Banks' Feedback on the PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

Bank Name	Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent? Page 8
A	Yes. The current framework requiring consent for the collection, use and disclosure of personal data poses constraints to new business opportunities that our organisation may want to explore. The current framework also poses constraints in areas of data collaboration and sharing of anonymized data with existing or future partners. As a business, we constantly seek new partners for data collaboration and sharing of data for the purpose of understanding general trends. In such situations, it is not practical to seek consent from each customer for every new engagement of partners. We note the proposals recognise the sharing of anonymised data to be legitimate, but this is not sufficient for accurate insights. There must be a greater ability to harness customer data to allow for organisations to gain deeper insights into what products are relevant. Having overly prescriptive or restrictive data protection frameworks can stand in the way of making headway in a global market. The Economist has recently observed that China is likely to emerge the world leader in AI technology, precisely because of the deep pool of data that it has, and how it is not shackled by privacy laws: "What really sets China apart is that it has more internet users than any other country: about 730m. Almost all go online from smartphones, which generate far more valuable data than desktop computers, chiefly because they contain sensors and are carried around. … Chinese do not seem to be terribly concerned about privacy, which makes collecting data easier. The country's bikesharing services, which have taken big cities by storm, for example, not only provide cheap transport but are what is known as a "data play". When riders hire a bicycle, some firms keep track of renters' movements using a GPS device attached to the bike." (See https://www.economist.com/news/business/21725018-its-deep-pool-data-may-let-it-lead-artificial-intelligence-china-may-match-or-beat-america). Requiring consent will limit the ability of the bank and Singapore generally to embrace its own existing data sets and to restrict innovation. We foresee that such scenarios will increase especially as the Smart City & Internet of Things ("IoT") initiatives increase and devices related data becomes increasingly available. With sensor based IoT data becoming increasingly prevalent, we expect situations where data will be captured from devices and fed to the bank. This information may: 1. be anonymous (i.e. does not identify the device and the end user); 2. identify the device (but not the customer); or 3. identify the actual end user. Notification of Purpose approach will be necessary for such situations as we may not be able to contact the end user, particularly in situations when only the device id is known. A Notification of Purpose approach is good as it provides more flexibility to the business while at the same time, safeguarding the interests of consumers. However, to provide flexibility to organisations (especially financial institutions) to conduct their business in a meaningful way, the law needs to ensure that it does not impose further conditions that may minimise the effectiveness of the Notification of Purpose approach. The present proposals do not go far enough in giving companies more latitude in mining their data. For instance, we note that the Consultation Paper provides for certain conditions to the Notification of Purpose approach which in our view may hamper the effectiveness of approach. Please see our response to Question 2 for a more detailed discussion of our view.
B	Yes, in addition, there should be provisions to allow organisations to provide Notification of Purposes "post" personal data collection as there may be situations where notification may not be feasible before or at the point of data collection.
C	This is a welcome initiative as the Notification Approach will allow banks to provide products and services which were previously not introduced to the market but are becoming available because of developments such as innovation, industry changes, Fintech partnerships. The Notification Approach means that the Bank can offer such products and services to its customers (which are in most cases genuinely beneficial to the customer without incurring significant privacy risks) without undertaking the onerous exercise of seeking specific consent each time (consent would have been obtained from the customer at time of account opening and it would not be feasible to draft the consent language so broadly to cover all such situations). In some situations, where a data privacy impact assessment indicates that the privacy risks arising from the collection, use and disclosure of personal data for a particular purpose is minimal, it may be too onerous to obtain clear and unambiguous consent from individuals.
D	Yes, that would provide more flexibility to the collection, use and disclosure of data. However, guidelines should be in place to provide further clarity on the terms "impractical" and "adverse impact" when the notification method is utilized.
E	Yes. More guidance is required on the level of detail that would be expected for an "appropriate notification" and examples of what PDPC considers "appropriate notification". Would a general notification on the bank's website suffice? Where someone leaves a positive feedback on social media and the company would like to quote the comments as a marketing/training tool, it would not be practical to obtain the individual's written consent. Can the bank make use of the Notification Approach to inform posters that the bank will be using his/her comments for marketing/training purposes?

F	We welcome the approach mentioned in the Consultation. While customer consent is generally obtained at the point of on-boarding for a variety of purposes, from time to time, the organisation does come across scenarios (example- usage of personal data for new technology usage) that involves collection, use or disclosure of personal data for purposes which may not have been obtained at the point of account opening. In such circumstances, it becomes impractical or onerous for the bank to seek customer's consent and may result in a less than optimal experience for the end user. We would also seek PDPC guidance in providing additional scenarios where Notification approach will generally be appropriate to be used.

Bank Name	**Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)? Page 8**
A	(a) Firstly, we query whether there is a need for the proposed conditions at all. For instance, the Consultation Paper proposes that organisations may only rely on the Notification of Purpose approach if, among others, it is "impractical" for the organisation to obtain consent and the collection, use or disclosure of the personal data is not expected to have any "adverse impact" to the individuals. It is unclear what the terms "impractical" or "is not expect to have any adverse impact to the individuals" mean. Does the term "impractical" cover only the limited situation where organisations do not have the latest contact details of its customers? In the Guideline to Data Sharing released concurrently with the consultation, the term "impractical" is also referenced as a criteria for a data sharing exemption ("DSA") application, but the examples provided are very narrow (eg. to prevent fraud in situations where the perpetrators of the fraud will not provide consent) and do not demonstrate clearly when the impracticality trigger may apply in more general commercially relevant scenarios. We are of the view that such restrictive or limited conditions would hamper the effectiveness of the Notification of Purpose approach. For example, we can envisage that in practice, the size of the data pool being too large will pose genuine difficulties to contacting each individual and be too onerous a task. Our experience has also been that response rates to direct outreach via mail or email can be very poor. The Commission should therefore provide clarity as to the test for "impracticality" eg. that cost or resources for securing consent is disproportionate to any harm or impact to the individual. In relation to the term "adverse impact", we note that PDPC has under para 3.8(b) of the Consultation Paper provided the example that organisations are to ensure that the personal data will not be used to, among others, circumvent a prior withdrawal of consent (e.g. target the individual for direct marketing after he had opted out of receiving marketing communications). Could PDPC clarify how this will tie in with the Notification of Purpose approach? Since the enactment of the PDPA, some customers would have withdrawn their marketing consent. In relation to the above example being cited, does this mean that the Notification of Purpose approach cannot be used on customers who have withdrawn their marketing consent? If so, we are of the view that this will defeat the purpose of the proposed Notification of Purpose approach and it does not cater for the needs of the banks. We therefore propose that the proposed conditions be dropped. Further, we note that the Consultation Paper provides that organisations are required to conduct a data protection impact assessment ("DPIA") when relying on the Notification of Purpose approach. With the DPIA being conducted, why would there be a need to subject organisations such as banks or financial institutions to the proposed conditions since proper risk assessments would have been done by the organisations? Accordingly, we strongly suggest that if a DPIA is done, organisations should not be required to satisfy the proposed conditions so long as the DPIA establishes that the proposed use does not pose a significant impact to any individual. If the PDPC is concerned about safeguards against completely subjective assessments, this is already addressed in the PDPA since there is an overarching concept of reasonableness – which then addresses the risk of DPIA conclusions which are not reasonable as to their conclusions. We have set out a list of practical scenarios in Annex A in which organisations should be able to rely on the Notification of Purpose approach without the need of having to satisfy the proposed conditions. In light of the above, for the DPIA to work effectively, it would be helpful if organisations are provided with guidelines for such assessments. In addition, such guidelines will ensure that the assessments performed will be consistent across industries and organisations. (b) However, if conditions are imposed on the Notification of Purpose approach, such conditions have to be clear, unambiguous, well defined and does not unnecessarily hamper the business needs of organisations. It would be helpful to be provided with guidelines to the Notification of Purpose approach. As it stands, the proposed two conditions (i.e. impractical to obtain consent and no adverse impact) on the Notification of Purpose approach is overly stringent. If one of the proposed two conditions needs to be met, the requirement for the Notification of Purpose approach will be less stringent. (c) In addition to the "proposed Notification of Purpose" approach, we also propose an "opt out" regime whereby customers should be treated as having given consent unless they have specifically informed us that they wish to opt-out. (d) The Notification of Purpose approach should be applicable to organisations conducting research and data analysis. For such activities, there should not be an "opt out" option nor should the law impose any conditions on organisations. We should not need to provide an "opt-out" option because at the end of the day, insights obtained would be for the betterment of customers and the organisation. By providing an "opt-out" option, data integrity may be affected and the products/services provided may not be up to standard. (e) Lastly, we are of the view that proper guidelines must be provided on the appropriate and/or acceptable channels of notifying individuals of the purpose. Other than the traditional modes of communications such as written notice (which should include letters by post and e-mails) and verbal communications, it should be made clear that notification via organisations' website is deemed as sufficient notice.

B	1) Propose that Data Protection Impact Assessment (DPIA) need not be performed every time an organisation would like to use the Legal or Business Purposes Exception. A risk-based approach to be taken. 2) We are very supportive of this approach. However, we would like to understand if there will be a "grandfathering" approach (for existing products and services) for us to perform notification without having to perform DPIA.
C	While it may be convenient for organizations if this new framework came without conditions, that would likely open up avenues for abuse and potentially result in a high number of customer complaints. Some conditions that this framework would be subjected to may include the risk of harm arising to individuals from a specific purpose of use of personal data, the practicality of asking for consent, whether the purpose of use of data is reasonably expected to benefit the individuals. The PDPC should provide some guidance on acceptable means of notification, as this is an important distinction for organizations with a large body of individual customers. While the bank can take reasonable steps to ensure that all customers have been notified, some individuals may not receive such notification because of simply reasons like the individual not checking their mail/email. In such circumstances, the organization's responsibility should be limited to taking reasonable steps to notify the individual.
D	Yes, however guidelines should be in place to provide further clarity on the terms "impractical" and "adverse impact" when the notification method is utilized.
E	Noted that an opt out must be made available "where feasible". There would be very few situations where an opt out is not technically feasible. What level of cost and difficulty of effort would make the option not feasible? The effectiveness of the DPIA (Data Protection Impact Assessment) is subject to the risk appetite of the organisation collecting the data. An individual's personal data could be used differently depending on the assessment of the collecting organisation. There is a need to build public awareness of this subjectivity, and set out principles or a baseline on how a DPIA should be conducted. We would also appreciate more information on PDPC's expectations regarding monitoring of the DPIA – will individuals be permitted to ask for a copy? If so, access should be limited to the data subject, and the organization should be permitted to produce a summary rather than its full analysis (which is confidential business information). Where someone leaves a positive feedback on social media and the company would like to quote the comments as a marketing/training tool, it would not be practical to obtain the individual's written consent. Can we make use of the Notification Approach to inform posters that the company will be using his/her comments for marketing/training purposes?
F	The organisation shall conduct the Data Protection Impact Assessment ("DPIA") and will also notify the individuals on various methods of opt-out where the opt-out options are feasible. We would suggest that the individual be given a reasonable period to facilitate opt-out and in the event the individual does not notify the bank; we can use the data for the notified purpose(s). The bank seeks clarity on what are the parameters that would be considered as "an adverse impact".

Bank Name	**Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification? Page 10**
A	Yes, but we question the need for the proposed conditions (our comments on the proposed conditions are set out in our response to Question 4 below). Also, it will be helpful if clear and practical guidelines as to what constitutes "business purpose" is provided. For instance, would PDPC consider the sharing of personal data among different organisations across different industries (e.g. Banking, Telecommunications, Properties and F&B) for the purposes of understanding consumer behaviour, product trends and insights constitute a valid business purpose exception? With the government encouraging data sharing in the move towards "Big Data", PDPC may wish to consider allowing for expressed exceptions to address such data sharing situations.
B	In addition to "Business Purposes", propose to include additional explicit conditions such as the collection, use and disclosure of Personal Data for "Risk Management" purposes (e.g Sanction, Counter Terrorists Financing/ Anti-Money Laundering) where the collection, use and disclosure of Personal Data is clearly in the interest of the individual and/or society.
C	The bank is very supportive of the Legal or Business Purposes Exception, as this balances the interests of the bank against the need for privacy of the individual. However, while Legal purposes are generally clear, the concept of Business Purposes comes with some ambiguity, so there should be additional guidance from the PDPC or agreements between industry participants on what such business purposes would be for a particular sector. It is important to note however, that what may seem reasonable to the organizations may not seem reasonable to each and every customer. There are other circumstances, such as offering certain products/discounts/promotions to customers who may be in need of that service/promotion or may have an interest in the promotion, however the bank may not be able to provide this to the customer due to the customer opting out of such offers from the bank. An example may include offering products with lower interest rates to customers who are currently already in debt to the bank and paying a higher interest rate. There may be examples where the bank is trying to promote a certain channel (e.g. online banking) and hence offering vouchers and promo codes to customers; however the bank is unable to inform certain group of customers about such offers as they would have opted out of receiving such information.

D	Yes, we are supportive as there are valid reasons / purposes for the processing of data without consent and notification.
E	Yes.
F	The bank welcomes the decision of collecting, using and disclosing personal data for Legal & Business reasons. Apart from the 2 conditions stated in 3.15 a) and b) we would also propose an additional condition: that the interest of the organisation are not overridden by the interest of the individual. Additionally, we seek clarity on whether sharing personal data to meet requirements of foreign laws/regulations, as well as cross border transfer of data would be covered in the Legal & Business reasons.

Bank Name	**Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)? Page 10**
A	Under the Consultation Paper, the proposed Legal or Business Purpose would be subject to the proposed conditions (i.e. not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual). Similar to our comments to Question 2 above, we are of the view that many organisations may find it particularly hard to determine the meaning of "not desirable or appropriate to obtain consent" and "benefits to the public clearly outweigh any adverse impact or risks to the individual". Further if there is a Legal Purpose, we query whether there should be a need for organisations to satisfy the proposed conditions and also conduct risk assessments? We are of the view that if an organisation determines that there is a legal purpose, there should not be a need for such organisation to satisfy the proposed conditions or conduct risk assessments. As for Business Purposes, rather than relying on the proposed conditions, we are of the view that the carrying out of a risk assessment is sufficient. Again, we note that PDPC has proposed that a DPIA be conducted. If DPIA is done, we are of the view that the proposed conditions should not be relevant. For a more detailed discussion of our comments on the DPIA, please refer to our response to Question 2 above.
B	Propose that Data Protection Impact Assessment (DPIA) need not be performed every time an organisation would like to use the Legal or Business Purposes Exception. A risk-based approach to be taken.
C	While it may be convenient for organizations if this new framework came without conditions, that would likely open up avenues for abuse and potentially result in a high number of customer complaints. Some conditions that this framework would be subjected to may include the risk of harm arising to individuals from a specific purpose of use of personal data, the practicality of asking for consent, whether the purpose of use of data is reasonably expected to benefit the individuals, **whether the business interest is fairly weighed against any potential privacy impact to the individuals involved**. **Other comments pertaining to the proposed alternatives to Consent** The PDPC should provide some guidance on acceptable means of notification, as this is an important distinction for organizations with a large body of individual customers. While the bank can take reasonable steps to ensure that all customers have been notified, some individuals may not receive such notification because of simply reasons like the individual not checking their mail/email. In such circumstances, the organization's responsibility should be limited to taking reasonable steps to notify the individual. The PDPC should also specify a framework for a data protection impact assessment ("DPIA"), otherwise there will be a lot left to interpretation. Would sales and marketing of certain products/services that an organization deems to have an overriding benefit to individuals, be considered an acceptable use of the business purposes exception? If yes, would this notification approach be extended to the DNC requirements as well (i.e. a bank could rely on the notification approach to existing customers to market certain products to them without checking whether these customers have listed their Singapore telephone numbers on the DNC registry).
D	Guidance on DPIA should be provided on the risk acceptance level and whether supervisory approval should / could be sought where residual risk assessment is rated high / very high.

E	Clarity on the conditions would be helpful in assessing how this basis can be applied. Guidance is needed on what be a "benefit" to the public, what constitutes an "adverse impact" to the individual". Can the development of better services or targeted marketing tools be considered a "benefit to the public"? Does "necessary" for a legal or business purpose include compliance with industry best practices or assistance to a foreign regulator although there is no binding legal requirement? Greater clarity on what is a "legal or business purpose" would be helpful.
F	The bank seeks clarity on what will be considered not desirable or appropriate.

Bank Name	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? Page 14
A	The current voluntary data breach notification should continue and banks should be allowed to continue making their own assessment on when to notify individuals and the relevant authorities. This is because the definition of "risk of impact or harm" may vary from organisation to organisation. Further, the Consultation Paper has given some examples on the types of breaches that will constitute "risk of impact or harm". These examples include NRIC number, health information, financial information and passwords. Some of these terms are too wide. For instance, for "financial information", would an inadvertent disclosure that a customer has used S$5 in his account amount to a "risk of impact or harm"? Although S$5 can be considered as "financial information", it is unlikely that such disclosure may cause material or significant "risk of impact or harm" to an individual. The words "risk of impact or harm" is a broad term which is likely to create an obligation on organisations to notify both PDPC and individuals about any and all breaches. To this, we note that PDPC has stated in Para 6.1 of the Consultation Paper that "PDPC is mindful not to impose overly onerous regulatory burdens on businesses in Singapore, or to create notification fatigue for individuals". When any notification is made mandatory and organisations are left to assess when to notify, especially with vague and loose terms like "risk of impact or harm", there is a very high possibility that many organisations will "err on the side of caution" and overly notify. This may indirectly impose burdens on businesses and customers may also be unnecessarily alarmed by the sudden increase of notifications, of which some may not be significant or real. As mentioned above, we are of the view that the current voluntary data breach notification should be retained and banks should be allowed to continue making their own assessment as to when to notify the individuals and the relevant authorities. If PDPC is of the view that such breach notification has to be imposed, we would propose that there be a materiality test imposed before the obligation to notify arises, rather than on account of the information falling within broad categories such as "financial information". In assessing materiality, both the potential adverse impact and the scale of the disclosure can be taken into account, again coupled with the test of reasonableness as discussed above, if the PDPC is concerned about there being too much subjectivity in such assessments. As such, if for example a document containing personal data (eg. a bank deposit slip) has been disclosed and that disclosure either does not pose material risk, or the document (eg. a share certificate) has been successfully retrieved from a single disclose, there should not be a need for a breach notification to be filed (whether to the PDPC or otherwise). Obligations of Data Intermediary We would like to clarify on the definition of Data Intermediary ("DI") (as per footnote 37). Could PDPC provide some clearer guidelines as to what constitute a DI? We ask this because in practice, determining whether a party in fact acts as a DI can be very difficult, particularly in the financial sector. For example, where a clearing house function or payment intermediary such as NETS is involved in a transaction, does it act on its own account, or as a data intermediary? The problem will be more acute with the increasing embrace of fintech solutions. For example, non financial institutions are now offering payment related services (eg. Google Android Pay, ApplePay, Samsung Pay), as well as card issuers (Mastercard now offers a Masterpass payment service). These service providers will often retain absolute control over their technology and platforms, yet could seek in a data breach situation to characterise themselves as a data intermediary processing payments on behalf of the card issuing bank. The UK ICO has recognised that the classification of data processors can raise difficult issues, as has the European Art 29 Working Party. Both have issued guidelines acknowledging the difficulties associated with such classification in some cases, but have nonetheless provided some clarity on guidelines for assessment. We note that the Consultation Paper proposes that a "DI" must inform the organisations immediately when a data breach occurs. Rather than imposing that DI must inform organisations immediately when a data breach occurs, we are of the view that such requirements should be left to organisations to negotiate with DI under the agreement governing their relationship.
B	Instead of a definite threshold (ie. 500), propose to include additional dimension such as a % of the total count of individuals within the specific part of the business, (e.g XX % of total credit card holders in the bank).

C	This new requirement may be onerous for organizations unless the reporting is required to be done based on very objective criteria that are easy to apply across different types of organizations. Otherwise, different standards may be followed across different organizations and industries. While 500 is a reasonable number, looking at numbers alone may not make sense for all types of data breaches. For example, unauthorized access of a 1000 customer email addresses may not be pose as much of a threat as the loss of 100 application forms that may include detailed demographic data, employment data, etc. Our suggestion would be to have some guidance based on absolute numbers, but also allow organizations to assess the risks involved before making the notification.
E	Significant scale of breach needs to be examined relative to the type of organisation, size of the customer base, type of breach, scale of breach etc. It is difficult to pin a number that applies across industry sectors and organisations of different sizes. For instance, 500 data sets may constitute only a small percentage of a large corporation's database whereas it would be substantial to a small entity. Instead of specifying a minimum number, PDPC can consider defining in terms of percentage, or developing a set of severity guidelines upon which the organisations can conduct their risk assessment with respect to severity of the breach. We look forward to guidance on the content of the notification to the individual. What rights should the individual have to additional information? Can the data subject insist on documentary evidence of how the breach occurred, names of the staff involved, etc? This should be left to the discretion of the bank, and the existing legal discovery process. Further guidance on "any risk of impact or harm" would be helpful. We note that the closed consultation referred to "significant risk of harm" which we submit is more meaningful. We respectfully submit that significance and likelihood of harm should be a consideration.
F	We would propose that the number of affected individual's criteria should be determined by the size of the organisation and the client base rather than a fixed number i.e. 500 to be applicable across industries. As such, we propose that determination of significant scale be left to the organisation's discretion. Additionally, instead of using "significant scale of breach", we propose to replace with "breach with severe and widespread impact" to convey similar expectation on the scale of the breach.

Bank Name	**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? Page 15**
A	For banks, the proposed concurrent application with Other Laws and Sectoral Breach Notification should only be limited to the situation where there is a data breach involving personal data **and** a breach of the Banking Secrecy.
B	For Banks, we have to report to (a) MAS, (b) PDPC, and potentially (c) Cyber Security Agency (CSA) for the same data breach incident. Suggest that there is an agreement within the different statutory bodies that a 'common' breach reporting template be used, regardless who the reporting is made to. Or an agreement that the reporting template to MAS (as host sectorial regulatory) is acceptable by both PDPC and CSA.
C	The reporting requirement for financial instituations regulated by the MAS should be aligned such that such FIs do not need to prepare 2 set of reports for 2 regulators with similar content but different formatting requirements. If possible, such requirements should be standardized within the industry, such that the reporting requirement and format do not vary greatly within the industry.
D	Agree that a standardized (initial and final) reporting process to regulatory entities would enable to streamline and focus resources on handling / investigating the data breaches incidents.
E	The proposals are reasonable.

Bank Name	Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements? Page 16
A	Could PDPC clarify whether Para 6.10(a) **AND** Para 6.10(b) must be fully satisfied for the exception to apply? We propose adding the exception where organisations will perform a risk assessment to determine the level of "risk of impact or harm" to individuals. In the event that organisations assess such levels of risk to be low, organisations will be exempted from the breach notification requirements. Para 6.10(b) states: “technological protection exception, where the breached personal data is encrypted to a reasonable standard”. Could PDPC clarify what is considered a “reasonable standard” of encryption?
B	1) Proposed to have another exemption whereby “notification to affected individuals may increase the risk of further detrimental impact to the affected individuals”. 2) Proposed to have another exemption whereby “notification to affected individuals may not be required with valid business justification that is agreed by PDPC.”
C	We seek clarification on whether this notification requirement extends to internal lapses where data is inadvertently disclosed to internal affiliates. We would point out that employees of the bank are subject to confidentiality requirements and therefore, suggest that the requirement for data breach notification should be limited to external breaches involving 3rd parties. Our ask here is that as long as the data is within the bank/organization’s protected environment, a notification should not be required, simply because another employee, who does not have a need to access the data, at a different branch of the organization (which may be operating under a different legal vehicle) has accessed the data.
E	We support the law enforcement exception and the technological protection exception. We ask PDPC to consider an additional exemption for accidental disclosures to a third party who can be identified and who is willing to give a written confirmation that he has not used or further disclosed the data that was inadvertently disclosed. There should not be an obligation to notify where the individual is already aware eg. disclosure was inadvertently addressed to both the individual and another party, or made in the presence of the individual.

Bank Name	Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC? Page 17
A	72 hours may not provide sufficient time for meaningful findings. We propose a time frame of 7 business days (excluding Saturdays, Sundays, bank or public holidays). Should an organisation require more time, it should be given the right to engage PDPC directly and request for an extension of the time frame.
B	Proposed to be explicit that 72 hours refers to "Singapore business hours", ie. exclude non-working days (weekends, public holidays).
C	72 hours notification to PDPC might seem reasonable but we have to be mindful of long holidays/weekends. We suggest 3 business days from the point of management escalation or breach determination instead. Furthermore, we suggest that this 72 hour period starts at the point in time when the organization has conclusively confirmed that there was a data breach. There are various scenarios where confirming that there was unauthorized access requires time, and making a notification to the PDPC and the individuals without such a confirmation, may result in unnecessary panic and higher volumes of notifications, many of which may have to be rescinded at a later time. Other comments pertaining to data breach notification Data Intermediaries Would organizations be required to sign agreements with data intermediaries within and outside of Singapore, to ensure that the data intermediary immediately provides data breach notifications to organizations? In the event that a data intermediary does not notify an organization about a data breach immediately, and as a result, the organization is unable to notify the PDPC and/or affected individuals within the stipulated timelines, will the organization be held responsible for being unable to meet the proposed notification requirements under the PDPA? Technological Protection Exception The PDPC should define specific encryption, hashing or anonymization techniques and processes that organizations must follow in order to rely on the technological protection exception, otherwise this may be left to interpretation. Contact Details Most banks will have customer service channels that are generally used for all customer communications and interactions. In the event of a data breach, we propose to use such customer service channels (such as a customer service email or a customer service hotline), instead of a DPO contact. This is especially important when the volumes are high.
D	To seek clarification on the requirement of providing information for breach notification. If the organization does not have sufficient information to the (potential) data breach within 72 hours, would a simple notification on the possibility of data breach (as the data leakage may not be personal data and / or encrypted anonymised data) fufill this proposed time frame requirement?
E	No comments.
F	While we welcome the proposal to inform the affected individual on the data breaches, we would propose the requirement proposed by the PDPC to notify affected individuals "as soon as practicable" to be replaced by "as soon as reasonable". This is because the organisation would require sufficient time and resources to manage the impacted individual's queries and expectations amid handling other matters in relation to the breaches.

ABS' collation dated 28 September 2017