RESPONSE TO CONSULTATION PAPER

Consultation topic:	Public Consultation for the PDP (Amendment) Bill
Organization:	American Express International, Inc.
Contact number for any clarification:	[Redacted]
Email address for any clarification:	[Redacted]
Confidentiality	
I wish to keep the following confidential:	Contact details provided above to be kept confidential.

Table of Contents

1. SUMARRY OF MAJOR POINTS 3
2. STATEMENT OF INTEREST 3
3. COMMENTS 3
   - 3.1 Mandatory Breach Notification 3
   - 3.2 Data Portability Obligation 4
   - 3.3 Marketing Messages to IM Accounts 5
   - 3.4 Obligation and Liability on Third-Party Checkers 5
   - 3.5 Derived Personal Data Exemptions 6
4. CONCLUSION 6

1. SUMARRY OF MAJOR POINTS

American Express International Inc. (“American Express”) would like to thank the Ministry of Communications and Information ("MCI”) and the Personal Data Protection Commission (“PDPC”) for the opportunity to participate in the public consultation on the Draft Personal Data Protection (Amendment) Bill (“Bill”).

2. STATEMENT OF INTEREST

American Express takes a very serious view of our obligations to protect our customers’ data and respect their privacy under the Personal Data Protection Act (“PDPA”) and the Spam Control Act (“SCA”). In light of the proposed changes to these key legislations, American Express would like to provide our feedback for your considerations.

3. COMMENTS

3.1 Mandatory Breach Notification

American Express commends MCI and PDPC for its proposal to strengthen the accountability of organisations in protecting all personal data under their care. In particular, we agree with that enforcing a mandatory breach notification will encourage organisations to enhance their data security controls.

In respect of the proposed requirements to the mandatory notification of data breaches, we note that PDPC previously issued the Guide to Managing Data Breaches 2.0 (“Guide”) on 22 May 2019. This Guide comprehensively illustrates the 4 key steps in managing data breaches effectively: Contain, Assess, Report and Evaluate.

Given that the Guide offers additional details that can benefit organisations in developing a thorough framework for managing data breaches, may we clarify if the Guide, in its entirety, will continue to apply to data breaches? More specifically, are organizations expected to rely on the Guide in respect of the following:

- Performing the assessment on whether a data breach will likely be considered to result in significant harm based on the considerations detailed under Step 2 - Assess.
- Expectation on organisations to carry out the assessment of the data breach expeditiously within 30 days from when they first become aware of a potential data breach.
- Method of notification and details to be provided to PDPC and to affected individuals for notifiable data breaches, as detailed in Annexes B and C of the Guide, respectively.

3.2 Data Portability Obligation

American Express supports to the concept of data portability as a means to increase competition, innovation and customer value. The frictionless exchange of data is the lifeblood of modern economies, and in the financial sector specifically. We commend the proposed amendment to include Data Portability in the Personal Data Protection (Amendment) Bill and are broadly in favour of the inclusion of the right to data portability in the legislation.

While we welcome the introduction of the mechanism of data portability, we would also call for the development of practical ways for individuals to exercise the portability right, specifically around:

- **Scope and data types.** Define who the rules will apply to and what data types should be in scope (e.g., user provided, and user activity data may include personal data). We would also suggest clarifying the scope of data portability (e.g. only personal data and not anonymised data), and more particularly the possibility to port third parties' data outside of the "personal or domestic capacity". Will details of third parties involved (along with the requester's personal data) which also concern the requester be included in the response to data portability? Also, we would suggest that companies should always consider whether there will be an adverse effect on the rights and freedoms of third parties, when transmitting data directly to another controller without consent.
- **Format and transfer process.** It is of paramount importance that there is a prescribed data format and transfer process that maintains the integrity and security of the data whilst remaining accessible and usable. Data will only be truly portable if it is accurate, secure and can be used. For example, what format to adopt (CSV or API), what data should be included, how should customer experience look like (incorporating flexibility where necessary), how to ensure the transfer is secured, etc.
- **Customer experience.** Considerations could also incorporate how experience will be navigated by individuals across different sectors of the industry, for example technology, finance, energy. Perhaps customer experience guidelines could be drafted to set out best practices.
- **Timelines.** Outline a prescribed timeline for data transfer, such as the 30 days outlined under GDPR. This will help 1) manage consumer expectation, 2) support data holders to operationalise a process to process data portability requests and, 3) aid innovation, through providing clarity on the length of time data will take to be processed.

We would also like to use this opportunity to advocate for joining up this proposed data portability right with the existing Open Banking infrastructure in Singapore. We recommend the working group is formed to think through best way of operationalising the framework for all ecosystem participants in a way that is effective, secure and sustainable. We suggest that MCI work with the Monetary

Authority of Singapore ("MAS") to investigate whether the Open Banking framework and learnings could be leveraged as a base for data portability.

3.3 Marketing Messages to Instant Messaging ("IM") Accounts

The proposed changes to the SCA are also welcomed as they give clarity on which legislation is applicable to electronic messages sent to IM accounts.

Under the PDPA, an individual can provide express, specific consent to receive marketing messages via telephone and / or email. American Express currently has a well-established process to manage consent to receive marketing messages obtained from our customers, whereby customers can indicate if they wish to receive marketing communication via SMS or email. Where such consent has already been obtained from the individual, may we clarify if organizations can continue to rely on this consent to send marketing messages to such individuals via their respective IM accounts, where such IM accounts are tied to a phone number? This would greatly benefit our operational efficiencies and costs to rely on existing consent (with appropriate disclosures to our customers) instead of building a new system to capture new consent.

3.4 Obligation and Liability on Third-Party Checkers:

Under Section 24 of the Bill, we note that PDPC will impose the obligation and liability on third-party checkers to accurately check against the Do Not Call ("DNC") Registry and communicate the results accordingly to organisations. With these amendments, the liability will be imposed on the checkers for any erroneous information provided by them to organisations, who would be deemed to have already complied with its duty to check the DNC Registry once informed by the checker.

However, we note that under the Guidelines on Outsourcing ("Outsourcing Guidelines") issued by MAS, any outsourcing activities by financial institutions do not diminish their obligations to comply with relevant laws and regulations in Singapore.

May we obtain further clarification on the application of Section 24 of the Bill, in respect of the requirements of the Outsourcing Guidelines? More specifically, will organisations who outsource the activity of checking against the DNC Registry, continue to be ultimately responsible for ensuring the accuracy of checks performed by third-party checkers, as required by the Outsourcing Guidelines?

3.5 "Derived Personal Data" Exemptions

Section 2 of the Bill broadly defines derived personal data to be "personal data about an individual that is derived by an organisation in the course of business from other personal data about the individual or another individual in the possession or under the control of the organisation". Under the Bill, it was also proposed that derived personal data will be exempted from the application of the Correction and Data Portability Obligations. However, under the Access requirements of the PDPA, organisations will still be required to provide individuals with information on the ways in which their derived personal data have been or may have been used or disclosed by the organisation, upon request.

In the current business environment where big data and data analytics are widely used by organisations, extracting and retrieving the derived personal data, as defined in the Bill, can be vastly expensive and challenging to organizations in order to comply with the Access requirements of the PDPA. On this note, will MCI/ PDPC provide further clarifications on the definition of a derived personal data, such as providing specific categories of derived personal data that will be in-scope of this requirement? Furthermore, will anonymized data and aggregated data also fall under the definition of derived personal data?

4. Conclusion:

American Express would like to thank the MCI and the PDPC for the opportunity to participate in this public consultation and we look forward to receiving further clarifications on the above points.