GUIDELINES FOR SUBSCRIBER VERIFICATION PROCESS

INTRODUCTION

1. Telecommunication operators perform verification of their customers' identities upon receiving service requests through channels such as customer service hotlines, websites, mobile applications and face-to-face engagement at retails shops or booths. Potential customers or subscribers are required to furnish information, according to the details requested by their operators, for the verification of their identity before signing up to new services or making changes to existing subscriptions.

2. In view of increasing cyber security threats, telecommunication operators should review and tighten existing subscriber verification processes to protect consumers from unauthorised and fraudulent access of their telecommunication subscriptions. These guidelines are advisory in nature and intended to enhance the robustness of the subscriber verification processes of telecommunication operators offering postpaid services to consumers.

SUBSCRIBER VERIFICATION PROCESS

3. The guidelines are recommended for service requests (except new service sign-ups where original identification documents ("**ID**") are verified by operators) received by operators over **customer service hotlines** and **online channels**. For face-to-face service requests, IMDA notes that service providers generally already perform verification using customers' or subscribers' original ID.

4. In establishing these guidelines, IMDA has taken into consideration that not all service requests made through customer service hotlines and online channels have monetary impact or lead to unauthorised disclosure of personal information on affected subscribers should there be wrong service requests made due to fraudulent activities. Accordingly, IMDA is of the view that more stringent subscriber verification processes should be accorded for service requests that have monetary impact or may lead to unauthorised disclosure of billing or usage records of affected subscribers due to the increased risk of unauthorised and fraudulent usage. These would include, but are not limited to, the following:

    - Re-contracting;
    - Service termination;
    - Value-Added Services ("**VAS**") activation and/or deactivation; and
    - Enquiries on billing or usage (e.g. call/SMS) records.

IMDA notes that general and billing enquiries, with the exception of queries on billing and usage records, would usually have no potential monetary impact or risk of unauthorised disclosure of personal usage or billing information.

5. For the purpose of these guidelines, name, NRIC number, address and date of birth will be collectively referred to as "**Basic Personal Information**".

Service Requests with Monetary Impact and/or Disclosure of Billing / Usage Records

6. For service requests with monetary impact on subscribers and/or potential disclosure of billing or usage records, operators should verify subscribers' identities using details beyond Basic Personal Information before processing service requests received over customer service hotlines and/or online channels.

7. Operators should verify subscribers' identities using a combination of the following:
   i. Basic Personal Information **AND**
   ii. Subscriber-unique information (e.g. last payment mode, other active services subscribed, VAS subscribed, user IDs, passwords, or pre-set security questions) **OR**
   Authentication measures such as One-Time Password ("**OTP**") or voice and/or other biometric authentication.

8. For avoidance of doubt, these guidelines need not apply to service requests received via customer portals or mobile applications that incorporate a subscriber authentication process (such as using user name and password, or fingerprint/ face ID for log-in).

Service Requests with No Monetary Impact and/or Non-Disclosure of Billing / Usage Records

9. For service requests with no potential monetary impact and/or non-disclosure of billing or usage records, IMDA notes that the impact of unauthorised access would be low. These requests would include general enquiries and billing enquiries, with the exception of enquiries for billing or usage records. Nonetheless, operators should protect against unauthorised disclosure of account information. IMDA thus considers that it is good practice for operators to minimally verify Basic Personal Information for such service requests, unless the queries are not account specific (e.g. queries on where to pay bills, price of mobile plan).