CODE OF BANKING PRACTICES –
THE PERSONAL DATA PROTECTION ACT ("PDPA")

This Code of Banking Practices ("**Code**") clarifies the practices for banks in Singapore in respect of the PDPA and its regulations, where applicable.

As part of the banks' commitment to treat their customers fairly and reasonably, persons who provide their personal data to banks should be assured that their information will be collected, used and disclosed in accordance with the high standards set by the Monetary Authority of Singapore ("**MAS**") and the Personal Data Protection Commission ("**PDPC**").

Following the amendments to the PDPA which will take effect in phases from 1 February 2021, this Code has been revised to reflect the updated practices for banks in Singapore. We hope that this revised Code will foster a better understanding of what you as an individual can reasonably expect from your bank concerning your personal data.

Mrs Ong-Ang Ai Boon
Director
The Association of Banks in Singapore

Contents

CODE OF BANKING PRACTICES – PDPA

Background

The PDPA 2012 governs the collection, use and disclosure of the personal data of individuals and establishes the Do Not Call ("**DNC**") Registry.

The PDPA provides a baseline standard of protection for personal data in Singapore. It complements sector-specific legislative and regulatory frameworks. For banks in Singapore, this would be Banking Act (Cap 19).

The PDPA contains 2 main sets of provisions, covering:

- the Data Protection Provisions in Parts III to VIA of the PDPA ("DP Provisions"); and
- the DNC provisions in Part IX and IXA of the PDPA ("DNC Provisions").

1. PURPOSE & SCOPE

a. This Code aims to provide information on how the PDPA may apply to the unique circumstances faced by the banking sector and its customers.

b. Banks in Singapore are already regulated on the disclosure of customer information by the MAS through statutes, regulations, directives, and notices (''Banking Regulations''). To the extent there are inconsistencies between the provisions of these Banking Regulations and the PDPA, the provisions of such Banking Regulations shall prevail.

c. In applying this Code, it should be borne in mind that Section 11(1) of the PDPA provides that "In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances." Banks are to consider what is reasonably appropriate and it is important for their customers to understand what this means to them and their personal data.

d. Please note that this Code does not amount to any advice, whether legal or otherwise, and is not legally binding on ABS or its members. It does not modify or supplement in any way the legal effect or interpretation of the PDPA and any subsidiary legislation (such as rules and regulations), and should not be construed as limiting or restricting the PDPC in its interpretation, administration and enforcement of the PDPA.

2. DATA PROTECTION PROVISIONS

2.1 Overview of DP Obligations

The DP Provisions contain 10 main obligations which banks are required to comply with if they undertake activities relating to the collection, use or disclosure of your personal data. In the context of banks, these obligations are:

a. Consent - banks must obtain your consent unless an exception applies (see below) before collecting, using or disclosing your personal data for a permitted purpose.

b. Purpose Limitation – banks may collect, use or disclose your personal data only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to you.

c. Notification – banks must use appropriate means to notify you of the purpose(s) for which it intends to collect, use or disclose your personal data on or before such collection, use or disclosure of personal data (see below), where applicable.

d. Access and Correction – banks must, upon request, (i) provide you with access to your personal data which is under the banks' control or possession and information about the ways in which your personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in your personal data that is under the banks' control or possession.

e. Accuracy – banks must make reasonable effort to ensure that your personal data collected by or on behalf of the bank is accurate and complete if your personal data is likely to be used by the bank to make a decision that affects you or is disclosed by the bank to another organisation.

f. Protection – banks must protect your personal data under their control or possession by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

g. Retention Limitation – banks must cease to retain documents containing your personal data, or remove the means by which your personal data can be associated with you as soon as it is reasonable to assume that (i) the purpose for which your personal data was collected is no longer being served by retention of your personal data; and (ii) retention is no longer necessary for legal or business purposes. As each bank has its own specific business needs, the PDPA does not prescribe a specific retention period for personal data (see below).

h. Transfer Limitation – banks must not transfer your personal data to a country or jurisdiction outside Singapore except in accordance with the requirements prescribed under the PDPA.

i. Data Breach Notification –banks must assess whether a breach involving your personal data is notifiable and notify you and/or the PDPC where breach is assessed to be notifiable.

j. Accountability – banks must implement data protection policies and procedures to meet their obligations under the PDPA and shall make information about the policies and procedures publicly available.

2.2 Exceptions under the DP Provisions

a. The DP Provisions do not apply to Business Contact Information ("BCI"). BCI, as defined under section 2(1) of the PDPA, would include an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, unless it was provided by the individual solely for his personal purposes.

Example:
You, a sole proprietor, gave your business card to your bank so that they can contact you about their corporate banking services. The bank may use the contact information contained in the business card (including your personal handphone number, if it is listed on the business card as a business contact) without your consent as it falls within the definition of BCI.

b. The DP Provisions contain an exception for personal data which is publicly available. Banks may collect, use or disclose publicly available personal data without consent. "Publicly available" is defined in the PDPA to mean personal data that is generally available to the public, including personal data that can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public, or if any member of the public could obtain or access the data with few or no restrictions. For example, banks may collect information about directors of a company from ACRA which is a publicly available information source.

c. The DP Provisions also do not apply to non-targeted marketing activities where no personal data is used. Examples include generic advertisements not targeted at specific individuals which are placed at the bank's internet banking website, mobile banking site, telephony systems, self-service machines, and the stationery or receipts of the bank concerned.

2.3 Consent, Purpose Limitation and Notification Obligations

a. Banks may not collect, use or disclose your personal data unless –

   (i) you have given, or deemed to have given, your consent under the PDPA to the collection, use or disclosure of the personal data; or

   (ii) the collection, use or disclosure of the personal data without your consent is required or authorised under the PDPA or any other written law.

b. Consent for collecting, using and disclosing your personal data can be obtained in several ways. Consent that is obtained in writing or recorded in a manner that is accessible is referred to as 'express consent'. Such consent provides the clearest indication that an individual has consented to notified purposes of the collection, use or disclosure of his personal data.

c. Banks will notify you of the purposes for collecting your personal data, how it will be used, and to whom the personal data may be disclosed unless exempted under the PDPA or any other law. To achieve this, banks will notify you through appropriate means (e.g. through a statement or undertaking on a product application form and/or via their privacy statements/policies on their website), depending on the circumstances.

d. When specifying the purposes relating to collection and usage of your personal data, banks are not required to specify every activity which they may undertake, but are required to state the objectives or reasons relating to collecting and using your personal data.

e. If you have questions about the bank's collection, use or disclosure of your personal data, you may request that the bank provides you with the relevant business contact information who is able to answer your questions on behalf of the bank.

Example:

Bank ABC wishes to conduct a customer satisfaction survey. Bank ABC may specify in its data protection policy published on its website, that it would like to collect, use and disclose your personal data as necessary for the purpose of conducting and administering the survey (e.g. to contact you to participate in the survey).

Bank ABC need not specify activities relating to exactly how your personal data will be collected and stored by it for the purposes of the survey; for example, that survey responses will first be recorded by hand on physical forms by employees of Bank ABC and then subsequently transferred to an electronic database, etc.

Examples of the types of personal data which banks may collect from you for the purpose of providing you banking products and/or services include but are not limited to:

- Full name, NRIC and/or passport number;
- Contact information such as telephone number and mailing address;
- Employment information;
- Financial information;
- Investment portfolios; and
- Personal data of any family members, or beneficiaries relevant to the provision of banking products and services to you. (Please ensure that you obtain consent from such family members or beneficiaries before providing their personal data to the bank.)

f. Banks may not, as a condition of providing a product or service, require you to consent to the collection, use or disclosure of your personal data beyond what is reasonable to provide the product or service to you. What may be considered reasonable purposes may vary based on the circumstances of the collection, use or disclosure. In assessing what is reasonable, a possible step that a bank could take is to view the situation from your perspective and consider what you would think as fair.

Example:

You purchase a cashier's order from Bank ABC. ABC cannot require you to provide consent to receiving marketing materials by email as a condition of providing the cashier's order, as it is beyond what is reasonable for the provision of the service.

g. Banks may not obtain consent by providing false or misleading information or using deceptive or misleading practices. Such practices may include situations where purposes are stated in vague or inaccurate terms, in an illegible font or placed in an obscure area of document or a location that is difficult to access.

2.3.1 Deemed Consent

You should be aware that under the following circumstances, you may have deemed to have given your consent:

Deemed consent by conduct

a. Deemed consent by conduct applies to situations where you voluntarily provide your personal data to the bank. You may be regarded as voluntarily providing personal data where you take certain actions that allow your personal data to be collected, without providing the data yourself. Consent is deemed to be given to the extent that you intended to provide your personal data and took the action required for the data to be collected by the bank. The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances.

Example:

As an online banking customer of Bank ABC, you logged into your online banking account with Bank ABC to perform a bill payment to a merchant. As part of the bill payment instructions, you include the merchant's bill payment account reference for the purpose of enabling the merchant to reconcile your payment.
Even if consent is not requested by the Bank as described in the Consent obligation above, you would have deemed to have consented to Bank ABC's collection, use and disclosure of your personal data to the merchant as you have voluntarily provided your personal data and it is reasonable that you would voluntarily provide your personal data for such purpose.

Deemed consent by contractual necessity

b. This applies to situations where the collection, use and disclosure of your personal data is reasonably necessary to conclude or perform a contract or transaction between you and an organisation (which may be an organisation other than the bank). This would include situations where in addition to arrangements stated in the banks' terms and conditions and their privacy statements/policies, disclosure to or use by another organisation is needed to fulfil or provide their products or services to you.

Example:

You visit Retailer XYZ and perform a credit card purchase of goods by providing Retailer XYZ with the details of your credit card issued by Bank ABC. To the extent that disclosure by Retailer XYZ to downstream organisations (e.g. Bank ABC, payment gateway etc.) is reasonably necessary to fulfil the transaction between you and Retailer XYZ, Bank ABC and other further downstream organisations may collect, use or disclose your personal data based on your deemed consent by contractual necessity.

Deemed consent by notification

c. When relying on your deemed consent by notification, banks will perform the following before proceeding to collect, use or disclose your personal data:

- conduct an assessment to eliminate or mitigate the likelihood of adverse effects;
- take reasonable steps to ensure you are informed about the bank's intention to collect, use or disclose your personal data and the purposes of such intended collection, use or disclosure. Such notifications will be communicated in a reasonable manner taking into account the bank's typical channel of communications to you, number of individuals to be notified and whether the matter is time-sensitive; and
- provide you with a reasonable opt-out period for you to opt out.

Banks are not required to provide its above-mentioned assessment to you if it contains commercially sensitive information.

Example:

You are a customer of Bank ABC and your voice data is collected when you call its customer service hotline for assistance. Bank ABC informs all its customers that their voice data is collected for this purpose.

Bank ABC intends to use your collected voice data (i.e. voiceprint) as an alternate means of authentication to complement existing verification methods (e.g. where you misplace your credentials or where your mobile number is tagged to your bank account).

Bank ABC assesses that its use of voiceprints to authenticate customers is sufficiently reliable and secure, and there is no likely adverse effect to its customers in using their personal data for this purpose. It also assesses that emailing customers on the intended use of their personal data would be an appropriate and effective method of notification, as the bank regularly sends emails to its customers regarding the changes in its business operations and privacy policy. It also assesses that 10 days is a reasonable period for customers to opt out.

Bank ABC sends an email to you to notify you of the intended use of their voice data for authentication purposes and provides a contact number for customer queries. A hyperlink is provided in the email if you wish to opt out of the use of their voice data for this purpose within 10 days from the date of the email.

If you do not opt-out within the 10-day opt-out period, you are deemed to consent to the use of their voice data for this purpose. After the expiry of the opt-out period, Bank ABC may commence using your voice data to develop the biometric signatures that would be used for authentication. Bank ABC must still allow and facilitate any requests from customers to withdraw their consent to use their voice data for this purpose after the 10-day opt-out period.

Banks may not rely on your deemed consent for the purpose of sending you direct marketing messages. Banks are still required to obtain clear and unambiguous consent from you where the purpose is to send marketing messages to you.

2.3.2 Exceptions to Consent

Subject to relevant constraints, including without limitation, the Banking Act, banks may collect, use or disclose your personal data without your consent in the circumstances or for the purposes set out in the First and Second Schedule of the PDPA. Such exceptions include:

a. **Legitimate interests exception** - Banks may collect, use or disclose your personal data, without your consent, where it is in the legitimate interests of the bank or other persons (including other organisations).

Specific Legitimate Interests Exceptions

Banks may rely on the specific legitimate interests exceptions in paragraphs 2 to 10 under Part 3 of the First Schedule to the PDPA which relate to specific purposes that would be considered legitimate interests. Examples where banks may collect, use or disclose personal data under these exceptions include circumstances where it is necessary for evaluation, investigations, proceedings or debt recovery.

General Legitimate Interests Exceptions

The general legitimate interests exception in paragraph 1 under Part 3 of the First Schedule to the PDPA is a broad exception that banks may rely on for any other purposes that meet the definition of "legitimate interests", when other specific exceptions do not apply.

To rely on the general legitimate interests exception, banks must conduct an assessment to eliminate or reduce risks associated with the collection, use or disclosure of personal data, and must be satisfied that the overall benefit of doing so outweighs any residual adverse effect on an individual. Banks must make known their reliance on this legitimate interests exception and this may be done via their privacy statements/policies. However, banks are not required to provide the above-mentioned assessment to you or the public.

Banks may not rely on the legitimate interests exception for the purpose of sending you direct marketing messages.

Example:

Bank ABC intends to integrate data across individuals and their associated organisations and businesses to build credit profiles about them. The use of personal data allows Bank ABC to identify credit inter-dependencies to form better assessments of actual credit standings and sources of funds for repayment.

Bank ABC conducts an assessment of legitimate interests and assesses that the benefits to Bank ABC of using the data (understanding prospects' or customers' financial standing) outweigh any likely adverse effect to the individuals (e.g. impact on credit facilities to individuals assessed to be of poorer credit standing).

Bank ABC includes in its online privacy policy that it is relying on the legitimate interests exception to collect, use and disclose personal data for conducting credit checks, analyses and due diligence checks as required under applicable laws.

In this case, Bank ABC may rely on the legitimate interests exception to collect, use and disclose personal data to perform credit analysis.

b. **Business improvement exception** - Banks may use your personal data, without your consent, for the following business improvement purposes:

- Improving, enhancing or developing new services;
- Improving, enhancing or developing new methods or processes for business operations in relation to the banks' services;
- Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or
- Identifying services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such services for individuals.

To rely on this exception, banks will need to ensure the following:

- The business improvement purpose cannot reasonably be achieved without sharing the personal data in an individually identifiable form; and
- The bank's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

The business improvement exception also applies to the sharing of personal data (i.e. collection and disclosure) between entities belonging to a group of companies, without consent, for the following business improvement purposes:

- Improving, enhancing or developing new services;
- Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' services;
- Learning or understanding behaviour and preferences of existing or prospective customers (including groups of individuals segmented by profile); or
- Identifying services that may be suitable for existing or prospective customers (including groups of individuals segmented by profile) or personalising or customising any such services for individuals.

Banks may not rely on the business improvement exception for the purpose of sending you direct marketing messages.

Example:

Bank ABC intends to use the personal data it has of its customers (i.e. income and transaction history with the bank) to create a credit risk model to reduce the time taken for it to assess and approve loan applications.

Bank ABC assesses that it requires the use of data in individually identifiable form for this purpose. Bank ABC also assesses that its use of personal data to create the credit risk model or loan application approvals is appropriate to a reasonable person, and the use of credit risks models for loan application approvals is a common industry practice.

Bank ABC may rely on the business improvement exception to use customers' personal data without consent to create a credit risk model to improve operational efficiency and service improvement such as reduced time for loan applications.

Bank ABC shares the personal data with ABC2 Corp, a related corporation which has experience with creating risk models, to create the relevant credit risk model. Organisation ABC2 Corp may use the personal data to create the credit risk model.

2.3.3 Withdrawal of Consent

a. You may withdraw your consent for the collection, use or disclosure of personal data by giving reasonable notice to the bank of the withdrawal in accordance with the bank's procedures. A withdrawal notice of at least 10 business days from the day the bank receives the withdrawal notice, is considered to be reasonable notice. Should a bank require more time to give effect to your withdrawal notice, the bank will inform you of the time frame by which the withdrawal of consent will take effect.

b. The bank will inform you of the likely consequences of withdrawing consent, if any, when it receives your notice of withdrawal of consent.

c. There may be legal consequences arising from your withdrawal of consent. For example, if you withdraw consent for the use of your personal data such that it is impossible for the bank to continue to provide services to you, it may result in the termination of the bank-customer relationship in relation to such services.

d. However, banks are not required to delete your personal data upon receipt of your withdrawal of consent. The bank may still retain your personal data if it is needed for legal or business purposes. The PDPA does not prescribe a specific time period for which banks can retain personal data. Concurrently, banks may retain your personal data to comply with record retention requirements under various written laws.

2.4 Accuracy, Access and Correction Obligations

a. Banks are required to make a reasonable effort to ensure the accuracy and completeness of your personal data collected by the bank, if your personal data is likely to be used by the bank to make a decision that affects you or is likely to be disclosed by the bank to another organisation. In determining what may be considered a reasonable effort, the bank will take into account factors such as the following:

- nature of the data and its significance to you;

- purpose for which your data is collected, used or disclosed;
- reliability of the data;
- currency of the data; and
- impact on you if the data is inaccurate or incomplete.

b. You may request for access to your personal data and information about the ways your personal data may have been used or disclosed in the past year. You may also request for correction of an error or omission in your personal data.

c. Banks may charge you a reasonable service fee for providing access, which may vary from bank to bank. In cases where you will be charged such a fee, the bank must provide a written estimate of the fee to you and will release the requested information only after you agree to pay the quoted fees.

d. Before processing your access or correction request, banks will verify your identity. For example, the bank may ask to see relevant identification documents. To protect your personal data, your request will be denied if the bank is unable to verify your identity. Upon receipt of your correction request, the bank is required to consider whether the correction should be made.

e. Banks may also seek consent from relevant individuals to disclose their personal data to each other if their respective personal data are captured in the same set of records.

f. In certain situations prescribed under the PDPA or other law, banks need not provide access to or correction of your personal data. For example, under the PDPA, banks need not provide you access to opinion data kept solely for an evaluative purpose, information derived from your transactions and interactions with them, or personal data which if disclosed, could reveal confidential commercial information that could harm the competitive position of the bank in the opinion of a reasonable person.

g. As another example, banks need not provide you with access to personal data if the burden or expense of providing access would be unreasonable to the bank or disproportionate to another individual's interest. The bank is required to respond to your access or correction request as soon as reasonably possible within 30 days after receiving your request and should inform you in writing of the time it will be able to respond to the request.

Example:

Bank ABC receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently that the individual was invited to.

The individual provides Bank ABC with sufficient information to determine when the event was held. The provision of access in this case would be reasonable and Bank ABC should provide the photo which the individual requested.

2.5 Data Protection and Data Breach Notification Obligations

a. As regulated financial institutions in Singapore, banks are subject to requirements under the Banking Act to protect the privacy of customer information and to put in place robust risk management framework to ensure IT and cyber resilience to safeguard data held. This includes the use of encryption or sharing of data via secured channels or means such that information shared are done in a safe manner or remains inaccessible to any unintended recipients. Further verification and authentication controls are in place to prevent the unauthorised access or use of individual's accounts.

b. The mandatory data breach notification provision requires banks to notify the PDPC and affected individuals of a data breach which is deemed to result in significant harm to the individuals whose data has been affected by the data breach or of a significant scale affecting 500 individuals and above.

c. A data breach has been defined to mean the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

d. A list of personal data has been prescribed under the PDPA, where it is deemed to result in significant harm to an individual when any of these are involved in a data breach. In the banking context, these would include an individual's full name, alias or full national identification number, in combination with non-public financial information; or an individual's account information in combination with any biometric data, security code or password where the account can be subsequently accessed or misused for unauthorised transactions.

e. Where a bank has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the bank must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. While there may be varying circumstances that would affect the time taken to establish the facts of a data breach and determine whether it is notifiable, banks should generally conduct the assessment within 30 calendar days.

f. Where a bank assesses that a data breach is a notifiable data breach, the bank must notify PDPC as soon as is practicable, but no later than 3 calendar days after the day the bank makes that assessment. The bank must also notify each affected individual affected by a notifiable data breach in any manner that is reasonable in the circumstances where there is significant harm to the individuals (e.g. via letter or email).

g. A bank would not be required to inform affected individuals of a data breach if, among other things, remedial action had been taken by the bank post-breach to prevent significant harm to the affected individuals or it had implemented technological measures that renders it unlikely that the data breach will result in significant harm to the affected individuals, or if the bank was directed not to notify affected individuals by the PDPC or a law enforcement agency.

Example: Bank ABC discovers that an employee had sent its mailing list containing information about 50 individuals' full name and contact to an unauthorised recipient. Bank ABC does not need to notify the affected individuals or the PDPC about the data breach as the breach is not on a

significant scale and only involves customers' full name and contact details and is deemed to be unlikely to result in significant harm to an individual.

Example:

Bank DEF sends an email stating a customer's full name and residential address to an incorrect recipient. The email also contains an attachment with the customer's transaction advice but this is encrypted. Upon discovery, Bank DEF immediately contacts the recipient to give notice of the unintended mail and obtain confirmation that the email has been deleted.

Bank DEF need not notify the affected customer of the data breach as technological measures had been applied to the personal data before the data breach which renders the personal data inaccessible or unintelligible to an unauthorised party (i.e. encryption with password). The Bank has also taken remedial action (i.e. confirmation that the email has been deleted).

Example:

Bank ABC discovers that the physical bank statement of customer A was inadvertently sent to customer B. As the bank statement shows the identity and non-public financial information of customer A, this is a notifiable data breach and should be reported to PDPC.

Additionally, Bank ABC should assess whether its remedial actions or technological measures in place are sufficient to render it unlikely that the data breach will result in significant harm to the customer A. These considerations may include obtaining confirmation from customer B that the statement was destroyed. Where the data breach is not contained and results in significant harm to the individual, notification should be provided to the affected individual involved.

2.6 Retention Limitation, Transfer Limitation and Accountability Obligations

a. The duration of time for which a bank can legitimately retain your personal data is assessed on a standard of reasonableness, having regard to the purposes for which your personal data was collected and other legal or business purposes for which retention of your personal data may be necessary. Although the PDPA does not prescribe a specific retention period for personal data, banks would need to comply with any legal or specific industry-standard requirements that may apply.

b. To transfer personal data outside of Singapore, banks must ensure that the personal data transferred is afforded protection comparable to the protection under Singapore law.

c. Banks are required to develop and implement data protection policies and practices to meet their obligations under the PDPA. Banks are also required to develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. This is to ensure that banks can effectively address your complaints and concerns with their data protection policies and practices and aid in their overall compliance efforts. Such safeguards to protect data and to provide feedback channels from customers, are already part of the existing MAS' requirements to ensure fair dealing with banks' customers.

d. Banks are required to have a Data Protection Officer responsible for ensuring that the bank complies with the PDPA. For further information on a particular bank's data privacy policy and processes, please refer to the relevant bank's contact details that are available on each bank's website.

3. DO NOT CALL ("DNC") PROVISIONS

a. The DNC Provisions enables individuals to opt out of receiving telemarketing messages or messages of a marketing nature which fall within the meaning of 'specified message' in section 37 of the PDPA ("Specified Messages") by registering their Singapore telephone numbers on one or more of the DNC Registers. In most instances, a marketing message of a commercial nature would be a specified message within the meaning of the PDPA.

b. The DNC Provisions apply equally to all means by which a sender may send a specified message to a Singapore telephone number. These include, for example, voice calls, SMS, or any applications (such as 'WhatsApp', 'iMessage' or 'Viber') which use a Singapore telephone number. The DNC Provisions apply only to specified messages sent to a Singapore telephone number. Push notifications wherein information is sent to a mobile device directly from a server without the use of a Singapore telephone number are not subject to the DNC Provisions.

c. Banks are prohibited from using dictionary attacks, address-harvesting software or similar automated means to send specified messages indiscriminately.

d. The Do Not Call Registry (DNC Registry) has three separate DNC Registers in which you may register your number, namely the:
   - No Voice Call Register;
   - No Text Message Register; and
   - No Fax Message Register.

e. You may still receive Specified Messages for up to 21 calendar days from registration of your Singapore telephone number with the DNC Registry; from banks that had checked the DNC Registry prior to your registration.

> **Example:**
>
> You register your telephone number with the No Text Message Register. Upon successful registration, you receive a confirmation message: "91234567 has been added to the No Text Message Register. You may still receive telemarketing messages within the next 21 days. For more options, SMS 'DNC' to 78771."

Two days later, you receive an SMS from Bank A, promoting their new high interest fixed deposit account. Bank A is not be in breach of the DNC Registry Provisions. Generally, a bank must not send a Specified Message to a Singapore telephone number, unless the bank had checked and received confirmation that the Singapore telephone number is not listed in the relevant DNC Register, within 21 days before sending the Specified Message.

f. There are some messages that are excluded from the DNC Registry Provisions. Specified messages will not include any of the messages referred to in the Eighth Schedule to the PDPA. Even after you have registered your Singapore telephone number with the DNC Registry, you may still receive these types of messages from your bank subject to the DP Provisions, for example:

- Messages to customers with an ongoing relationship with the bank and relates to the subject matter of the ongoing relationship;
- Specified Messages to individuals who have given clear and unambiguous consent;
- Messages of a purely administrative, servicing and non-marketing nature;
- Messages solely to provide information you have requested for;
- Messages solely to facilitate, complete or confirm a transaction;
- Messages solely to deliver goods or services, including product updates or upgrades previously agreed;
- Messages solely to provide notification concerning a change in terms and features.

Messages to customers with an ongoing relationship with the bank

g. Even if your Singapore telephone number is registered with the DNC Registers mentioned above, a bank may send certain messages by voice call, text or fax to you, if at the time of sending the message, the bank has an ongoing relationship with you, and the purpose of the message is related to the ongoing relationship. Ongoing relationship means a relationship, on an ongoing basis, between the bank and you, arising from the carrying on conduct of a business activity or an activity (commercial or otherwise) by the bank.

h. If you do not wish to receive telemarketing messages relating to your ongoing relationship with the bank, you must inform your bank separately, even if you have registered your number in the DNC Registers.

Example:

You hold a credit card issued by ABC Bank since February 2021. In March 2021, you registered your Singapore telephone number on the No Text Message Register, but did not separately inform the bank that you wish to stop receiving text messages related to your credit card.

Since you hold ABC Bank's credit card, since February 2021, there is an ongoing relationship between ABC Bank and yourself. Even if your number is registered on the No Text Message Register, ABC Bank may continue to send you text messages for purposes related to the ongoing relationship, such as messages on credit card usage, credit card promotions or lower interest rates for your card.

Examples of such messages would include:

- "Spend a min. of S$200 on your ABC Bank Credit Card and pay over 6 or 12 months instalment."
- "Up to 25% off online shopping at GHI Co, DEF Co & more with your ABC Bank Credit Card."
- "Apply for Transfer of Balance at effective interest rate of 1.90% p.a. on your ABC Bank Credit Card/Instant Credit."

Specified Messages to individuals who have given clear and unambiguous consent

i. Even if your Singapore telephone number is registered with one or more of the DNC Registers listed above, you may still receive Specified Messages from your bank if you have provided consent in a clear and unambiguous manner in evidential form to receiving such marketing messages at your Singapore telephone number.

Example:
You opened a fixed deposit account with ABC Bank in February 2021. In the application form, you ticked a box indicating that you would like to receive information on ABC Bank's promotions and new products by text messages at your mobile telephone number.
Subsequently, in May 2021, you register your phone number in the DNC Registry's No Text Message Register.
ABC Bank can continue to send you such text messages on its promotions and new products, as it has your clear and unambiguous consent to the sending of such Specified Messages to your telephone number in evidential form.

j. You may choose to receive Specified Messages from a bank, after you have already registered your number in a DNC Register by providing clear and unambiguous manner in evidential form to the bank.

k. Clear and unambiguous consent for the purpose of receiving marketing messages may be requested from you in the following ways:

- Through written forms with appropriate means of recording opt-in consent, for example, via a tick-box;
- Through opt-in mechanisms on the bank's website or the bank's mobile application (e.g. by asking you to click on an icon or pop-up to indicate agreement);
- Through opt-in mechanisms on the bank's ATM machine (e.g. by asking you to tap on an on-screen "agree" button); and
- Through opt-in mechanisms via non-DNC channels (e.g. by asking you to reply to e-mails.)

Messages of a purely administrative, servicing and non-marketing nature

l. If your Singapore telephone number is registered with the DNC Registry, you may still be able to receive messages from your bank that are of a purely administrative, servicing, and non-marketing nature. You do not need to inform your bank separately that you wish to continue receiving such messages.

m. Examples of such messages would include messages sent solely for the following purposes and that do not have any marketing element:

- To request that you update your personal data with the bank;
- An alert or notice relating to your accounts, products and other banking services provided to you;
- To remind you to pay a bill; or top up your Supplementary Retirement Scheme(SRS) account by the year-end deadline
- To conduct market research or market survey; or
- To obtain service feedback.

Examples:

"This is a reminder that your ABC Bank Credit Card bill is due on 1 March 2021. Do arrange payment as soon as you can to avoid late payment penalties."

"Thank you for calling our customer service hotline. For training and service quality improvement purposes, we would like to invite you to participate in a 1 minute customer feedback survey."

Messages solely to provide information you have requested for

n. A bank may also contact you solely for the purpose of providing information that you requested for. Such a message would not be considered a specified message.

Example:

"Thank you for your query with ABC Bank. We are investigating the matter. For reference you may call ABC Bank at 12345678 & provide ref no. QUERY123."

Messages solely to facilitate, complete or confirm a transaction

o. A message sent solely to facilitate, complete or confirm a transaction that you have agreed to enter into with the bank would not be considered a Specified Message.

Example:

"Your six digit One Time PIN is 123456. Please enter this to proceed with your secure transaction."

Messages solely to deliver goods or services, including product updates or upgrades previously agreed

p. A message sent solely to deliver goods or services, including product updates or upgrades, that you are entitled to receive under the terms of a transaction you have previously agreed to enter into with the bank would not be considered a Specified Message.

Examples:

You have signed up for wealth and product management solutions and services of Bank ABC. These solutions and services that you have engaged Bank ABC for includes:

- Financial planning solutions;
- Product upgrades and updates;
- Wealth planning solutions;
- Trust and insurance solutions;
- Product replacement; and/or
- Product segment advice.

You may then be contacted by Bank ABC at your Singapore telephone number to discuss your financial portfolio, provide you with product segment advice or other of the product and portfolio solutions and services that you have engaged Bank ABC for.