Agenda

• Recent Development of Internet Banking in Hong Kong
• Regulatory Requirements on Internet Banking
• Supervisory Approach
• Public Education by the HKMA
• Security Tips for Internet Banking Users
Recent Development of Internet Banking in Hong Kong
Recent Development of Internet Banking in Hong Kong

No. of institutions offering internet banking services

75 institutions offer internet banking services to customers

* As of June 2013
Recent Development of Internet Banking in Hong Kong

No. of internet banking accounts

End of 2012

8.4 million

Mid of 2013

8.5 million

765 thousand

798 thousand

* Customers may have more than one internet banking account in different institutions.

* As of June 2013
Recent Development of Internet Banking in Hong Kong

Growth of Internet Banking Accounts

Number of Internet Banking Accounts

- PIB (million)
- BIB (thousand)

Year | PIB (million) | BIB (thousand)
--- | --- | ---
End 2005 | 3.3 | 162
End 2006 | 3.8 | 234
End 2007 | 4.9 | 307
End 2008 | 5.7 | 401
End 2009 | 6.2 | 477
End 2010 | 7.0 | 573
End 2011 | 7.7 | 658
End 2012 | 8.4 | 765
Mid 2013 | 8.5 | 798
Recent Development of Internet Banking in Hong Kong

High mobile service subscription penetration rate in Hong Kong

- **233.2% as of July 2013** (around 2.3 mobile service subscription per person)
  
  *Source: Office of the Communications Authority (OFCA) in HK – Key Communications Statistics*
Recent Development of Internet Banking in Hong Kong

Mobile Banking in Hong Kong (as of June 2013)

**Personal Mobile Banking**
- 16 banks
- 7,600,000 accounts

**Business Mobile Banking**
- 10 banks
- 590,000 accounts
Recent Development of Internet Banking in Hong Kong

- **NFC Mobile Payment**
  - *Contactless* payment in point-of-sale terminals
  - Currently offered by a number of banks in Hong Kong
  - Other possible functions
    - E-coupons
    - Transaction history enquiry
Recent Development of Internet Banking in Hong Kong

Electronic Bill Presentment and Payment (e-bill) system
Regulatory Requirements on Internet Banking
Regulatory Requirements on Internet Banking

- HKMA aims to create a **safe** and **sound** environment for electronic banking development in Hong Kong without standing in the way of progress

- **Independent assessment** before launch of **new** Internet banking service or **major enhancement** to the existing Internet banking service
Regulatory Requirements on Internet Banking

**Two-factor authentication for high-risk transactions**

- Unregistered third party fund transfer
- Online registration of third party account for fund transfer
- Bill payment to high-risk merchant categories (e.g. credit cards, telebet service)
- Increase of Internet banking daily transaction limit
- Online change of sensitive personal information
Regulatory Requirements on Internet Banking

Two-factor authentication

- Why we need two-factor authentication?
  - User ID and password alone no longer sufficient – cases reported where user IDs and passwords were stolen through phishing, fake website, virus, Trojan, etc

- What is two-factor authentication?
Regulatory Requirements on Internet Banking

Major types of two-factor authentication

- **Digital Certificate**
- **SMS-based OTP**
- **Security Token-based OTP**
Regulatory Requirements on Internet Banking

**Controls over fund transfers**

- **Default transaction limit** – set the default transaction limit to **zero** when a new Internet banking account is first activated.

- **Increase of transaction limit** – customers can increase the transaction limit through **secure channels** (e.g. at branches or by post).

- **Reset transaction limits for inactive customers** - reset the transaction limit to **zero** if such a facility has not been used for a **prolonged** period (e.g. 1 year).
Regulatory Requirements on Internet Banking

Protection of one-time password (OTP) and customer alerts

- **Validity of OTP** – shorten the *expiration* of OTP (e.g. within 100 seconds) used for authenticating online high-risk transactions

- **SMS OTP message** – prominently display *transaction details* (e.g. type of transaction, partial payee account number and transaction amount) before the OTP within the SMS OTP message

- **SMS notification** – include *transaction details* in the SMS message notifying customers of the execution of high-risk transactions
Supervisory Approach
Supervisory Approach

- International co-operation
- Independent compliance assessment
- Continuous monitoring and examinations
- Awareness & training
- Policies & guidance
Public Education by the HKMA
Public Education by the HKMA

- **Press release** on fake bank websites / phishing emails
- **InSight articles** on emerging threats
- **Online learning** on the HKMA website
- **Cooperation campaign** with the Police, OGCIO and HKCERT
- **Radio broadcast**
Security Tips for Internet Banking Users
Security Tips for Internet Banking Users

- Apply **security patches** for your OS and applications regularly

- Install anti-virus, anti-spyware and personal firewall with **up-to-date** definition applied

- **NEVER** access your Internet banking website from a **public** computer (e.g. in a cyber cafe)

- Always **log off** after using Internet banking service
Security Tips for Internet Banking Users

**Mobile security**

- **Lock** your mobile device when not in use
- Install mobile [security software](#) if available
- Install the **official** mobile banking app from reputable sources (e.g. Apple App Store or Google Play)
- Do **NOT** access banking services with [jail broken](#) / [rooted](#) devices
- Avoid accessing banking services through [public Wi-Fi](#) network
Security Tips for Internet Banking Users

Do NOT access bank websites through
- hyperlinks embedded in e-mails
- internet search engines
- suspicious pop-up windows

Banks in Hong Kong will
- NOT send e-mails to customers with embedded links to the transactional websites
- NEVER ask customers for sensitive information (e.g. logon passwords or one-time passwords)
Security Tips for Internet Banking Users

Beware of unusual log-on process and notify your bank if you encountered

- Unusual pop-up screen
- Abnormally slow computer response
- Unexpected steps or information required for log-on