Comments to the Public Consultation Issued by the Personal Data Protection Commission on 5 February 2013 on:

(i) Proposed Regulations on Personal Data Protection in Singapore;
(ii) Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act; and
(iii) Proposed Advisory Guidelines on the Personal Data Protection Act for Selected Topics.

Submitted by:
American Express International Inc.
Mapletree Business City
#08-00 Block C20 (West)
Pasir Panjang Road
Singapore 117439

Submission Date:
19 March 2013

Contact Persons:
Jane Foo
Director, Compliance & Ethics
 65-6317-6026 | jane.foo@aexp.com

Joanne Tay
Senior Manager, Compliance & Ethics
 65-6317-6206 | joanne.p.tay@aexp.com

Annabell Koh
Senior Analyst, Compliance & Ethics
 65-6317-6035 | annabell.koh@aexp.com

A. Introduction

By way of background, American Express International, Inc. ("American Express") carries various businesses in Singapore including the issuance of consumer and corporate cards, merchant acquisition and servicing, acting as corporate agent to various insurers, provision of money-changing, remittance and other travel-related services. In the course of providing our services in Singapore, including marketing activities, American Express collects, uses and discloses personal data of our customers.

We refer to the three public consultation papers issued by the Personal Data Protection Commission ("Commission") on 5 February 2013 (together, the "Consultation Papers"), relating to the:

(1) Proposed Regulations on Personal Data Protection in Singapore;
(2) Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act ("PDPA"); and
(3) Proposed Advisory Guidelines on the PDPA for Selected Topics.

We have enclosed our detailed comments to the Consultation Papers in this document, and thank you for the opportunity to share our feedback.

B. Summary of Major Points

In general, we welcome the additional clarity provided by the Commission to the PDPA in the Consultation Papers. We have set out our views and proposals in greater detail in the following pages, in particular in relation to the Consent Obligation.

C. Comments to the Proposed Regulations on Personal Data Protection in Singapore ("Proposed Regulations")

Part II: Administration of Requests for Access to and Correction of Personal Data

6.4 Key considerations in relation to the administration of access and correction requests

The Commission has stated at Section 6.4 of the Proposed Regulations that it does not intend to specify the maximum amount chargeable for access request fees. We believe it would nonetheless be helpful to organizations if the Commission could provide a range of fees that would be deemed acceptable, to avoid a very wide range of access request fees in the market.

Part IV: Individuals who may act for others under the PDPA

8.2 Exercise of rights and powers of individuals

The Commission has stated at Section 8.2 of the Proposed Regulations that it is possible for an individual ("A") to exercise on behalf of another ("B"), a right or power conferred under the PDPA on B. It is unclear from section 14(4) of the PDPA whether a written authorization from B would be required to evidence, though the Commissioner's view in Section 8.2(b) seems to indicate that written consent from B may be necessary. We take the view that this would be unduly onerous for organizations and propose that it would be sufficient for an organization to obtain a declaration from A, that he/she has been duly authorized and is validly acting on behalf of B. This is especially so in instances of customer referral programs, whereby A is providing the organization with the basic contact details of B.

9.9 Priority of nearest relatives to an individual

The Commission has proposed an order of priority list for relatives of a deceased individual. We respectfully submit that it would be unduly onerous and difficult for an organization to ensure adherence to this order of priority. An organization would not usually have such detailed information on the deceased customer's family tree and relationships. Therefore we propose that instead of placing the onus on organizations to determine the priority of the relatives, organizations should be entitled to rely on the following steps to allow a relative to act on behalf of the deceased:

(i) sight a death certificate of the individual;
(ii) obtain a signed declaration from the relative purporting to act on behalf of the deceased individual, to confirm that he/she is entitled to act on behalf of the individual.

D. Comments to the Proposed Advisory Guidelines on Key Concepts in the PDPA ("Advisory Guidelines")

Part II: Important Terms used in the PDPA

5.10 Personal Data

We believe a voice recording would be deemed as "personal data", if an individual can be identified from that voice recording. However in instances whereby a specific individual cannot be identified (eg: general call to customer service hotline with no other personal data provided), we take the view that the voice recording would not constitute personal data.

Part III: The Data Protection Provisions

11.7 The Consent Obligation - Obtaining consent from an individual

In Section 11.7 of the Advisory Guidelines, the Commission stated its default position is that an individual's failure to opt-out would not constitute consent. Further, that failure to opt-out would only be considered consent in **certain limited circumstances**.

We respectfully submit that this default position appears to contradict other sections of the PDPA, in particular section 15 on "deemed consent". If deemed consent is allowed, then a failure to opt-out should be construed as consent where the conditions in section 15 of the PDPA are met.

In the event the Commission prefers to retain this statement, we propose that for clarity, the Commission may state that these "limited circumstances" include a scenario where the provision of data is essential to the provision of goods and services. In other words, an organization may rely on a failure to opt out as consent, where the data subject has voluntarily provided personal data, data use is necessary and essential to enable the organization to supply goods and services requested by the data subject, and the data subject has been notified of such purpose and use. This would not be inconsistent with the deemed consent provisions under the PDPA.

11.26/7 The Consent Obligation - Obtaining personal data from third party sources with the consent of the individual

Please see our comments to Part IV, section 8.2 of the Proposed Regulations on Personal Data Protection in Singapore on page 3 above.

11.39 The Consent Obligation - Withdrawal of Consent

As set out in the Third Schedule of the PDPA, an organization is not required to obtain the individual's consent for the use of his personal data for debt recovery. However at Section 11.39 of the Advisory Guidelines, the Commission states that an organization cannot prohibit an individual from withdrawing his consent to the use of his data.

We propose the Commission clarifies that an individual should be prohibited from withdrawing his consent to use of his data for debt recovery. This principle should apply as well in other cases where the use of data falls within one of the exclusions set out in Schedules II to IV of the PDPA.

11.48 The Consent Obligation - Publicly Available Data

At American Express' foreign exchange retail outlets in Singapore, CCTVs are installed for security purposes. These CCTVs capture video images of individuals at the retail outlets. Since these retail outlets are open to the public, we take the view that the video images are publicly available personal data, and explicit consent from individuals is not required. We respectfully request that the Commission clarifies that it would be sufficient for organizations to comply with the obligations under the PDPA, if organizations display a notice at retail outlets informing the public that the area is being monitored by CCTV and that their images might be captured.

In addition, organizations will also often conduct private events at reserved function areas, which are not accessible by the public. Based on the example provided by the Commission, since this is a private event, the images of attendees captured by photographers hired for the event will not be publicly available data. We submit that it would be onerous and administratively difficult for the organization to obtain written consent from every attendee for the collection, use and disclosure of his/her photograph, especially at mega-events involving thousands of individuals. Therefore we respectfully propose that the Commission allows organizations to meet its obligations under the PDPA in such situations, by including a clear notification (eg: at the event registration counter) to inform attendees of the photography activities.

14.1 The Access and Correction Obligation – Access to Personal Data

Section 21 of the PDPA requires an organization to provide information about the ways in which personal data has been or may have been used or disclosed by the organization within a year before the date of the individual's request. In Section 14.5 of the Advisory Guidelines, the Commission proposed that an organization may develop a list of all possible third parties to whom personal data may have been disclosed by the organization, instead of a list that specifically relates to the personal data of a particular individual.

We respectfully propose that the Advisory Guidelines should permit an organization to respond to a data subject's request by providing a list of general categories of third parties to whom personal data may have been disclosed. For instance, instead of specifying that data has been or may have been provided to Company A, Company B, Company C…Company Z etc, an organization may state that data has been or may have been provided to (i) affiliates within the organization's group, (ii) insurance companies for whom the organization is acting as an agent, (iii) third party outsourced service providers etc. This would recognize the fact that large multinational companies have extensive and complex supplier relationships and organizational structures. It would be excessively burdensome on and potentially diminish the competitive position of an organization if it was required to disclose each of these third parties specifically.

17.2 The Retention Limitation Obligation – Retention of personal data

The Commission stated in section 17.2 of the Advisory Guidelines that organizations are prohibited from retaining personal data in perpetuity where it does not have legal or business reasons to do so. We wish to highlight that organizations may have historically collected and stored hardcopies of customer application forms and other documents containing personal data in secure warehouses. These documents may date back tens of years and involve hundreds of thousands of customers. It would therefore be excessively burdensome for organizations to retroactively review all these documents to identify and destroy the ones no longer required (eg: closed accounts, deceased customers). We respectfully propose that such historical data should be excluded from the Retention Limitation

Obligation and that this requirement only be applied from the effective date of the corresponding PDPA provisions.

19.1 The Openness Obligation

The Commission stated in section 19.1 of the Advisory Guidelines that organizations must make their data protection policies and practices available. We propose that only policies and practices that are targeted at customers be made available at customers' requests, and respectfully request the Commissioner clarify that an organization's internal or other operational policies and procedures need not be made available to the public.

Part IV: Other Rights, Obligations and Uses

22.1 Other written law

This section states that the provisions of any other law shall prevail over the Data Protection provisions of the PDPA. Under the Banking Act (Third Schedule, Part 2 Row 9), banks are allowed to disclose customers' information (ie: name, identity, address and contact number) to other financial institutions, for the promotion of financial products and services. This means that Banks will be able to rely on this provision of the Banking Act, to exchange customer data without consent. We believe this creates an unlevel playing field between banks and non-bank entities, and would appreciate the Commission's views on the rationale for the different treatment.

Part V: The Do Not Call Provisions

33.2 Clear and unambiguous consent

Section 13 of the PDPA states that an organization must have obtained a customer's consent before it can collect, use or disclose the customer's personal data. Section 43(3) of the PDPA in relation to the Do Not Call ("DNC") Registry, contemplates that an organization may use the customer's telephone number without verifying with the DNC Registry, if it has clear and unambiguous consent from the customer.

It is not clear to us whether the consent obtained under the data protection principle in section 13 of the PDPA, would suffice as clear and unambiguous consent for the purposes of the DNC Registry. Alternatively, is the Commission requiring organizations to collect additional explicit and distinct consent from a customer in relation to the DNC Registry?

In the Commission's example in section 33.2 of the Advisory Guidelines, it is also not clear whether the Commission expects organizations to adopt an opt-in approach to satisfy the clear and unambiguous consent requirement for the DNC Registry. We propose that an opt-in approach is not necessary. Accordingly, taking the Commission's example in Section 33.2, if the check box says instead "click here if you do not wish to receive information about our products and services, including special offers we may have from time to time by SMS", and Sarah does not check the box, Sarah should be deemed to have given clear and unambiguous consent to receive such messages by SMS.

34.1 Duty to identify the sender of a message

We propose that abbreviations of an organization's name would suffice for this sender requirement (eg: "Amex" instead of "American Express International Inc"), in particular in view of the character limitations of various messaging systems.

E. Comments to the Proposed Advisory Guidelines on the PDPA for Selected Topics

We have no comments on these proposals at present.

F. Conclusion

We appreciate your consideration of our comments and look forward to your further clarification. If you need any additional information, please feel free to contact us (details on cover page).