American Express International Inc.
Incorporated with Limited Liability in the State of Delaware, U.S.A
10 Marina Boulevard #15-00,
Marina Bay Financial Centre Tower 2,
Singapore 018983
UEN S68FC1878J

BY EMAIL

20 September 2017

Personal Data Protection Commission Singapore
460 Alexandra Road
#10-02 PSA Building
Singapore 119963
corporate@pdpc.gov.sg

Dear Sirs

PDPC's Public Consultation for Approaches to Managing Personal Data in the Digital Economy

American Express welcomes the opportunity to provide its comments on the Public Consultation issued by the Personal Data Protection Commission on 27 July 2017 in respect of Approaches to Managing Personal Data In The Digital Economy.

Introduction to American Express

Founded in 1850, American Express is a global payments, network, and travel company. We first established business in Singapore in 1925 and American Express operates in Singapore through a branch of American Express International, Inc., that has been licensed as a financial institution by the MAS under Section 57 of the Banking Act to issue credit and charge cards. In addition, American Express holds a license under the Money-Changing and Remittance Businesses Act pursuant to which it provides remittance services to corporations in Singapore.

Feedback from American Express

Our feedback to certain questions raised in the Consultation Paper is set out in the attached Annex A for your consideration. Where we have not provided feedback to a question in the Consultation Paper, American Express has no further comments to the proposal.

We thank you again for the opportunity to share our thoughts on these proposals with the PDPC.

Yours sincerely,

Kiyoko Toda
Vice President, International Regulatory Compliance – Head of Japan & Southeast Asia (Singapore/Thailand)
For and on behalf of
American Express International, Inc.

ANNEX A

1. Criteria for Breach Notification

Question 5: *What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?*

1.1 American Express appreciates that in the event of a personal data breach, the PDPC and affected individuals who may be impacted by such breach should be informed of the breach without undue delay, so as to allow the affected individuals to take the necessary steps to protect themselves from the risks or impact of such breach and the affected organization will also be able to receive guidance from the PDPC on remedial actions. The aim of such a proposal is to build public trust and confidence in an organization's handling of and safeguards over personal data.

1.2 We note at paragraph 6.2 of the Consultation Paper that PDPC has proposed the following criteria for notification to affected individuals and/or PDPC of a data breach:

(i) Risk of impact or harm to affected individuals; or

(ii) Significant scale of breach.

1.3 In respect of notification of a data breach which poses any risk of impact or harm to affected individuals, we respectfully urge that the PDPC adopt a materiality threshold similar to the approach taken in Australia where there should be sufficient grounds to believe that the data breach will result in a serious risk of harm to an individual. For example where there has been attempted fraud or financial loss on a customer's account.

Where there is a lack of a materiality threshold, the requirement to notify an affected individual may create an onerous regulatory burden on the organization and may also unnecessarily cause alarm to an individual.

We would also suggest that the PDPC provide risk assessment guidelines to organizations in assessing the severity of the risks and impact of a data breach (such as the type of information involved in the breach, whether there were measures in place to minimize the impact of a breach) to ensure a consistent approach of risk assessment across organizations.

1.4 In respect of the proposed threshold of 500 impacted individuals for the purposes of determining the significance of the scale of a data breach, we agree with the proposed threshold if this refers to 500 impacted customers of American Express in Singapore and not globally as this threshold may not be significant in terms of the scale of our global business.

2. Concurrent Application with Other laws and Sectorial Breach Notification Regimes

Question 6: *What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?*

2.1 We agree with the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations (such as the MAS Technology Risk Management Notice and Guidelines, the MAS Outsourcing Guidelines and the impending Cybersecurity Act). A concurrent application will reduce regulatory overlap and ensure that organizations are not subject to multiple regulatory requirements in respect of the same data breach. This will also allow organizations to prioritize resources on investigating, resolving, containing and remediating the data breach.

2.2 However, in order to enable organizations to manage queries from various regulators in an efficient manner whilst still focusing on resolving, containing and remediating the data breach, we propose that the relevant sector regulator take the lead in communicating with the organization on behalf of PDPC and other regulators (such as the CSA). For example any queries from the PDPC and updates on the resolution and remediation of the data breach by the organization and guidance to the organization by the PDPC could be channeled through the sector regulator.

3. Time Frame for Breach Notification

Question 8: *What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?*

3.1 We note that the PDPC has suggested that organizations notify the PDPC as soon as practicable, and no later than 72 hours from the time it is aware of the data breach. The Consultation Paper further proposes that the organization is required to notify notwithstanding that the breach is not confirmed, and whether or not it has essential facts about the breach in order to give a meaningful notice. The remaining information can be provided to the PDPC as soon as possible after the initial notice.

3.2 Whilst we appreciate that a cap of 72 hours provides clarity for organizations as to the definitive time by which to notify PDPC, we would respectfully urge the PDPC to recognize that:

(i) Global organizations may require more time to understand the impact of a breach on customers in Singapore therefore it may be challenging to meet the cap of 72 hours; and

(ii) Follow up queries from the PDPC and other regulators should not hinder or impede the foremost priority of the organization to contain the data breach, conduct investigations, make the necessary risks assessments, and implement appropriate remedial and preventive measures. Accordingly, we would propose that following the notification to the PDPC, organizations should be provided with sufficient time to carry out its data breach management and response plan and thereafter provide a follow-up report to PDPC with details of the breach, cause of the breach, risk impact assessment of the breach, and a description of actions taken to address, resolve and remediate the breach and information on notification to affected individuals.

4. Additional Comments

Time Frame for Implementation of Amendments

4.1 The proposed enhancement to the PDPA will require all organizations to review their current processes on the handling of data breaches, implement changes to internal personal data policies and processes, review contracts with third parties (such as DIs) and make corresponding amendments to comply with the regulatory changes.

4.2 We respectfully request that the PDPC provide for an implementation period of 12 months to allow organizations to comply with the amendments to the PDPA.

Obligations of Data Intermediary

4.3 We would also urge the PFPC to clarify the responsibility between an organization and its data intermediaries (DI) in notifying data breaches under the new proposals.

4.4 As proposed in the Consultation Paper, the DI is only required to immediately inform the organization of any level of data breach, and the organization is thereafter responsible for complying with the breach notifications under the PDPA.

4.5 There could be instances where a DI would perform the role of a service provider in addition to processing personal data for and on behalf of another organization. An example could be a hotel which accepts cards as a payment method for reservations at the hotel and would need to transmit data to the card issuer for authorization. The hotel would also collect other personal data (apart from the card details) from the customer for the purposes of fulfilling the reservation. Where the hotel's reservation system is compromised and a data breach occurs involving the card details and other personal data of the customer, the hotel would be best placed to provide information on and notify the customer of the data breach as the point of compromise is on the hotel's systems. Requiring the card issuer to also notify the customer would not be ideal as the card issuer would only be able to notify the customer that payment card details were compromised and this could also lead to confusion and a lack of clarity in terms of the appropriate steps that the customer would need to take to protect themselves.

4.6 Accordingly, where an organization performs a dual role of a service provider and a DI,and is the point of compromise of a data breach, such an organization should be primarily responsible for notifications of the data breach.

.