Reference Guidelines On Best Practices To Support E-Banking Service Security

1 Background

Over the past few decades, telecommunications services have evolved rapidly and have been widely adopted. Majority of population in the world can now afford personal communication services including voice calls, SMS and emails deployed across different platforms such as fixed line telephone, mobile phone, PC, tablet and others.

The banking industry has been a pioneer in developing applications around telecommunications systems to ensure the accuracy, reliability, and security of financial transactions. For instance, voice calls and SMS communication have been commonly used in confirming financial transactions or validating the identity of individuals in banking services. Although there is no doubt that using voice and SMS are convenient and secure, frauds have occurred occasionally, perhaps due to insufficient or lack of end user communications to properly educate the public on how best to protect themselves. In addition, differences in defining industry best-practices between telecommunications providers and the banking industry may also be a contributing factor. Hence, the Hong Kong Association of Banks, Hong Kong Police Force, Hong Kong Monetary Authority and Communications Association of Hong Kong (CAHK) are keen to work together with the objective to tighten these gaps and to provide the best of breed banking services to the general public in Hong Kong.

A research was conducted on what the banks and telecommunications service providers are using for identity verification and password change in nine (9) different countries, namely USA, UK, France, China, Japan, Taiwan, Philippines, Singapore and South Korea. Please refer to item 6 for details. Commonalities and best practices observed from this snapshot formed the foundation for the recommendations outlined in this Best Practice Guideline prepared by CAHK that aims to provide fixed and mobile service providers with a minimum set of recommendations on operation procedures and security protection methodologies for the following that may be used in e-Banking:

1) Voice call forwarding
2) SMS forwarding
3) Email forwarding
4) "Password Change" workflow that may be applicable to the above services

These recommendations are grouped under 3 main initiatives, namely:
a) Service Activation and Cancellation: With the needs of e-Banking transactions in mind, what additional measures can be adopted and standardized to further enhance the security of selective telecommunication services?
b) "Password Change" in the context of telecommunications services: With the needs of e-Banking transactions in mind, what additional measures can be adopted and standardized for the workflow on "Password Change" for telecommunications services?
c) Customer Education: What activities can both telecommunications and banking industries implement to advocate increased vigilance on personal identity and password protection where selective telecommunication services are being used for e-banking transactions?

Findings from the research show that although email and telephone number forwarding are common in other countries and regions, only China, Hong Kong and Taiwan have SMS forwarding service. This could be related to the risk involved in SMS forwarding - that the perpetrator may

be able to eavesdrop on consumers' communications if he/she is able to divert consumers' SMS, including possibly banks' one-time passwords, to their own devices. In view of this risk, item 2.3 of this Reference Guideline provides the "Minimum Set of Security Protection" for service providers to implement to strengthen the security of SMS handling in supporting online banking transactions. In addition, although not written into the minimum set of recommendations, service providers may take note of other measures that other service providers in the countries surveyed have adopted for future reference as the need arises, or during individual ongoing discussions with banking customers. As an example of these reference measures: China has adopted the process of always sending banking-related SMS to the original registered mobile phone numbers, restricting the forwarding of selected banking SMS to one level of forward only, adding authentication factors (e.g., requiring an OTP from hardware tokens) for SMS forwarding services and alerting consumers about the risk of SMS forwarding.

2 Service Activation & Cancellation: Recommended Minimum Set of Operation Procedures & Basic Security Protection

2.1 Voice Call Forwarding (Mobile Phone Service)

Type of Service	Service Activation & Cancellation: Minimum Set of Operation Procedures	Minimum Set of Security Protection
2.1.1 Directly from the handset containing the original registered SIM	1. Dial ****21*** + **number to be call forwarded to** + **#** + 📞 to activate. 2. Dial **##21#** + 📞 to cancel.	1. Confirmation is displayed on the handset
2.1.2 Remote Call Forward via phone	1. Dial **designated short code or phone number** on any touch tone phone to access system 2. Follow instructions to input and confirm (i) Mobile Station International Subscriber Directory Number (MSISDN) number to be forwarded, (ii) number to be call forwarded to, and (iii) pre-registered password or PIN 3. To cancel call forward: (i) Dial **##21#** + 📞 via the SIM, or (ii) **designated short code or phone number** on any touch-tone phone to access system. Following instructions to input (a) MSISDN number and (b) registered password or PIN.	1. Use of password should be mandatory for a subscriber to activate or cancel call forwarding 2. Network should return a confirmation SMS to the SIM whose MSISDN has been remotely forwarded, or has call forward cancelled remotely.
2.1.3 Remote Call Forward via Internet	1. Log on to designated website using MSISDN number and password and following instructions to activate remote call forward. 2. To cancel, log on to designated website using MSISDN number and password and following instructions to cancel remote call forward.	1. Login ID and password should be mandatory for a subscriber to access his/her account via the Operator's website/customer service portal to activate or cancel call forwarding. 2. Network should return a confirmation SMS to the SIM whose MSISDN has been forwarded or has call forwarded cancelled

		via the Operator's website/customer service portal.

2.2 Voice Call Forwarding (Fixed/Landline)

Note: For users whose fixed/landline service involves customer premises equipment (CPE) such as PABX, SIP server, etc. where customized settings may have been implemented, the operation procedures described below may be outside of the network operator's control and hence may not be applicable.

Type of Service	**Service Activation & Cancellation: Minimum Set of Operation Procedures**	**Minimum Set of Security Protection**
2.2.1 Direct from the registered phone line/extension	1. Dial designated code (e.g. ***05)** + **phone number + #** for activation. 2. Dial designated code (e.g. **#05)** to cancel. 3. Consider providing appropriate user guide to assist customer with above activation and cancellation	1. After activation, subscriber should receive some form of audio or visual confirmation, e.g. hear a special dial tone when he/she picks up the phone set connected to the landline that has been forwarded. 2. After activation, every time there is an incoming call, the customer should be alerted via some form of audio or visual cue, such as a reminder ring (short ring) to signal that call forwarding has been activated.
2.2.2 Remote Call Forward	1. Dial **designated phone number or code** to access system 2. Follow instructions to input and confirm (i) phone number to be forwarded, (ii) pre-registered password or PIN, and (iii) phone number to be forwarded to. 3. Dial **designated phone number or code** to cancel.	1. After activation, subscriber should receive some form of audio or visual confirmation, e.g. hear a special dial tone when he/she picks up the phone connected to the landline that has been forwarded. 2. After activation, every time there is an incoming call, the customer should be alerted via some form of audio or visual cue, such as a reminder ring (short ring), on the phone set connected to that landline to signal that call forwarding has been activated. 3. If this phone number is associated with a designated MSISDN, a confirmation SMS should also be sent to that number.

2.2.3 Remote Call Forward via Internet	1. Log on to designated website using pre-defined account number/user name and password. Follow instructions to activate or cancel remote call forward.	1. After activation, subscriber should receive some form of audio or visual confirmation, e.g. hear a special dial tone when he/she picks up the phone connected to the landline that has been forwarded. 2. After activation, every time there is an incoming call, the customer should be alerted via some form of audio or visual cue, such as a reminder ring (short ring), on the phone set connected to that landline to signal that call forwarding has been activated. 3. If this phone number is associated with a designated MSISDN, a confirmation SMS message will also be sent to that number.

2.3 SMS Forwarding & Remote SMS Management

Type of Service	Service Activation & Cancellation: Minimum Set of Operation Procedures	Minimum Set of Security Protection
2.3.1 Direct from the subscriber's SIM	1. Activation: (i) Press **designated short code + mobile number + # +** 📞, or (ii) Log on to Operator's WAP menu to access this function 1. Cancellation: (i) Press **designated short code + # +** 📞, or (ii) Log on to Operator's WAP menu to access function	1. Regardless of channel used, network should return a confirmation SMS message to the original SIM where the SMS forwarding function has been activated or cancelled before the actual kick-in of the function.
2.3.2 Via Internet	1. Log on to designated website using pre-defined user ID and password to activate forwarding, cancel forwarding, check SMS forwarding setting/status and manage SMS (send, check, delete)	

2.4 Auto Email Forwarding

Type of Service	Service Activation & Cancellation: Minimum Set of Operation Procedures	Minimum Set of Security Protection
2.4.1 Via Internet	1. Log on to designated website using pre-defined user name (such as email account, account number, user defined user ID) and password.	1. If the email account being forwarded is associated with a MSISDN, confirmation

	2. Following instructions to set Auto Forward 3. Confirmation on screen for successful Auto Forward Setting.	message will be sent to that number.

2.5 Change Password

Type of Service	Service Activation & Cancellation: Minimum Set of Operation Procedures	Minimum Set of Security Protection
2.5.1 Change Password Via Internet	1. Log on to designated website using pre-defined user name/login ID (such as mobile number, email account, account number or user defined user ID) and password. 2. Forward screen prompts to enter (i) current password, (ii) new password, and (iii) retype new password to confirm.	1. In addition to entering pre-defined user name and password, asking the requester to correctly answer a pre-defined security question can also be considered. 2. Confirmation on screen for successful password change. 3. If password associated with a MSISDN, confirmation SMS will also be sent to that number.
2.5.2 Change Password Via Customer Service Hotline	1. Call designated CS hotline, dial designated short code with his/her mobile number or dial IVR or designated short code to change password. 2. Certain operator's CS Hotline agent may only be able to perform limited manipulations with changing password, such as only reset account status to "Absent of Password" upon customer's request and customer will need to setup his/her own password through Internet, IVR or designated short code. 3. CS Officer will verify caller's identity by checking : (i) Mobile number, (ii) Registered Account Name, (iii) Registered HKID/Passport for personal subscribers, Business Registration number for business subscribers, 4. CS Officer will perform any combination of the following tasks, depending on individual operator's workflow or policy: (i) Reset password to default, or (ii) Send default/randomly-generated password via SMS to user's MSISDN. (iii) Reset account status to "Absent of Password" upon customer's	1. Regardless of reason for change, user should be strongly advised to change their password away from the Default setting. 2. If an email address is associated with the account, sending the new password to user's pre-defined email address should be considered.

	request and customer need to setup his/her own password through Internet, IVR or designated short code.	
2.5.3 Change Password Direct from the subscriber's SIM	1. Dial **designated short code or phone number +** 📞 to access function. 2. Log on to Operator's WAP menu to access function. 3. Dial IVR or designated short code with his/her mobile number to change password directly.	1. Confirmation should be sent back to that MSISDN after successful password change.

3 Consumer Education: Recommended Scope and Frequency

Passwords are a very, if not the most, common form of authentication used for services worldwide, and are often the only barrier to unauthorized access to someone's personal information, money and available credit. Given the vast number of these services, with each often carrying a different password, it is often frustrating and difficult at times to keep track of all the numbers, letters and word combinations. Many people, therefore, use passwords that are based on personal information and are easy to remember. However, this practice also tends to make it easier for an attacker to guess them. Independent of any system-assisted programs and tools that may be deployed by financial institutions and telecommunications service providers to help safeguard end-users password, consumers should be properly educated on how to set strong passwords and be regularly reminded about how to maintain them in order to safeguard against online fraud and other malicious activities. The following highlights the topics and precautions that need to be covered:

3.1 Password Strength

This refers to the effectiveness of a password in resisting guessing and brute-force attacks, and is usually a combination of length, complexity, and unpredictability. The following guidelines should be clearly conveyed to end-users to promote the practice of setting strong passwords:

3.1.1 Longer passwords are comparatively more secure because there are more characters to guess. Where possible, use a minimum password length of X characters

3.1.2 Do not use passwords based on personal information that can be easily accessed or guessed: birthdays, digits from HKID cards, passports, addresses or phone numbers. Such information can easily be discovered.

3.1.3 Do not use words that can be found in any dictionary of any language. Develop mnemonic verses or codes to help remember complex passwords instead of writing them down or saving them on computers/devices

3.1.4 Use both lowercase and capital letters.

3.1.5 Use a combination of letters, numbers, and special characters.

3.1.6 Use different passwords on different systems.

3.1.7 Passphrases, e.g., “this is a sample login passphrase,” should be encouraged. The addition of white space increases the complexity and makes it significantly more difficult for perpetrators to gain access by brute-force search. It also helps users remember the passphrase easily.

3.2 Password Protection

This refers to cautions that an end-user should follow to protect his/her password from exposure to others. The following guidelines should be clearly conveyed:

3.2.1 Do not write password(s) down on papers and expose them in plain sight. Also, do not save passwords on non-secured computers or devices that can easily be accessed by unauthorized third parties.

3.2.2 Keep password(s) confidential at all times. Do not share passwords for others to access your accounts or banking services. Watch out for suspicious phone calls, email messages, SMS or phishing sites requesting for passwords and/or other personal information. Banks and financial institutions will never request its customers to provide update or verify account or card information online, or via email, telephone or SMS.

3.2.3 Approach the "Remember your password" options on Internet browsers with care. These browser programs have varying degrees of security protecting that information, and anyone with access to the computer may be able to retrieve all saved passwords and information. Never click “yes” to “Remember your password” options on public computers.

3.2.4 Always remember to log out from your account after using a public computer (at the library, Internet cafe, or even shared computers at the office).

3.2.5 Change your passwords immediately if a suspected compromise has happened or periodically where practical.

3.3 Other Precautions

In addition to password protection, the following are other precautions that end users should be educated and reminded of when using e-Banking services:

3.3.1 Where a SIM card containing MSISDNs that has been registered or linked to e-Banking services, the owner should report the loss to relevant banks, financial institutions and mobile service provider immediately.

3.3.2 Do not store login names, passwords and other items used for online logins (e.g., hardware tokens, e-banking code cards) in the same locations or personal belongings such as handbag or wallets.

3.3.3 If a digital certificate is issued and used by service providers in accessing online banking accounts, always remember to save the digital certificate in a secured computer and use a strong password to restrict access to it. Do not store the digital certificate in unprotected USB drives.

3.3.4 Precautions on using telecommunications service forwarding:

3.3.4.1 Only forward telephone calls or SMS to reliable and uncompromised telephone handsets. Do not forward telephone calls or SMS to devices provided by unknown others.

3.3.4.2 When travelling abroad, it is advisable to use the Hong Kong SIM card and cellphone in receiving SMS instead of forwarding all SMS to another mobile phone or SIM card.

3.4 Frequency of Communication/Reminders

As password protection should be an ongoing activity, simply informing end-users once may not be enough, lest they forget over the course of time. The following are areas where both telecommunication service providers can consider making available to their respective customers:

3.4.1 Display prominently or make available for download guidelines for setting strong password and subsequent password protection guidelines on the various channels where end users can manage their passwords.

3.4.2 Login pages on a service provider's website or customer portal can show a reminder to encourage end users to periodically change their password for security purposes.

4 Suggested Telecommunication Operator Practices in Supporting Online Banking Transactions

Since banking transactions entail manipulation of financial resources that can affect the risk of users, consumers are often wary of the security of online banking transactions. This section recommends several practices which the telecommunications operators can consider adopting to support online banking transactions seamlessly and with a higher level of security and protection. Whether to adopt and, if so, how best to implement in order to avoid violation of licensing obligations and other relevant legislation will be entirely up to discussions between individual operators and banks.

4.1 Identification of electronic banking transactions

4.1.1 Where possible, service providers can consider introducing the necessary infrastructure to identify SMS sending requests from banks for financial transactions vis-à-vis general consumer transactions.

4.1.2 Where the infrastructure is available, service providers are recommended to discuss and agree with banks if they would consider also forwarding banking-services-related SMS to the SIM whose MSISDN has been remotely forwarded.

4.2 Recommended practice for forwarding of banking-related SMS

4.2.1 Where the infrastructure in item 4.1 is not available, service providers can consider alerting consumers about the risk of unauthorized forwarding of their email, voice and SMS services. For remote voice and SMS forwarding, service providers should also forward a copy of the forwarding activation SMS to the SIM whose MSISDN has been remotely forwarded. Please refer to items 2.1 and 2.3.

5 Liability Disclaimer

While the information contained herein is assumed to be accurate, CAHK assumes no responsibility for any errors or omissions. In no event shall CAHK, its employees, its contractors, or the authors of this document be liable for special, direct, indirect, or consequential damage, losses, costs, charges, claims, demands, claim for lost profits, fees, or expenses of any nature or kind that may arise out of the recommendations contained herein, including but not limited to the respective circumstances of individual user of the services described, any changes in technology or regulatory environments.

6 Appendix

To support the recommendations outlined in this document, a research was done on what different banks and telecommunication service providers are using for identity verification and password change in nine (9) different countries, namely USA, UK, France, China, Japan, Taiwan, Philippines, Singapore and South Korea. The findings and discoveries are attached herewith for your information. Appendix 1 summarizes the common banking operations to protect consumers account information. Appendix 2 summarizes the telecommunications carrier practices related to service forwarding in other countries. Appendix 3 summarizes the practices currently adopted by Hong Kong telecommunications carriers.

Appendix 2: Password Change and Service Forwarding practices by Telecom Carriers

	China	Singapore	Korea	France	USA	UK	Japan	Philippines	Taiwan
Password change									
-- via telephone	✓	✓	✓	×	✓	×	○	×	×
-- via Internet	✓	✓	✓	✓	✓	✓	✓	✓	✓
-- via SMS	✓	×	×	×	×	×	×	×	×
-- others									
Email forwarding									
-- via telephone	○	×	×	×	×	×	×	×	×
-- via Internet	✓	○	○	○	○	○	×	×	×
-- via SMS	×	○	×	×	×	×	×	×	×
-- others									
Telephone number forwarding									
-- via telephone	✓	✓	✓	✓	✓	✓	✓	✓	✓
-- via Internet	✓	×	○	✓	✓	×	×	×	×
-- via SMS	○	×	×	×	×	×	×	×	×
-- others									
SMS forwarding									
-- via telephone	✓	○	×	×	×	×	×	×	○
-- via Internet	✓	○	×	×	×	×	×	×	○
-- via SMS	○	×	×	×	×	×	×	×	×
-- others									

✓ – Commonly adopted by carriers; ○ – adopted by some carriers; × – Not adopted or not sure.

China

- Carriers covered: China Mobile, China Unicom, China Telecom
- Key findings/operations:
  - Password change via SMS, Internet, or customer service hotlines. **Identity card number** is need for authentication. **SMS OTP** will also be necessary for password reset. China Mobile further allows users to add **security questions** for multi-factor authentication in password reset.
  - Email forwarding service via telephone and Internet.
  - Call forwarding via SMS, customer service hotline, Internet, or directly via the mobile phone with designated codes.
  - SMS forwarding via SMS, telephone, or Internet. The SMS can only be forwarded once. Some operators have discontinued this service.

Singapore

- Carriers covered: M1, SingTel, StarHub
- Key findings/operations:
  - Password change via Internet or customer service hotlines. **Identity card number** is need for authentication. Same for password reset, except that the system will also send the default password to the mobile phone after verifying the SIM card and customer's identity card number.

- Email forwarding service via Internet and SMS.
- Call forwarding only via mobile phone.
- SMS forwarding (only provided by SingTel) via Internet or directly from the subscriber's SIM card with designated codes.

Korea

- Carriers covered: Korea Telecom (KT), LG U+, SK Telecom
- Key findings/operations:
  - Password change via Internet or customer service hotlines. **Identity card number** is need for authentication. Password reset via Internet or customer service hotlines. The system will send the default password to the mobile phone after verifying the SIM card and customer's identity card number.
  - Email forwarding service only via Internet.
  - Call forwarding via Internet or mobile phone with designated codes.
  - SMS forwarding service not provided.

France

- Carriers covered: Orange S.A., SFR
- Key findings/operations:
  - Password change via Internet.
  - Email forwarding service via Internet.
  - Call forwarding requires PIN for remote activation. Additional options are provided allowing users to **specify the day and time** and **forwarding calls to one or more telephone numbers** via Internet.
  - SMS forwarding service not provided.

USA

- Carriers covered: AT&T, Sprint, T-Mobile, Verizon Communications
- Key findings/operations:
  - Password change via Internet or customer service hotlines. Password reset only via customer service hotlines.
  - Email forwarding service only via Internet.
  - Call forwarding via Internet or customer service hotlines. PIN is required for remote activation.
  - SMS forwarding service not provided.

UK

- Carriers covered: BT Group, EE, O2, Virginia Media
- Key findings/operations:
  - Password change only via Internet. Password reset only via Internet with username and email address, or by answering security questions, providing personal or bill information, or using a software token.
  - Email forwarding service via Internet
  - Call forwarding via telephone.
  - SMS forwarding service not provided.

Appendix 2

Japan

- Four carriers in Japan, all have online systems for customer service.
- Key findings/operations:
  - Password change via Internet or telephone.
  - Email forwarding service not provided.
  - Call forwarding via specific telephone numbers or directly via mobile phone with designated codes.
  - SMS forwarding service not provided.

Philippines

- Six carriers operated by two main operators. Three carriers have online systems for customer service, and one allows customers to use Facebook, Google or Yahoo to login the system.
- Key findings/operations:
  - Password change via Internet. Other than login ID and password, no extra verification is needed.
  - Email forwarding service not provided.
  - Call forwarding directly via mobile phone with designated codes.
  - SMS forwarding service not provided.

Taiwan

- Five carriers in Taiwan, all have online systems for customer service.
- Key findings/operations:
  - Password change via Internet. Other than login ID and password, no extra verification is needed.
  - Email forwarding service not provided.
  - Call forwarding via telephone.
  - One carrier offers SMS forwarding via Internet or telephone. SMS can be forwarded to other telephone number or email address.

Appendix 3: Practices by Local Carriers

	China Mobile	Unicom	HKBN	HKT	HKT mobile	Hutchison	Hutchison mobile	NWT	SmarTone
Password change -- via telephone -- via Internet -- via SMS -- others (via CS ?)	✓ ✓ ×	✓ ✓ ×	✓ ✓ ×	✓ × ×	✓ ✓ ×	✓ ✓ ×	× ✓ ×	✓ ✓ × ✓	× ✓ ×
Email forwarding -- via telephone -- via Internet -- via SMS -- others (via CS ?)	N.A.	× × ×	× ✓ ×	N.A.	N.A.	× × ×	N.A.	× × × ×	N.A.
Telephone number forwarding -- via telephone -- via Internet -- via SMS -- others (via CS ?)	✓ ✓ ×	✓ × ×	✓ × ×	✓ × ×	✓ × ×	✓ × ×	✓ ✓ ×	✓ × × ×	✓ × ×
SMS forwarding -- via telephone -- via Internet -- via SMS -- others (via CS ?)	× × ×	× × ×	N.A.	N.A.	✓ ✓ ×	N.A.	✓ ✓ ×	N.A.	× × ×

China Mobile Hong Kong

- Password change via Internet or customer service hotlines. Password reset via Internet or directly via the subscriber's SIM card. Business customers need to show business registration copy and company chop in retail outlets to reset the password.
- No email service.
- Call forwarding via customer service hotlines, Internet, or a designated app "Call Manager" on mobile phones.
- SMS forwarding not allowed.

China Unicom

- Password change via Internet or customer service hotlines. Password reset via Internet or directly through the subscriber's SIM card.
- Email forwarding not allowed.
- Call forwarding via customer service hotlines or directly via the mobile phone with designated codes.
- SMS forwarding not allowed.

Appendix 3

Hong Kong Broadband Network (HKBN)

- Password change via Internet or customer service hotlines. Password reset via Internet. The new password will be sent via email or SMS to registered email address or mobile phone number.
- Email forwarding via Internet.
- Call forwarding via customer service hotlines.
- SMS forwarding not applicable (not mobile service provider).

Hong Kong Telecom (HKT)

- Password change via Internet. Password reset via Internet with HK identity card or passport numbers and by answering a security verification question. The new password will be sent via SMS to registered mobile phone number.
- No email service.
- Call forwarding via telephone with designated codes.
- SMS forwarding not applicable (not mobile service provider).

Hong Kong Telecom Mobile (1010, CSL, and Sun Mobile)

- Password change via Internet. Password reset via Internet with HK identity card or passport numbers and by answering a security verification question. The new password will be sent via SMS to registered mobile phone number.
- No email service.
- Call forwarding via mobile phone with designated codes.
- SMS forwarding via Internet or telephone.

Hutchison

- IP phone password change via the phone handset. Password reset via telephone and Internet.
- Email forwarding not allowed.
- Call forwarding directly via the phone with designated codes. Remote call forwarding allowed by dialing a designated number and codes.
- SMS forwarding not applicable (not mobile service provider).

Hutchison Mobile

- Password change and reset via Internet with email address as login ID.
- Password change via Internet, mobile app, IVRS or designated short code. Customers after logon to 3HK website or mobile app using their mobile number as Login ID can change password by inputting existing password and new password. If forget password or setup password for the first time, customers do it via Internet, designated short code and IVRS. On 3HK website, setup password/forget password, customers shall input mobile no, HKID and Date of Birth. To setup or reset password via designated code on handset or IVR, customers must use their own mobile phone to dial in and setup the password directly.
- No email service.

- Call forwarding via Internet or directly via the mobile phone with designated codes.
- SMS forwarding via telephone or Internet.

NWT

- Password change via Telephone, Internet or customer service hotlines. Password reset via Internet or customer service hotlines.
- Email forwarding not allowed
- Call forwarding directly via the phone with designated codes. Remote call forwarding allowed by dialing a designated number and codes.
- SMS forwarding not applicable (not mobile service provider).

SmarTone

- Password change and reset via Internet.
- No email service.
- Call forwarding via customer service hotlines or directly via the mobile phone with designated codes.
- SMS forwarding not allowed.