Real-name Registration Programme for SIM Cards

Consultation Paper

Commerce and Economic Development Bureau

Real-name Registration Programme for SIM Cards

Consultation Paper

Commerce and Economic Development Bureau
January 2021

ABOUT THIS CONSULTATION PAPER

1. This consultation paper is issued by the Communications and Creative Industries Branch of the Commerce and Economic Development Bureau (CEDB) to seek the views of members of the public, the telecommunications industry and other stakeholders on a proposed real-name registration programme for subscriber identity module (SIM) cards. This consultation paper consists of four chapters.

2. Please send your comments to us on issues covered in this consultation paper on or before **28 February 2021** by one of the following means:

   By mail: Communications and Creative Industries Branch
   Commerce and Economic Development Bureau
   21/F, West Wing, Central Government Offices
   2 Tim Mei Avenue, Tamar
   Hong Kong

   By email: SIM@cedb.gov.hk

   By fax: 2511 1458

3. Electronic copy of this consultation paper is available on the website of the CEDB (http://www.cedb.gov.hk/ccib). All relevant Hong Kong ordinances are available for viewing and downloading on the websites of Hong Kong e-Legislation[1] maintained by the Department of Justice.

4. Submissions received will be treated as public information and may be reproduced and published in whole or in part and in any form for the purposes of the consultation exercise and any directly related purpose without seeking permission of or providing acknowledgement of the respondents.

5. Any personal data collected in the written submissions will be used for the purpose of the consultation exercise and any directly related purpose. Unless otherwise specified, the names and affiliations of the respondents may be posted on the website of the CEDB or referred to in other documents published for the purpose of the

[1] https://www.elegislation.gov.hk/

consultation exercise and any directly related purpose. Personal data collected may also be transferred to other relevant bodies for the same purposes. For access to or correction of personal data contained in your submission, please contact the CEDB (see paragraph 2 above).

CONTENTS

List of Abbreviations

CA	Communications Authority
CEDB	Commerce and Economic Development Bureau
CLOTS	Class Licence for Offer of Telecommunications Services
eKYC	electronic Know Your Customer
IMDA	Infocomm Media Development Authority
LEAs	Law Enforcement Agencies
MNOs	Mobile Network Operators
MVNOs	Mobile Virtual Network Operators
PPS	Pre-paid SIM
SIM	Subscriber Identity Module
SSPs	SIM Service Plans
TO	Telecommunications Ordinance (Cap. 106)

Chapter 1

Mobile Services in Hong Kong

1.1 Mobile services in Hong Kong have undergone rapid development in the last decade. The subscriber penetration rate has reached 279%, meaning on average, each person in Hong Kong has almost three SIM cards[2]. As at August 2020, there are more than 20.9 million mobile subscribers[3] in Hong Kong. The number has increased drastically by 60% as compared to around 13.1 million mobile subscribers recorded in August 2010. In general, there are two major types of mobile service subscriptions offered for users, namely the SIM service plans (SSPs) and pre-paid SIM (PPS) cards. Out of 20.9 million subscribers, around 9.2 million (44%) used SSPs while some 11.7 million (56%) used PPS cards.

1.2 Currently, SSPs are largely subscription plans under which users enter into contractual agreements with the mobile service providers to obtain telecommunications services and generally commit to a specified minimum service period. Payment is settled normally on a monthly basis according to the service package subscribed and actual usage. It has been the established practice for the operators to require users to provide personal particulars (such as name, identity document number, date of birth, etc.) for regular billing and customer service purposes.

1.3 On the other hand, PPS services generally operate on a pay-as-you-go basis, i.e. users can pay to top-up talk time, data and other value added services as they wish. Users normally do not need to sign any fixed-term contract with the mobile service provider. The PPS can be used immediately upon purchase after following simple set-up procedures. There is no requirement for the operator to register personal particulars of the PPS users for the use of service. PPS services are popular because of such flexibility and convenience, particularly for low-volume users and those who do not wish to be bound by a fixed-term monthly plan or service package. As a result, circulation of PPS cards has almost doubled from 6.4 million in the last decade to some 11.7 million in August 2020.

---

[2] On the basis of Hong Kong's population recorded at 7.5 million in mid 2020 and 20.9 million of mobile service subscribers in August 2020.

[3] All mobile statistics in this document do not include machine type connections.

1.4 At present, there are four Mobile Network Operators (MNOs) in Hong Kong which are large licensed carriers permitted to establish and maintain core telecommunications network infrastructure and radio base stations throughout the territory of Hong Kong for providing public mobile services. At the same time, there are around 20 mobile virtual network operators (MVNOs) procuring network capacity/data volume/call minutes from MNOs; and many other service providers operating under the Class Licence for Offer of Telecommunications Services[4] (CLOTS) procuring the same from MNOs/MVNOs also offer SSP or PPS services under various brand names with different service features, pricing levels, and marketing/selling the products through their own network of retailers and distributors to cater for the needs of their customers.

1.5 Under the existing regulatory framework for CLOTS, the licensee is not required to register its information with the Communications Authority (CA) unless it has a customer base of 10 000 subscriptions or more.

[4] Under section 7B of the Telecommunications Ordinance (Cap. 106) (TO), a class licence gives a person the right to carry on the activities specified in the class licence that are otherwise prohibited. The activities are generally of smaller scale and do not involve establishment or maintenance of any means of telecommunications. Service providers operating under class licences are not required to make any active application for approval by the Communications Authority. Any party which meets the criteria and conditions set out in the class licence would automatically be deemed as being granted a class licence and hence subject to the licence conditions therein. CLOTS is one form of class licences created under the TO.

Chapter 2

Need for Regulation of PPS Cards

2.1 Welcoming the 5G era and in light of the revolutionary applications and convenience likely brought about by 5G technologies, it is imperative to ensure the integrity of the telecommunications services as well as the security of our communications network by minimising misuse and abuse.

2.2 While PPS services have benefited local users and visitors looking for affordable, flexible and convenient mobile services usage, the anonymous nature of PPS cards have also been exploited by criminals in committing serious and organised crimes such as telephone scams, human smuggling, home-made bombs, drug trafficking, syndicated burglary, technology crime, terrorist activities, immigration-related racketeering, etc.

2.3 Anonymous PPS cards enables criminals to conceal their real identity and evade detection. Telephone deception, for instance, is a common type of crime committed by criminals taking advantage of anonymous PPS cards. Typically in these cases, swindlers used PPS cards to approach the victims, making it difficult for the Police to unveil their identities, apprehend the perpetrators and recover the deceived property. In many of these cases, victims are ordinary telephone users, who ended up in suffering from huge monetary losses. People in vulnerable groups, the elderly, retirees or those who are less familiar with the use of technology are particularly at risk. The prevalence of telephone deception cases making use of anonymous PPS cards have caused inconvenience and anxiety among the public towards telephone calls from unknown telephone numbers, occasionally causing them to miss important calls from legitimate callers. This will affect public confidence in the telecommunications services in Hong Kong. There is a genuine need to take effective action to deter such abuse.

2.4 Anonymous PPS cards are also a common tool used by criminals in committing serious and violent crimes that threaten public safety. For instance, PPS cards were deployed to detonate home-made bombs remotely, blatantly putting our community at risk. In 2019, bombs equipped with PPS cards for remote detonation were found in populous spots in the city. Had these bombs exploded, the consequence would have been unimaginable. PPS cards are also used by drug trafficking rings and smuggling syndicates to communicate

clandestinely about orders and delivery. In recent years, overall crime rates as well as illegal activities involving PPS cards are notably on the rise. Without any requirement to register PPS users, it is difficult for law enforcement agencies to trace, identify and apprehend the ringleaders behind the scene.

2.5 In the past three years (from 2018 up to October 2020), there are a total of 1 120 "Guess Who"[5] reported cases involving monetary losses of some $59 million, increasing from 262 cases ($13.52 million) in 2018, to 418 cases ($22.76 million) in 2019 and 440 cases ($22.70 million) in 2020 (up to October). Amongst those deception cases involving local mobile phone numbers, some 70% use local anonymous PPS cards to reach out to potential victims.

2.6 PPS cards were also used extensively in different kinds of deception cases. From January to October 2020, in the 5 728 e-shopping fraud cases recorded, some 3 000 local SIM cards (89% of which were anonymous PPS cards) were involved. In telephone deception (993 cases), investment fraud (372 cases), employment fraud (259 cases), advance fee fraud (632 cases), where local SIM cards were used, PPS cards accounted for 82% to 90%. In serious crimes such as homicide, robbery, burglary, wounding and serious assault, serious drug-related offences, arson and rape, etc., where local SIM cards were involved, up to 70% were PPS cards.

2.7 The anonymous nature of such services undermines people's confidence in the integrity of telecommunications services, jeopardises genuine and legitimate use of telecommunications services and creates obstacles for law enforcement. There is hence an urgent need to plug this loophole by introducing a real-name registration programme for better regulation of use of PPS cards as well as for facilitating the prevention and detection of crimes.

2.8 It is clear that the prevalence of criminal activities associated with PPS cards needs to be cracked down and tackled. As regards SSPs, although currently the personal information of users are collected and kept by mobile service providers for the purpose of billing, collection of charges and customer services, the arrangement is purely a commercial practice and the types/records of information collected are entirely up to

---

[5] "Guess Who" refers to calls made by fraudsters to victims asking them to guess the caller's identity. Once the victims have made a response, the fraudsters would then impersonate their relatives or friends to cheat them out of money with various excuses.

individual service providers to serve their own business needs rather than to comply with any regulatory requirements. From the regulatory perspective, there are no strong justifications to apply less stringent registration requirements on SSP as compared to PPS services. Such regulatory imbalance, if allowed, clearly creates a loophole and may result in possible circumvention. We therefore consider it necessary to provide relevant statutory backing for mobile service providers to collect and store the same types of personal information.

2.9 We intend to put in place a real-name registration programme covering both PPS and SSP users to strike a balance between prevention of SIM card abuses and protection of privacy and freedom of communication. Given that currently, personal information of SSP users are generally collected by mobile service providers already as mentioned in paragraph 2.8 above, the proposed real-name registration framework should not have significant impact on them.

Experience in Other Jurisdictions

2.10 Many other jurisdictions (including a number of Organisation for Economic Co-operation and Development economies) have put in place a registration system for SIM cards to enhance telecommunications services and curb terrorist and serious crimes. According to a paper published by the GSM Association in March 2020, real-name registration is in fact a common practice. Some 155 jurisdictions globally have implemented SIM registration requirements including Australia, Mainland China, France, Germany, Italy, Japan, Macau, Malaysia, Singapore, South Korea and Taiwan. The report also noted that SSPs are usually linked to fixed term contracts with MNOs and tend to involve credit worthiness checks. As regards PPS, some jurisdictions such as Mainland China, Malaysia, Singapore and Taiwan have also imposed a cap to limit the number of PPS cards that can be registered by each user.

2.11 Australia, for example, introduced the ID checks requirement for prepaid mobile services in 2000. Users purchasing mobile prepaid services are required to provide telecommunications operators with personal information including name, identity documents, date of birth, address and the number of registered SIM cards at hand. Australia, under normal circumstances, limits the number of PPS cards for each user to less than five, unless the user provides additional identification documents for verification. Telecommunications operators have devised their own registration means (e.g. mobile websites or mobile

apps) to facilitate registration by users. To date, the programme has been operating smoothly without bringing much inconvenience to the general public. For SSPs, telecommunications service providers are required under the Telecommunications Consumer Protections Code to take a credit assessment before providing a customer with the services with a view to preventing consumers from over-committing themselves when entering into the relevant contracts, which involves information to identify a person such as name, date of birth, address and employer.

2.12 Macau introduced a registration programme for PPS cards in 2019. The information required for registration includes name and date of birth of the users, as well as serial number of their identity documents and the scanned copies. The registration programme was implemented in phases. Registration for new PPS cards started 180 days after the commencement of the programme. Users of existing PPS cards should register with the respective operators in the subsequent 120 days, after which any unregistered PPS cards would be suspended for use. There was a further phase of 180 days allowing users of suspended PPS cards to apply for reactivation upon registration.

2.13 Under Macau's registration programme, both SSP and PPS cards are covered and are subject to the same registration requirements where individual customers are required to provide the personal particulars (i.e. name, gender, date of birth, and number and country/destination of issue of the identity document) for registration. Macau's registration programme also covers business/corporate customers where information including name and number of the business registration (with a copy lodged with the application) as well as personal particulars of the authorised representative of the business/corporate (who may not be the actual users of the SIM cards) will be registered.

2.14 In Singapore, the Ministry of Home Affairs in collaboration with the Infocomm Media Development Authority (IMDA) set up the regulatory framework for recording the customer personal details of PPS cards since 2005. In January 2019, IMDA launched the implementation guide of electronic Know Your Customer (eKYC) which prescribes the requirement to deploy remote registration of subscribers for SSPs and pre-paid cellular mobile services using the eKYC solution. The minimum age for SIM registration is 15 years old, and the maximum number of PPS cards permitted for each user is three.

2.15 From the experience in other jurisdictions set out above, it is not uncommon for both PPS and SSP users to be subject to real-name registration and a cap on maximum number of PPS cards registrable. Their experience also suggests that sufficient grace period will be useful for citizens to adapt to the new registration requirement, and it would not result in major disruption to telecommunications services users.

Chapter 3

Proposed Real-name Registration Programme

3.1 To better regulate SIM services for the purpose of ensuring proper use, control and conduct of telecommunications services, and to maintain the integrity of the telecommunications services through more effective enforcement against abuse, we intend to introduce a real-name registration programme for SIM cards used for person-to-person communication. To provide the legal basis for the operation of the registration programme, a Regulation will be made by the Chief Executive in Council pursuant to section 37(1)(a) of the TO. The proposed registration programme would cover both SSP and PPS cards so as to provide the necessary statutory backing for licensees to register, collate, keep and, where necessary, disclose relevant personal information of the users as required under the Regulation. The CA will be invited to promulgate guidelines for licensees to comply with the registration requirements. Since mobile operators already keep the particulars of their SSP customers, we do not intend to require existing users/customers of SSPs to separately re-register with their mobile service providers. The measure will therefore mainly affect PPS cards users, requiring service providers to treat PPS cards on par with the practice for SSPs. The key features of the registration programme are set out in the ensuing paragraphs.

Registration of Personal Particulars

3.2 Currently, for subscribers of SSPs, personal particulars such as names, identity document number (normally with a copy for records) are registered by the licensees as part of the contract or agreement of provision of relevant telecommunications services. To minimise the burden on licensees for SSPs, we propose that the operators/mobile service providers would not be required to re-register their existing users/customers all over again, so long as the required information is properly kept with them and are available for disclosure as required under the Regulation. The operators/mobile service providers will need to ensure full compliance with the registration requirements under the Regulation for their SSP customers upon commencement of new service contracts or contract renewal.

3.3 Drawing reference to the practice for SSPs, we propose that the following information as set out in their identity document, together with

its copy, should be provided to operators/mobile service providers for registration –

- name in Chinese and English (as applicable);
- identity document number (HKID number or serial number of other acceptable identity documents such as travel documents for visitors);
- copy of the identity document; and
- date of birth.

3.4 Under the proposed Regulation, licensees should not activate a SIM card to give access to telecommunications services provided by them unless the above information has been provided by a user. While currently SSP users will normally need to provide the above information to the licensees face-to-face for subscribing to the services, licensees can make use of other means and channels to register their PPS customers. For example, self-registration/activation by users can be facilitated online or through mobile apps when they activate their new PPS or top-up their existing PPS cards after the registration requirements have come into effect.

3.5 At the moment, some SSP subscribers are registered as company/corporate users. The information they provide to licensed service providers includes name of company, business registration number (normally with a copy for record), name and contact details of the responsible person, payment information, etc. We consider that a company or corporation can be registered as a PPS user if it can provide similar business registration information and designate a person (and furnish his or her personal particulars same as those requested in paragraph 3.3 above) as representative or responsible person for the company/corporate user.

3.6 Drawing reference to the arrangement implemented in other major jurisdictions and to enable PPS card users to meet their genuine needs, we propose that each user (including company/corporate user) can register no more than three PPS cards with each licensee. Otherwise, it may create a big loophole and contribute to a black market where readily registered cards may be sold to unknown people for illegitimate purposes.

3.7 To prevent young people from being exploited by criminals, we propose that registration of an SSP or PPS user below the age of 16 (young person) should be endorsed by an "appropriate adult", who may be the parent, relative or guardian of the young person or someone who

has experience in dealing with the young person having special needs (e.g. a registered social worker). The personal particulars of the appropriate adult should also be registered to prevent exploitation of minors for unscrupulous purposes.

Proposal 1

SIM card users should provide the following information as set out in their identity document, together with its copy, for registration –

- name in Chinese and English (as applicable);
- identity document number (HKID number or serial number of other acceptable identity documents such as travel documents for visitors);
- copy of identity document; and
- date of birth.

A company or corporation can be registered as a PPS user if it can provide business registration information and designate a person (with provision of his or her personal particulars as listed above) as representative or responsible person for the company/corporate user.

Proposal 2

Each user (including company/corporate user) can register no more than three PPS cards with each licensee.

Proposal 3

Registration of an SSP or PPS user below the age of 16 (young person) should be endorsed by an "appropriate adult" who may be the parent, relative or guardian of the young person or someone who has experience in dealing with the young person having special needs (e.g. a registered social worker).

Licensee's Responsibility

3.8 We propose that the personal information of SIM card users be kept and stored by respective licensees (including MNOs, MVNOs and CLOTS licensees) offering the relevant SIM services. The licensees will therefore be required to establish systems/database to register and safe keep the personal particulars of their respective SIM services. All licensees will be subject to the same set of registration requirements, duties and sanctions. We also propose that all licensees will be

required to designate a contact person who will be responsible for communication with the authorities and provide information as requested under the Regulation. They can use the information in relation to the service they offer in accordance with the applicable laws, such as charging, contract administration and verifying customer identity for re-issue of SIM cards in case of loss or damage.

3.9 Licensees should check, clarify and verify the information provided by users, and to deregister the concerned SIM cards if there is reasonable ground to believe that the information provided is false, misleading or incomplete. SSP users will not be affected as licensees would normally have already verified the information prior to activating the concerned services. The personal particulars so registered will be stored in a format to be determined by the CA. The storage and use of the personal particulars will also need to comply with the relevant requirements including the Data Protection Principles under the Personal Data (Privacy) Ordinance (Cap. 486), e.g. on data security, access, sharing and correction, etc.

3.10 In order to facilitate relevant enforcement actions over improper use of telecommunication services, licensees need to maintain records of their registered users for at least 12 months after the SIM cards are deregistered. This is to ensure that perpetrators who have committed crimes would not become untraceable even if they deactivate and destroy the concerned SIM cards immediately afterwards.

Proposal 4

Licensees should check, clarify and verify the information provided by users, and to deregister the concerned SIM cards if there is reasonable ground to believe that the information provided is false, misleading or incomplete.

Proposal 5

The personal information of the registered SIM card users should be kept and stored by respective licensees (including MNOs, MVNOs and CLOTS licensees) offering the relevant SIM services for at least 12 months after the SIM cards are deregistered.

Phased Implementation

3.11 Currently, there are some 11.7 million of PPS cards circulating in the market. In order for the licensees to comply with the registration requirements, reasonable transition and grace periods will be required for the licensees to recall unsold PPS cards from their agents and retail outlets, manage the affected existing users, reprint and replace all packaging and activation instructions, as well as to adjust their work flow and internal business processes. The licensees will also need some time to set up or upgrade their systems or database. We propose that the programme be implemented in phases as below -

3.11.1 First phase: licensees to set up the registration system with a database ready within the 120 days after the date of commencement of the Regulation. On the 121st day, i.e. the Registration Day, all **new PPS cards** that are available for sale in the market as well as **new SSPs** effective from this day will need to comply with the real-name registration requirement before service activation.

3.11.2 Second phase: all **existing PPS cards sold by licensees before the Registration Day** will need to comply with the real-name registration requirement before the end of a 360-day period after the date of commencement of the Regulation (i.e. the Registration Deadline for PPS cards). We expect that licensees will in practice commence registering the users of existing PPS cards starting from the Registration Day (presumably a registration system should have been established and up and running as mentioned in paragraph 3.11.1). These PPS cards can no longer be used on the 361st day after the date of commencement of the Regulation if the users fail to register themselves with their respective service operators. To avoid bottlenecks and bunching close to the Registration Deadline, licensees should implement measures to register their PPS customers in phases, for example, sending regular SMS to remind them to register when they top-up their PPS cards.

Proposal 6

The real-name registration programme will be implemented in **two phases**. In the **first phase**, licensees should put in place a registration system with a database ready within the 120 days after the date of commencement of the Regulation. On the 121st day, i.e. the Registration Day, all **new PPS cards** that are available for sale in the market as well as **new SSPs** effective from this day will need to comply with the real-name registration requirements before service activation.

The **second phase** will allow 360 days after the date of commencement of the Regulation for users of **existing PPS cards sold by licensees before the Registration Day** to register their PPS cards in use (i.e. the Registration Deadline for PPS cards). Cards that have not completed real-name registration can no longer be used on the 361st day after the date of commencement of the Regulation.

3.12 Regarding SSPs, as mentioned in paragraph 3.2 above, operators have already been keeping relevant personal particulars of users including name and identity document information, etc. To keep the impact on existing SSP users and operators minimal, we do not intend to mandate operators to re-register their customers all over again or to contact them for updating their database of personal particulars, so long as the required personal particulars (including name and identity document number, etc.) are properly kept with them and are available for disclosure for enforcement purposes as required under the Regulation. That said, licensees should, after the commencement of the Regulation, take steps to give notices to existing customers of the possibility of disclosing their personal particulars to Law Enforcement Agencies (LEAs) under the Regulation. Licensees are required to conduct real-name registration for new customers and to ensure full compliance with the real-name registration requirements under the Regulation for their existing SSP customers upon commencement of new contracts or renewal of existing contracts. We do not see a need to specify a deadline for licensees to record or update the required personal information of existing SSP users.

3.13 We understand that some of the users especially the elderly and some needy groups may have difficulties in registering their SIM cards. We will collaborate with the mobile service providers and relevant non-governmental organisations in providing assistance to them in fulfilling the real-name registration requirements.

Proposal 7

Licensees should not be required to re-register their existing SSP customers but should be required to ensure compliance with the real-name registration requirements upon commencement of new contracts or renewal of existing contracts.

A diagram summarising the key procedures of the real-name registration programme is as below –

A: Licensees to set up registration system during the 120 days under 1st Phase

B: PPS cards sold by licensees before Registration Day to complete registration with licensees during the 240 days under 2nd Phase

Note: Licensees are required to ensure full compliance with the registration requirements for their existing SSP customers upon commencement of new contracts or renewal of existing contracts.

Request for Information from Licensees

3.14 In line with the existing mechanism, LEAs can request licensees to provide SIM cards registration records (i.e. records of the particulars referred to in paragraphs 3.3 and 3.5 above) pursuant to a warrant issued by a magistrate. Considering the nature of certain crimes (e.g. home-made bombs, kidnapping, drug trafficking and smuggling, etc.) that necessitates swift enforcement actions to be taken, relevant LEAs could, with the authorisation of an officer not below the rank of Superintendent, request licensees to urgently provide registration information of a SIM card user under exceptional circumstances to deal with certain urgent or emergency situations where the application for a magistrate warrant would cause undue delay resulting in loss or destruction of evidence and is hence impracticable. Such exceptional circumstances refer to those situation where there is reasonable ground for suspecting that a serious offence has been, is being, or is about to be committed that it is necessary to obtain the registration information of a SIM card user kept by a licensee for investigation or prevention of the offence, and any delay caused by an application for a warrant may result in loss or destruction of evidence, or for any reason it is not reasonably practicable to make the application. Such arrangements are similar to those under existing legislation (such as Crimes Ordinance (Cap. 200), Immigration Ordinance (Cap. 115), Dangerous Drugs Ordinance (Cap. 134) and Societies Ordinance (Cap. 151)).

Proposal 8

LEAs can request licensees to provide SIM cards registration records pursuant to a warrant issued by a magistrate or without warrant in certain urgent or emergency situations.

Sanctions

3.15 Licensees are currently required to comply with various regulatory requirements under the TO as well as terms and conditions of their licences and directions issued by the CA. The non-compliance with and breaches of the requirements of the proposed real-name registration programme under the new Regulation will be subject to applicable sanctions currently provided under the TO. For instance, under section 36C(1), the CA may impose a financial penalty on the licensees for breach of a licence condition, provision of the TO or its regulation, or CA's direction. The maximum levels of penalties imposed by the CA are $200,000 for first occasion on which a penalty is

so imposed; $500,000 for second occasion on which a penalty is so imposed; and $1,000,000 for subsequent occasion on which a penalty is so imposed, as set out in section 36C(3) of the TO. Moreover, where a financial penalty allowed under section 36C(3) is considered inadequate for a breach committed by a licensee, the CA may apply to the Court of First Instance under section 36C(3B) for a penalty of a sum not exceeding 10% of the turnover of the licensee in the relevant telecommunications market in the period of the breach, or $10 million, whichever is higher.

3.16 The effectiveness of the registration programme hinges on the accuracy of information provided by SIM card users. The provision of false information, for instance, fundamentally defeats the objective of the programme in enabling effective enforcement. Provision of false information and/or false document under the registration programme could constitute a criminal offence. Depending on the nature of the act and the availability of evidence, the applicable offences may include obtaining services by deception under section 18A of the Theft Ordinance (Cap. 210) and/or using false instrument under section 73 of the Crimes Ordinance (Cap. 200). The offence under section 18A of the Theft Ordinance has a maximum penalty of 10 years' imprisonment and the offence under section 73 of the Crimes Ordinance has a maximum penalty of 14 years' imprisonment. In addition, depending on the nature of the case and the availability of evidence, a person who knowingly provides a SIM card registered under his/her name to another party to facilitate the commission of an offence may be liable for, among others, aiding and abetting the commission of the relevant offence.

3.17 It is in the interest of our telecommunications industry and the general public to have an effective registration programme for SIM cards to further safeguard the use of telecommunications services. We consider the existing sanctions such as those mentioned in paragraphs 3.15 and 3.16 above are sufficient and effective, and propose that these sanctions be applicable to all licensees in cases of non-compliance and breaches.

Proposal 9

The existing sanctions such as those mentioned in paragraph 3.15 above (including financial penalties imposed by the CA on licensees) should be applied to all licensees in enforcing the real-name registration programme.

3.18 The regulatory requirements under the real-name registration programme will only apply to licensees offering SIM services. Retailers and distributors whose business involves only the sale and distribution of SIM cards issued by these licensees are not subject to the regulation of the proposed programme. However, we notice that in some jurisdictions, black markets involving retailers using their own or other person's personal particulars to register on behalf of their customers have emerged. Depending on the availability of evidence, the parties involved in such activities may be prosecuted for offences applicable in those circumstances.

Registration of CLOTS Licensees

3.19 As explained in Chapter 1 above, under the existing regulatory framework for CLOTS, only licensees with a customer base of 10 000 subscriptions or more are required to register their information with the CA. For the purpose of better implementation of the proposed real-name registration programme, we propose that all CLOTS licensees offering SIM services should be registered with the CA for more effective enforcement of the registration programme and other regulatory purposes. CLOTS licensees will be subject to the same set of registration requirements and obligations as those applicable to MNOs and MVNOs under the Regulation. We would invite the CA to consider revising the "Guidelines for Administration of the Class Licence for Offer of Telecommunications Services" before implementation of the above registration requirement.

Chapter 4

Summary of Proposals

4.1 The proposals are recapitulated below as aide-memoire:

Registration of Personal Particulars (para 3.2 to 3.7)	
1.	SIM card users should provide the following information as set out in their identity document, together with its copy, for registration – • name in Chinese and English (as applicable); • identity document number (HKID number or serial number of other acceptable identity documents such as travel documents for visitors); • copy of identity document; and • date of birth. A company or corporation can be registered as a PPS user if it can provide business registration information and designate a person (with provision of his or her personal particulars as listed above) as representative or responsible person for the company/corporate user.
2.	Each user (including company/corporate user) can register no more than three PPS cards with each licensee.
3.	Registration of an SSP or PPS user below the age of 16 (young person) should be endorsed by an "appropriate adult" who may be the parent, relative or guardian of the young person or someone who has experience in dealing with the young person having special needs (e.g. a registered social worker).
Licensee's Responsibility (para 3.8 to 3.10)	
4.	Licensees should check, clarify and verify the information provided by users, and to deregister the concerned SIM cards if there is reasonable ground to believe that the information provided is false, misleading or incomplete.
5.	The personal information of the registered SIM card users should be kept and stored by respective licensees (including MNOs, MVNOs and CLOTS licensees) offering the relevant SIM services for at least 12 months after the SIM cards are deregistered.

Phased Implementation (para 3.11 to 3.13)	
6.	The real-name registration programme will be implemented in **two phases**. In the **first phase**, licensees should put in place a registration system with a database ready within the 120 days after the date of commencement of the Regulation. On the 121st day, i.e. the Registration Day, all **new PPS cards** that are available for sale in the market as well as **new SSPs** effective from this day will need to comply with the real-name registration requirements before service activation. The **second phase** will allow 360 days after the date of commencement of the Regulation for users of **existing PPS cards sold by licensees before the Registration Day** to register their PPS cards in use (i.e. the Registration Deadline for PPS cards). Cards that have not completed real-name registration can no longer be used on the 361st day after the date of commencement of the Regulation.
7.	Licensees should not be required to re-register their existing SSP customers but should be required to ensure compliance with the real-name registration requirements upon commencement of new contracts or renewal of existing contracts.
Request for Information from Licensees (para 3.14)	
8.	LEAs can request licensees to provide SIM cards registration records pursuant to a warrant issued by a magistrate or without warrant in certain urgent or emergency situations.
Sanctions (para 3.15 to 3.17)	
9.	The existing sanctions such as those mentioned in paragraph 3.15 above (including financial penalties imposed by the CA on licensees) should be applied to all licensees in enforcing the real-name registration programme.

~ The End ~

Printed by the Government Logistics Department
Hong Kong Special Administrative Region Government