out at paragraph 41 of the notice, and that it has been suggested this could be addressed by allowing the regulator, or third parties, to access lists of relevant customers to allow them to communicate with the customer. Sharing customer information in this manner raises a number of significant data protection and privacy issues and we would advise the CMA contact us to discuss further should it be concluded this is an avenue to be pursued. We note there may be wider policy issues to consider, and that the CMA's own recent study, *The commercial use of consumer data*, concluded that "many consumers are concerned about sharing their data and how it will be used. Consumers have a range of concerns, including potential data loss, data misuse and unexpected data sharing. While they often share data despite these concerns, trust may be fragile and at risk if negative perceptions about new developments in data use take hold.". [3]

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, p 97

11. Marketing that is not directed to anybody in particular, for example generic newspaper and television advertising, is not covered by the DPA or PECR.

Remedy 3 – Facilitate price comparisons between providers by making customer-specific transaction data more easily available and usable, including by PCWs.

12. Broadly speaking, the Information Commissioner is supportive of initiatives that empower individuals to use the information organisations hold about them for their own benefit. We were pleased to have been consulted by HM Treasury and the banking industry during the development of the existing Midata scheme allowing consumers to download their financial transaction history for price comparison purposes. We are, however, cautious about the opening up of access to financial transaction data without there being sufficient safeguards in place to adequately protect consumers from the risk of fraud, unauthorised access or theft, or to ensure that the data is used fairly and in a way that is not going to erode consumer trust and confidence.

13. In our response to HM Treasury's call for evidence on data sharing and open banking we stated the following:

> Obtaining information about an individual's spending habits presents a powerful way in which to build a very detailed profile about that individual and the way in which they choose to lead their life. This position is exacerbated following the growth in contactless payments for small transactions which might previously have been undertaken, in cash, with relative anonymity. Profiling in this way is potentially very privacy intrusive and careful consideration needs to be given to ensure the risks arising are identified and appropriately managed.
>
> Whilst in most cases financial transaction data is not likely to be sensitive personal data according to the strict legal definition[4], we suggest that information about an individual's financial affairs and standing is a matter that many people would consider to be confidential. In 2014 the ICO issued civil monetary penalties against two organisations which failed to take appropriate technical and organisational security measures to protect payment card information in what amounted to a serious breach of the Data Protection Act.
>
> It should be appreciated that whilst access to financial transaction data is intended to improve competitiveness in the personal current account market and facilitate development of

[4] Data Protection Act 1998, Section 2

fintech products, both of which are entirely laudable objectives, the danger is that this is a case of "opening Pandora's box" with consequences for individuals' privacy extending beyond the envisaged applications. It is not something to be entered into without sufficient thought being given to what the implications are for individuals' privacy.

Individuals can currently download a copy of their personal current account statements through online banking services, or receive a paper copy on demand. It is expected that the public will soon be able to download a copy of their personal current account (PCA) 'midata file' containing a partially redacted version of their transaction history in a standardised CSV format which may, in turn, be uploaded to an online price comparison service.

In the existing cases it should be more readily apparent to the individual what data they are sharing because they can physically inspect it. Conversely, where an API is used to access and share data there is less visibility and this creates a challenge in terms of ensuring any consent given by the individual for the processing of their data is specific, informed and freely given. The issue is exacerbated when the access provided is ongoing, i.e. does not require future action from the individual, and is more than simply a "one time" permission. Individuals need sufficient control of their data and an informed understanding of what organisations are doing with it.

The Open API standard should also address the fact that financial products and transactions can relate to more than one individual. Current accounts and mortgages can be held in multiple names and transaction histories can include details of payments made direct to family and friends.

It is foreseeable that the introduction of an open API standard will lead to the development of new products and services which seek to utilise the data which becomes accessible. It will be essential that organisations, and regulators, understand the risks arising when processing individuals' personal data in such volumes and with such variety. It is important to understand that analysis of financial transaction data to make conclusions about individuals, and then to use this data to make decisions has the potential to be unfair (or unethical), and appropriate care should be exercised.

In relation to the financial transaction Midata download previously described, the data is partially redacted to ensure that the price comparison service only receives the information that is needed to make a comparison of PCA options. This element is

integral to the scheme and helps safeguard against processing of excessive and unnecessary data. Consideration also needs to be given as to how granular any permission might be and whether any privacy enhancing features can be built in.

It will be essential that organisations, supported by government, are able to build consumer trust and ensure that individuals can make informed decisions about whether to share their data, and on what terms. Taking steps to build consumer trust and confidence should be an integral part in development of the standard.

The ICO advocates the adoption of 'privacy by design' principles and privacy impact assessments (PIAs) to ensure privacy risks are identified from the outset, and that measures to address these are built in to any projects and not 'bolted on' at a later stage.

14. Given the CMA's interest from recent work looking at the commercial use of consumer data, the conclusions reached regarding the potential fragility of consumer trust, and the impact lack of confidence may have on consumers' willingness to share data, consideration should be given to helping ensure the development of an API allows for individuals to have sufficient control and understanding over the use of their financial transaction data by third parties, and ensure the risk of any adverse consequences are minimised.

Remedy 9 – Require banks to retain and provide ex-customers, on demand, with details of their BCA and PCA transactions over the five years prior to their account closure.

15. The fifth data protection principle requires personal data is not kept longer than necessary. Retaining data creates a security risk. In our published guidance on the DPA and principle 5 we give the example of a bank, and state that even after an account has been closed, the bank may need to continue holding some of this information for legal or operational reasons.[5] If a retention period is to be mandated then it would be wise to explore how this fits with the retention periods currently used by banks and to make an assessment of risk.

16. In terms of charging for the information, an individual already has a legal right to obtain a copy of the information an organisation holds about them. The maximum that can be charged for this information is currently prescribed at £10, although there is no obligation for an

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

organisation to charge. We encourage organisations to provide individuals with the means to easily access their information without needing to exercise their legal right of subject access request. This approach is beneficial to organisations and their customers.

17. It should also be noted that we expect the GDPR will strengthen the existing provisions around individuals' access to data held about them, requiring it to be provided in a portable format at a minimal or no cost.

November 2015