From: Loo, Irene
To: MCI DataRegulation (MCI
Subject: Public Consultation for the PDP (Amendment) Bill

PART II: STRENGTHENING ACCOUNTABILITY

<u>Mandatory data breach notification requirement</u>

i. Noted the intent to have "credit card numbers" prescribed in Regulations categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals, and therefore, subject to the mandatory breach notification.

   We would like to put forth that credit card numbers – on its own – would not allow for an individual to be identified, and would not be considered "personal data" as defined in the current version of PDPA. The risk of fraud based on credit card numbers alone is also limited. For cards not in present transaction, additional details such as card expiry date, card verification value and One-Time-Pin authentication (in some instances) is required to complete the transaction.

   Protection over individual consumer interest is well established by the various regulations issued by MAS – including but not limited to ePayment User Protection Guidelines, TRM Guidelines. Further, consumers are protected against fraud by the Dispute Resolution process under the Association (Visa/MasterCard) Rules.

   In addition, Issuing Banks have established measures in place to protect individuals customers which include blocking and reissuing cards.

   Given the above, would put forth that given the adequate and multi-layered stablished regulatory/industry oversight for credit cards to prevent significant harm to individuals, mandatory breach notification to PDPC will not be required just for "credit card numbers".

   In addition, there are corporate cards without personal liability, hence any risk of harm (in relation to data breach of credit card numbers) is not on the individual.

ii. On the requirement to contact individuals of the data breach. For corporate cards, our bank's usual direct contact would be with the corporations rather than the individual cardholders. We would to clarify if data breaches can be notified to the corporate clients instead as our corporate clients are able to reach out to/contact the individual cardholders. We would also request that in a joint account situation or supplementary card situation, that PDPC allow the bank to communicate to impacted accountholders according to its customary method or as provided in the account terms and conditions

e.g. if the bank account terms and conditions provide that notification to any accountholder is treated as a notification to all accountholders.

iii. We note that the organisation must notify all affected individuals as soon as practicable upon determining that a data breach meets the criteria for notifying affected individuals, but at the same time, organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. As affected individuals may already have been notified before PDPC directs the organisations not to (and may need some time to stop the outreach effort), would request if PDPC can provide further clarity in the relevant Guidelines. We also request the PDPC to clarify whether it is sufficient for a regulated entity like a bank to notify its primary regulator about a data breach or is the expectation that the organization should inform PDPC as well.

iv. Would request PDPC to provide in the Guidelines or Guides, some examples where it is deemed acceptable for organisations to apply remedial action exception, in not notifying affected individuals of a data breach.

PART III: ENABLING MEANINGFUL CONSENT

Enhanced framework for collection, use and disclosure of personal data

i. The new Section s15(4) imports the concept of "reasonable necessity". In particular, an individual (P) who enters into a contract with an organisation (A) and provides personal data to A is deemed to consent to:

(a) A's disclosure of the personal data to another organisation (B) is deemed, where the disclosure is "reasonably necessary", for the performance of a contract between P and A;
(b) the collection and use of that personal data by B, where the collection and use are "reasonably necessary" for any purpose mentioned in paragraph (a);
(c) the disclosure of that personal data by B to another organisation where the disclosure is "reasonably necessary" for any purpose mentioned in paragraph (a).

Whilst we note that the concept of "reasonable necessity" must have a nexus with the purposes of the contract with P, or where the contract is in P's interest, we welcome further clarification on its meaning and application in the Act, updated Regulations and/or new Guidelines. Where global businesses are concerned, it is often necessary to rely on outsourced service providers and specialist services to benefit from economies of scale and leverage international best practices. It is respectfully submitted that the concept should be wide enough to embrace the example described as various value/supply chain partners essential to in the performance of the contract.

ii. For the Business improvement exceptions scenarios listed in para 40b) of the Consultation paper, would request if the additional three scenarios (iv to vi) can be considered for inclusion:

This new exception is intended to make clear that organizations may use personal data (that was collected in accordance with the DP Provisions) without consent for the following business improvement purposes:

(i) operational efficiency and service improvements;
(ii) developing or enhancing products/services;
(iii) knowing the organization's customers.
(iv) Finding the most appropriate customer - Product match
(v) Marketing the most appropriate products, which the customers will have highest propensity to acquire
(vi) Sharing data and analysis with trusted partners in order to offer personalized products, services, rewards, discounts and privileges

iii. On the same the Business improvement exception.We welcome that the intended policy position that this exception would apply to a group of companies (e.g. subsidiaries of the organisation). Would like to seek clarification if the use of the exception is intended to exclude the transferring party from the Transfer Limitation Obligation when the receiving party (who belongs to the same group of companies) is not based in Singapore.

PART IV: INCREASING CONSUMER AUTONOMY

Data Portability Obligation

We note that additional requirements will be prescribed for data porting requests and transmissions of personal data thereunder. It would be helpful if the Act, updated Regulations and/or new Guidelines could provide for, or clarify, the following:

(a) A porting organisation shall have no legal liability to the receiving organisation for the personal data. This is because (i) there is no contractual nexus between the parties, and (ii) an organisation that collects and uses personal data assumes responsibility for the personal data, including verification of the personal data and having to comply with the Accuracy Obligation under the PDPA.

(b) Similar to the Access Obligation and PDPC's current advisory guidelines on individual's access to their personal data, would request PDPC to provide the necessary clarification that the transmitting organization reserves the right to reject a porting request "if the request is otherwise frivolous or vexatious". A limit to the number of times that an individual can request for portability of his/her personal data. In the absence of any limitation, it becomes a burden to the same porting organisation, and creates a risk of exploitation by individuals to rely on the same modus and party to demonstrate the legal standing, credit worthiness, reputation/social standing, etc., of the individual (especially where the porting organisation is operating in a regulated industry, eg. finance, and would have more stringent checks).

(c) A receiving organisation shall have a right to refuse the ported data. This is because the receiving organisation remains responsible for complying with the requirements under the PDPA when collecting personal data, including verification of consent or such other legitimate purposes and ensuring accuracy of the personal data from the relevant individual.

PART VI: OTHERS

Transitional Provisions and Sunrise Period

In light of the efforts that will be needed to update internal processes and comply with the new and significant requirements, we would recommend that the Act expressly provide for transitional provisions where the changes act can be implemented in phases. For example:

> Phase 1: Updated Do-Not-Call Provisions and New Data Portability Provisions will be effective 6 months from date the Amendment Act is passed in Parliament
>
> Phase 2: New Provisions requiring mandatory Data Protection Impact Assessments for Use of Personal Data, e.g. (i) Updated Deemed Consent Provisions and (ii) Legitimate Interests Exceptions will be effective 12 months from date the Amendment Act is passed in Parliament.
>
> Phase 3: New Breach Notification Provisions will be effective 18 months from date the Amendment Act is passed in Parliament.

The transition and sunrise period would also be helpful (i) to allow individuals and organisations to be educated on the new rights and obligations, and (ii) to allow organisations to regularize their existing contracts with data intermediaries to account for the new changes.