Via email: pdpc_consultation@pdpc.gov.sg

April 1, 2013

Personal Data Protection Commission
Singapore

Re: **Consultation Paper:**
Proposed Advisory Guidelines on Key Concepts and Selected Topics
Proposed Regulations on Data Protection in Singapore

Dear Sirs:

1. MasterCard Worldwide ("**MasterCard**")[1] welcomes the opportunity to provide its comments to the Personal Data Protection Commission (the "**Commission**") on the Advisory Guidelines on Key Concepts in the PDPA ("**Key Concepts Advisory Guidelines**"), Advisory Guidelines on Selected Topics ("**Selected Topics Advisory Guidelines**") and the Proposed Positions for Regulations under the PDPA ("**Regulation Proposed Positions**").

2. The publication of the Guidelines and Regulation Proposed Positions for public consultation is a positive step that will further the understanding and interpretation of privacy and data protection issues as they relate to industry, business, individuals and the Singapore Government.

3. MasterCard, as a global payments processing company, is committed to protecting and respecting the personal data of our cardholders and customers. We are committed to working with the Commission to craft and develop these Guidelines, the Regulations and any future guidelines and regulations that the Commission may consider, in a manner that protects the individual while ensuring ease of commerce.

[1] MasterCard is a global payments and technology company that connects billions of consumers, thousands of financial institutions, millions of merchants, governments and businesses in more than 210 countries and territories, enabling them to use electronic forms of payment instead of cash and checks. We use our technology and expertise to make payments more convenient, secure and efficient to enable consumers to meet their needs and to provide value to all stakeholders in the payments system.

4. The Guidelines and the Regulations are an important aspect of the data protection regulatory framework and will provide the rules of the road for the Commission, industry and the public in the implementation of the PDPA. We believe that they should continue to be refined to provide practical guidance on what the Commission will view as acceptable in a specified situation.

5. We submit the following comments below for the Commission's consideration, and offer them to further assist the Commission in the process of refinement. We are happy to assist the Commission in the continued development of the regulatory framework, and the development of privacy and data protection in Singapore.

Summary of Major Points

6. Our major points are summarized below as follows:

- Definition of Personal Data – We support the Commission's contextual approach in the determination of personal data. We suggest that the Commission further refine the definition to indicate that an organization must be able to identify the individual based upon the nature and type of data in its possession. We would suggest a standard that would reference the likelihood for an organization to be able to identify an individual taking into account the amount of time, effort and expense involved.

- Data Intermediary - We welcome the streamlined and simplified approach adopted by the Commission. We agree that the written contract is a necessary factor in determining whether an organisation is a data intermediary for the purposes of section 4(2) of the PDPA and that the contents of the contract will provide an indication of whether an entity is a data intermediary.

- Obtaining Consent from an Individual – We appreciate the Commission's position regarding the "failure to opt-out as consent" as noted in paragraph 11.7 of the Key Concepts Advisory Guidelines, and suggest that the Commission further explain "the limited circumstances" where failure to opt-out would be considered consent.

- Access & Correction Requests - In relation to paragraph 14 of the Key Concepts Advisory Guidelines, it should be clarified that where a data intermediary receives an access or correction request, the data intermediary may ask the individual to contact the relevant organisation that had engaged the data intermediary. This will ensure all parties are aware of the need for access or correction.

- Identification of Officers – We suggest that in relation to paragraph 19.6 of the Key Concepts Advisory Guidelines, the Guidelines should adopt the Ministry's clarification that organisations may identify officers by their positions or titles, instead of by their names.

- Contractual Performance – We suggest that in relation to paragraph 21 of the Key Concepts Advisory Guidelines, the Guidelines should be clarified to state that the performance of a contractual obligation may be a relevant factor in determining compliance with the obligations of the PDPA.

- Anonymisation - We have made several suggestions which we believe will provide more certainty for organisations, and which will encourage organisations to anonymise data. Given the potential protections and benefits of anonymisation, companies should be encouraged to implement anonymisation techniques. We suggest adding more guidance to the document as that would be helpful to ensure adequate protections are put into place to limit the risks of re-identification.

A more comprehensive discussion of these points and several other points is submitted for your consideration below.

7. Definition of Personal Data

7.1 We suggest that the Commission further refine the definition to indicate that an organization must be able to identify the individual based upon the nature and type of data in its possession. We would suggest a standard that would reference the likelihood for an organization to be able to identify an individual taking into account the amount of time, effort and expense involved.

7.2 In relation to paragraphs 5.9 to 5.12 of the Key Concepts Advisory Guidelines, we note that the Commission has taken a contextual approach to determining whether an individual can be identified from a set of data, and hence whether the data will be considered as personal data. We fully agree that this is an appropriate approach.

7.3 In summary, we propose that the Key Concepts Advisory Guidelines could be amended to add the following sentences to paragraph 5.12 of the Key Concepts Advisory Guidelines:

> "The threshold for determining an individual to be identifiable from personal data should be that the organisation must be reasonably able to link the data and hence identify an individual from that data. Further, hypothetical possibilities of identifying an individual from personal data should not be considered as the test. The Commission will also take into account considerations relating to the cost, difficulty and practicality of access to the different data sets when determining whether an individual is identifiable from the data."

8 Data Intermediaries

8.1 In relation to paragraph 6.22 in the Key Concepts Advisory Guidelines, we note that the Commission places significance on the written contract (specifically the setting out of the respective parties' responsibilities and liabilities) between the parties in determining whether an organisation is the data intermediary or not.

8.2 We agree that the written contract is a necessary factor in determining whether an organisation is a data intermediary for the purposes of section 4(2) of the PDPA and that the contents of the contract will provide an indication of whether an entity is a data intermediary, and we welcome the streamlined and simplified approach which the Commission has adopted.

9 Obtaining consent from an individual

9.1 In relation to paragraph 11.7 of the Key Concepts Advisory Guidelines, we note that the Commission has taken the view that "failure to opt-out would only be considered consent in certain limited circumstances". We appreciate the Commission's position and flexibility in providing this definition, but ask for additional clarity and examples. While one example is provided after paragraph 11.7, additional examples would be helpful.

10 Deemed consent

10.1 We appreciate the guidance provided by the Commission in the examples after paragraphs 11.18 and 11.22 as a growing number of payments in Singapore are transacted using credit cards. A typical credit card transaction will involve other actors (besides the bank identified in the examples) that will be receiving the transaction data but will not have a direct relationship with the individual. In order to further aid in providing clarity and certainty, we suggest that the examples mention the other parties (e.g. payment system providers and the bank's processors) that may be in the chain of processing the payment transaction.

11 Withdrawal of consent

11.1 In the event of withdrawal of consent, the Commission has taken the view that "the organisation must inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the organisation's purpose".

11.2 We suggest it would be preferable to require the organisation to take reasonable steps rather than introduce the concept of "ensure". The word "ensure" may imply that the

organisation must in some way guarantee that the data intermediary and agent stop the collection, use or disclosure of the personal data.

12 The Access and Correction Obligation

12.1 In relation to paragraph 14 of the Key Concepts Advisory Guidelines, we suggest that the Guidelines could clarify that where a data intermediary receives an access or correction request, the data intermediary may ask the individual to contact the appropriate organisation directly.

12.2 This redirection of the request to the organisation would also be consistent with the usual contractual obligation placed on the data intermediary to inform the organisation of any access or correction rights. The guidance will also ensure that individuals will not be surprised by the redirection of the request to the instructing organisation as they may not understand the concept of a data intermediary.

13 Business Contact Information of an individual designated by the organization

13.1 In relation to paragraph 19.6 of the Key Concepts Advisory Guidelines, we propose that paragraph 19.6 of the Key Concepts Advisory Guidelines should repeat the Ministry's clarification that organisations may identify officers by their positions or titles, instead of names of the officers. This clarification was mentioned in the public consultation document on the proposed Personal Data Protection Bill conducted by the Ministry of Information, Communications and the Arts on 19 March 2012. The Ministry had clarified that "organisations could be given the flexibility to designate the appropriate contact point accountable for DP issues" and "organisations may identify officers so designated by their positions or titles, instead of names of the officers".

14 Existing rights, etc under law

14.1 In relation to paragraph 21 of the Key Concepts Advisory Guidelines, we note that the Commission makes it clear that the performance of a contractual obligation shall not be an excuse for contravening the PDPA. We agree with this position as one cannot contract out of the requirements of the law. However, we think that there would be a situation where it would be relevant for an entity to assert the performance of a contractual obligation as a relevant factor in determining one's compliance with an obligation under the PDPA.

14.2 For example, if a data intermediary stores data on behalf of an organisation, and the organisation contractually requires the data to be stored for a specified number of years for its business purposes then it may be necessary for the data intermediary to assert this contractual obligation in justifying its storage of the data under section 25 of the PDPA (which is one of the 2 provisions in the PDPA which a data intermediary would be subject to).

14.3 Therefore, we would suggest that the following paragraph be added as a new paragraph 21.3 in the Key Concepts Advisory Guidelines to clarify that the performance of a contractual obligation may in a limited situation be a relevant factor in determining compliance with the obligations of the PDPA:

> "There may, however, be certain situations where the assertion of a contractual obligation will be a relevant factor in determining compliance with an obligation under the PDPA. Specifically, where a data intermediary stores data on behalf of an organisation, and the organisation contractually requires the data to be stored for a specified number of years for its business purposes, it may be necessary for the data intermediary to assert this contractual obligation in justifying its storage of the data under section 25 of the PDPA."

Advisory Guidelines on Selected Topics

15 Anonymisation

15.1 We agree with the rationale presented in the Selected Topics Advisory Guidelines that there are several benefits to anonymisation including serving as a protection measure against inadvertent disclosures and security breaches, and using of the data where personal identifiers are not necessary.

15.2 We also believe that organisations should be encouraged to implement anonymisation techniques where it is appropriate to their business. In this connection, we believe that some changes could be made to the Selected Topics Advisory Guidelines to encourage organisations to implement anonymisation.

15.3 We note that paragraphs 4.16 to 4.19 of the Selected Topics Advisory Guidelines contains a general description of the "effectiveness of anonymisation" (which is the title of the section), and a brief discussion of two studies (the Netflix study and the Group Insurance Commission study). We believe that the description in paragraphs 4.16 to 4.19 may present an incomplete picture of the effectiveness of anonymisation and the degree of difficulty in re-identifying de-identified information.

15.4 In this connection, we would quote Dr. Ann Cavoukian, the Information & Privacy Commissioner of Ontario, Canada:

> "We believe it is highly misleading to suggest that the re-identification of individuals from de-identified data is an easy task. As long as proper de-identification and re-identification risk measurement techniques are employed, the re-identification of individuals is relatively difficult in actual practice. In fact, a recent review of the evidence indicates that there are few cases in which properly de-identified data have been successfully re-identified. Further, in those cases where properly de-

identified data were successfully re-identified, the re-identification risk was very low. The evidence is not consistent with the popular view relating to the fabled failure of anonymisation."

Dispelling the Myths Surrounding De-identification: Anonymisation Remains a Strong Tool for Protecting Privacy (June 2011)

15.5 While we accept that there are challenges involved in ensuring that information remain de-identified, we do not believe that the two case studies presented are representative of the "effectiveness of anonymisation".

15.6 It is important to note that the two case studies in paragraphs 4.16 to 4.19 of the Selected Topics Advisory Guidelines published databases of individualized records, and the linking of these published databases with other data sets. As noted in paragraph 4.25 of the Selected Topics Advisory Guidelines, the risk of this can be minimized by taking precautions to limit the disclosure of the information and adding enforceable restrictions on the use of the data. This, we believe, would more accurately portray the effectiveness of anonymisation.

15.7 We also suggest this section in the Selected Topics Advisory Guidelines acknowledge anonymisation (if implemented correctly) can make re-identification significantly difficult, and can be an effective and important tool in protecting personal data. It may also be useful to present positive studies which reflect the relative difficulty of re-identifying de-identified data.

15.8 Given the potential protections and benefits of anonymisation, companies should be encouraged to implement anonymisation techniques. We suggest that adding more guidance to the document would be helpful to ensure adequate protections are put into place to limit the risks of re-identification, and also to encourage companies to adopt anonymisation.

15.9 Potential guidance to include in the Selected Topics Advisory Guidelines will include:

- Case studies which are similar to that used by the UK ICO in Annex 2 of the Anonymisation: Managing Data Protection Risk Code of Practice, with an assessment of re-identification risk.

- Information related to the difficulty and practicality of re-identification. We suggest that the test should be whether it is reasonable that identification may occur notwithstanding the anonymisation process. If it is too costly, difficult or impractical to identify the individual, then the data should be considered as anonymised (and hence not personal data).

- Identifying anonymisation of personal data as a purpose which is clearly in the interest of the individual under paragraph 1(a) of the Second and Third Schedules of the PDPA. As anonymisation may be considered as a "use" of personal data under the PDPA, identifying anonymisation as a purpose which is clearly in the interest of the individual under paragraph 1(a) of the Second and Third Schedules of the PDPA will benefit both the individual (in terms of increasing protection for the individual), and also the organisation.

15.10 In summary, we suggest the following changes:

15.10.1 Amendment to paragraph 4.19 of the Selected Topics Advisory Guidelines:

> "Hence, while data can be anonymised, it is not guaranteed that data will stay anonymised. Re-identification of individuals by combining anonymised datasets with other information presents a significant challenge to the protection of personal data. <u>This is especially so where the datasets are published and widely available (as was the case in the case studies mentioned above). Such re-identification risks can be lowered by taking the steps identified in paragraph 4.25 of these Guidelines."</u>

15.10.2 A new paragraph 4.20 of the Selected Topics Advisory Guidelines could be included as follows:

> "However, anonymisation, if implemented correctly, can make re-identification significantly difficult, and can be an effective and important tool in protecting personal data."

15.10.3 Amendment to paragraph 4.23 of the Selected Topics Advisory Guidelines:

> "Various jurisdictions have considered the issue of anonymisation and re-identification risks in the context of data protection. Like many jurisdictions, the Commission will take a practical approach towards anonymisation and risks of identification. If the risk of re-identification is high, then the data will be considered personal data. If the possibility of re-identification is trivial, the Commission will consider the data anonymised. <u>In addition, the Commission will consider whether it is reasonable that re-identification will occur. If it is too costly, difficult or impractical to identify the individual, then the data would be considered as anonymised.</u>"

15.10.4 A new paragraph 4.39 of the Selected Topics Advisory Guidelines could be included as follows:

"To encourage organisations to implement anonymisation of personal data as a way of protecting individuals' personal data, the Commission will take the view that anonymisation of personal data is a purpose which is clearly in the interest of the individual under paragraph 1(a) of the Second and Third Schedules of the PDPA."

Regulation Proposed Positions

16 How organisations should respond to access and correction requests

16.1 In relation to paragraph 3.7(b) of the Regulation Proposed Positions, we note that the Commission has proposed that an organisation must provide the requested personal data within 30 days of the individual's request. It is not clear whether the 30 days commence from the date of receipt of the request, or the date of sending of the request, or the date identified on the request itself. Further, it is unclear whether the request must conform to the requirements in the Regulations in order for time to start running.

16.2 We propose that the Regulations should clarify that the 30 day period commences from the date of receipt by the organisation of a request from the individual that conforms to the requirements in the Regulations (on the point of conforming to the requirements, please see our comments in paragraph 17 below). This would be similar to the approach taken in the UK and Hong Kong. It will also:

- allow the organisation to have the full 30 days to respond to a request;
- prevent any backdating of the date of the request (if the request is sent by letter); and
- avoid misunderstandings of when the response is to be expected.

17 How access and correction requests should be made by individuals

17.1 In relation to paragraph 4.1 of the Regulation Proposed Positions, we agree with the proposed approach to require the access request or correction request to include sufficient details to enable the organisation to which the request is made to identify the individual and the personal data or correction that is being sought.

17.2 To provide greater clarity to this provision, we suggest the following additional conditions for consideration:

- The request or correction request should contain the contact details of the individual in order to respond to the individual. This will ensure that the individual may be contacted for clarifications, etc; and

- Where the requestor is acting on behalf of an individual, the request or correction request should contain sufficient information to satisfy the organisation of the identity of the individual and that the requestor has the necessary authority to act in such capacity.

18 Transfer of Personal Data Outside Singapore

18.1 In relation to paragraph 7.9 of the Regulation Proposed Positions, we note that the Commission has proposed that the contractual clauses contained in a legally binding contract that is enforceable against every organisation receiving personal data under the contract.

18.2 We believe that the requirement in paragraph 7.9 of the Regulation Proposed Positions should be revised to reflect that the contractual clauses are enforceable against the parties to the contract. The requirement of enforceability should not extend to other entities which are not parties to a contract as there are difficulties in enforcing a contract against such entities.

18.3 For example, if a sub-contractor of the contracting entity is or will be receiving personal data under the contract, the sub-contractor will not be a party to the contract (which leads to difficulties in enforceability), and may also not be identified at the time of entering into the contract. This proposed approach will not derogate from the principle of accountability as the contracting entities will still be accountable for the contractual obligations which they have entered into.

19 Individuals who may act for others under the PDPA

19.1 In relation to paragraph 8 of the Regulation Proposed Positions, while we agree that there will be situations where a person will need to act "on behalf of" an individual in the exercise of rights and powers under the PDPA, we believe that there may be difficulty when determining whether the person will be acting "on behalf of" the individual. The organisation in most situations is not in a good position to determine this or even the veracity of such claims.

19.2 There are practical difficulties for organisations to determine whether a person is actually acting on behalf of the individual, and the organisation is very much dependent on the information and documentation provided by the person. The potential consequence for the organisation (who responds due to misrepresentations or misinformation provided by the person) is that it may then disclose information without the consent of the individual concerned, and would be subject to both private rights of action by the individual (or the properly authorized person) and the Commission. We, of course, understand that there may be penalties for a person who accesses information without the authority of the individual (under section 51(1) of the PDPA), however that

would still be cold comfort for the organisation as it could still potentially face the uncertainty of an action from both the individual or the Commission. Organisations need to know that they will not be held responsible for disclosures if a misrepresentation or fraud has been committed on them.

19.3 As such, we propose that the Regulations should reflect that (i) the person purporting to act on behalf of the individual must provide the necessary proof to support the relationship, and (ii) if an organisation acts in good faith in response to a request and on the basis of the information and documents presented by a person purporting to act on behalf of an individual, the organisation would not be liable in so responding if the information and documents are fraudulent, invalid or incorrect.

Thank you again for the opportunity to comment on the Proposed Advisory Guidelines and the Regulation Proposed Positions. We would welcome the opportunity to meet with the Personal Data Protection Commission to further discuss our views. Please do not hesitate to contact us if you have any questions regarding our comments.

Sincerely,

Derek Ho
Privacy & Data Protection Counsel

Dave Tan
Vice President
Public Policy, Asia Pacific