HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B1/21C
B9/29C

2 September 2015

The Chief Executive
All authorized institutions

Dear Sir / Madam,

Supervisory Policy Manual ("SPM")
Revised Module TM-E-1: "Risk Management of E-banking"

I am writing to inform you that, following consultation with the two industry Associations, the Monetary Authority is issuing a revised version of the above SPM module as a guidance note today.

The revised module consolidates and updates all relevant guidance issued by the HKMA in the past in relation to electronic banking (e-banking) services offered by authorized institutions (AIs). The revised module sets out the sound risk management principles and practices applicable to AIs' e-banking services, including areas involving strengthened controls. In the light of technological advancement and industry development, the HKMA considers it also appropriate to allow more flexibility for AIs to offer e-banking services. These include, among others:

(i) The option for customers to effect small-value funds transfers to third-party payees through Internet banking, without the need of using 2-factor authentication to re-authenticate the customer's identity. Such funds transfers should be subject to the transaction limit(s) determined by the customer and bounded by prudent cap(s) established by AIs. At this stage, AIs' prudent cap(s) should not exceed the aggregate rolling total value of HK$3,000 over 2 days per Internet banking account; and

(ii) The ability of customers to use mobile devices (such as smartphones or tablet computers) to conduct a wide range of transactions including funds transfers to unregistered third-party payees and the above mentioned small-value funds transfers. AIs should take adequate security measures to address the risks specific to the mobile channel.

As in the case of other services, it is the primary responsibility of AIs to ensure that the risks posed by e-banking are properly managed and to educate and protect their customers. To this end, AIs should complete by the end of 2015 an assessment to identify any material gaps of their existing risk management controls (including customer protection and education programme) against the revised module and any other relevant guidance. On the basis of the assessment, AIs should establish action plans to implement appropriate measures promptly to strengthen their risk management controls whenever necessary. As regards new or enhanced e-banking services, AIs should ensure that the risk management controls of the new service or enhancement concerned are in line with the revised module and any other relevant guidance before its launch.

On-line access to the module is available under the item for "Supervisory Policy Manual" on the HKMA's public (http://www.info.gov.hk/hkma) and private (http://www.stet.iclnet.hk) websites.

Should you have any questions regarding this revised module, please feel free to contact Mr George Chou on 2878-1599 or Mr Tsz-Wai Chiu on 2878-1389.

Yours faithfully,

Henry Cheng
Executive Director (Banking Supervision)

Encl.

c.c. The Chairman, The Hong Kong Association of Banks
The Chairman, The DTC Association
FSTB (Attn. Mr Jackie Liu)

This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To provide guidance to AIs on the risk management of e-banking

Classification

A non-statutory guideline issued by the MA as a guidance note

Previous guidelines superseded

Circular "Suspected ATM fraud cases" dated 14.10.03

TM-E-1 "Supervision of E-banking" (V.1) dated 17.02.04

Circular "Strengthening Security Controls for Internet Banking Services" dated 23.06.04

Circular "Precautionary Measures against Fake E-mails or websites" dated 30.09.04

Circular "Implementation of two-factor authentication" dated 31.12.04

Circular "Capacity planning for Internet banking and/or online securities trading services" dated 16.10.07

Circular "Examinations on System Capacity and Contingency Planning for On-line Securities Trading Services" dated 04.09.08

Circular "Strengthening Security Controls for Internet Banking Services" dated 13.07.09

Circular "Risk Management Controls over Internet Banking Account Aggregation Service" dated 16.07.10

Circular "Strengthening Security Controls for Automatic Teller Machine (ATM) Services" dated 01.06.11

Circular "Online Behavioural Tracking" dated 19.09.12

Application

To all AIs

Structure

1. Introduction
    - 1.1. Background
    - 1.2. Types of e-banking
    - 1.3. Supervisory objective and approach
    - 1.4. Applicable risk management principles
2. Major risks inherent in e-banking
    - 2.1. Operational risk
    - 2.2. Reputation and legal risk
    - 2.3. Risks associated with underlying financial services
3. Risk governance of e-banking
    - 3.1. Board and senior management oversight
    - 3.2. Accountability and staff competence in the three lines of defense
    - 3.3. Independent assessment and penetration tests
4. Customer security
    - 4.1. Administration of Internet banking accounts
    - 4.2. Authentication of customers

4.3. Notifications sent to customers

4.4. Security advice for customers

4.5. Customer protection

5. System and network security for Internet banking

5.1. Confidentiality and integrity of information

5.2. Internet infrastructure

5.3. Application system security

5.4. Threat monitoring and vulnerability assessment

6. Controls related to services offered via Internet banking or the Internet

6.1. Funds transfers

6.2. Online submission of information

6.3. Account aggregation service

6.4. Provision of other online financial services

7. Security controls in respect of specific e-banking channels

7.1. Internet banking accessed via mobile devices

7.2. Internet banking accessed via social media platforms or other portals

7.3. Self-service terminals

7.4. Phone banking

7.5. Contactless mobile payments

8. Fraud and incident management

8.1. Fraud monitoring and continuous intrusion detection

8.2. Incident response and periodic drills

9. System availability and business continuity management

9.1. Service level of e-banking for customers

1. Introduction

1.1 Background

1.1.1 As the banking industry is increasingly making use of technology to deliver services to customers, this module aims to consolidate and update all relevant guidance issued by the HKMA on the sound risk management principles and practices applicable to AIs' electronic banking services ("e-banking" as further described in subsection 1.2 below). This module has taken into account latest developments in the banking industry and in relevant technologies as well as supervisory guidance used in other major jurisdictions so as to facilitate the further development of e-banking in Hong Kong while also enhancing the industry's risk management controls in this area.

1.2 Types of e-banking

1.2.1 For the purpose of this module, e-banking refers to financial services (which could be transactional, enquiry or payment services) provided to personal or business customers and delivered over the Internet, wireless networks, automatic teller machines (ATMs), fixed telephone networks or other electronic terminals or devices.

1.2.2 Accordingly, e-banking includes: (i) Internet banking[1]; (ii) contactless mobile payments [2]; (iii) financial services delivered through self-service terminals[3]; and

[1] Internet banking refers to financial services delivered over the Internet to customers' devices including personal computers (including desktop computers, laptop computers and notebook computers), mobile devices such as smartphones or tablet computers (other than laptop computers), or other devices.

[2] Contactless mobile payments refer to the use of contactless or wireless technology (e.g. Near Field Communication (NFC) technology) to transmit payment transaction information (e.g. credit card information) between the customer's mobile device and the payee (e.g. a merchant).

[3] Self-service terminals refer to interactive terminals (including ATMs, cash deposit machines (CDMs), cheque deposit machines and virtual teller machines) which are used by AIs to provide financial services.

(iv) phone banking[4]. Except for certain guidance in this module on the notifications to be sent to customers regarding Card-Not-Present (CNP) credit card transactions (see subsection 4.3 below), this module does not cover other controls for managing the risks associated with AIs' credit card business (see in this regard CR-S-5 "Credit Card Business"). This module also does not intend to cover controls related to electronic terminals provided to merchant clients by merchant acquiring AIs, although some control practices in this module may also be relevant to addressing the risks associated with those services. Further, services[5] where AIs allow customers to send their instructions (e.g. funds transfers to third-party payees) through emails or faxes are not covered because such services should not be regarded as e-banking.

1.3 Supervisory objective and approach

1.3.1 The HKMA's supervisory objective is to promote a safe and transparent regulatory environment for e-banking, thereby maintaining public confidence in e-banking at large and fostering its further development. In this connection, the HKMA works periodically with the banking industry to develop sound risk management principles and practices that are technologically neutral and commensurate with the associated risks of e-banking in order to mitigate the risk of fraud as well as other key risks.

1.3.2 The HKMA adopts a risk-based supervisory approach (see also SA-1 "Risk-based Supervisory Approach") to

[4] Phone banking refers to banking services provided through fixed telephone line or mobile telecommunication network, covering both manned and Interactive Voice Response (IVR) phone banking services. For the purpose of this module, phone banking does not include the provision of banking services, over fixed telephone or mobile telecommunication networks, for the purpose of sales promotion or activity notification/call-back confirmation, or by a designated staff member (e.g. a relationship manager) who knows the relevant customer very well.

[5] In such cases, AIs should implement stringent controls for detecting and preventing any associated frauds (see the HKMA's circular of 5 June 2014 "Control measures for guarding against some recent fraud cases").

assess AIs' risk management practices. In particular, the HKMA will undertake onsite examinations or perform various off-site supervisory reviews and activities to assess how AIs manage the risks of e-banking.

1.4 Applicable risk management principles

1.4.1 Given that e-banking involves the delivery of financial services through technological means, both general risk management principles applicable to the provision of the underlying financial services and typical technological controls are applicable to e-banking. This module does not repeat the HKMA's general guidance in these areas but rather elaborates on how the relevant risk management measures may be applied or refined in the case of e-banking for different types of customers[6].

1.4.2 AIs should use a risk-based approach to managing the risks associated with e-banking. In this connection, AIs should not only make reference to this module but also other relevant Supervisory Policy Manual modules and HKMA guidance issued from time to time. AIs are also expected to refer to the Code of Banking Practice (the "Code") and any relevant guidelines issued by the banking industry associations on applicable risk management principles. Furthermore, AIs are reminded to be vigilant with regard to, and to take risk management measures that may be required under, any other relevant legal or regulatory requirements, as applicable.

2. Major risks inherent in e-banking

2.1 Operational risk

2.1.1 Operational risk is a key risk associated with e-banking, usually in terms of frauds, information

[6] For the avoidance of doubt, the guidance set out in this module should be observed by AIs in respect of e-banking services for both personal and business customers whenever applicable, unless specified otherwise.

leakages, service disruptions or system processing errors. This is because e-banking usually entails (i) provision of financial services to a sizeable group of customers over a network or via terminals or devices that are beyond AIs' direct control or that are not protected by the more stringent physical security controls generally found within AIs' premises (hence these terminals/devices could possibly be accessible by unknown parties even outside Hong Kong); (ii) reliance on multiple service providers (including the vendors of the relevant terminals or devices, telecommunication network operators, other service providers operating or supporting the e-banking computer systems or related networks, overseas offices or even other banking institutions); or (iii) relatively new or complicated system architecture or processing logics. Furthermore, the threat of attack and fraud related to e-banking and the form it may take are evolving over time, and hence the nature of operational risk is dynamic.

2.2 Reputation and legal risk

2.2.1 In the light of the heightened operational risk mentioned above, AIs could easily be exposed to increased reputation risk arising from operational incidents such as significant security breaches, data leakages, e-banking system slowdown/disruptions or malfunctions, or the inability of AIs' alternate channels to cope with the impact caused by any disruptions. Reputation risk will also arise if AIs fail to properly deal with customers' complaints and disputes related to e-banking. In the event that operational incidents or disputes lead to legal actions taken by the affected customers or other relevant parties, AIs would face reputation and legal risk.

2.2.2 In addition, AIs are subject to potential reputation and legal risk if they offer e-banking services involving transmission of sensitive customer information to and from other institution(s) (which could be outside Hong Kong), storage of AIs' customer data by other institutions, or the potential need to deal with customer disputes or losses that may be related to, or caused by,

other institutions or events taking place in other jurisdictions. AIs should also be mindful that e-banking provides additional channels for their customers / potential customers to access their services / products and this may present a similar range of risks as other channels or render the AIs exposed to additional risks depending on the scope of services offered through these channels. For example, an AI may be exposed to additional legal and reputation risk if its e-banking services increase its vulnerability to the abuse of money laundering and terrorist financing (such as facilitating anonymity), or if its e-banking services involve cross-border funds transfers while the overseas authorities regard the service as targeting overseas residents and requiring authorization in their jurisdictions.

2.2.3 Separately, an AI may face higher reputation and legal risk if it offers cross-border financial services to persons in another jurisdiction in which it does not have a physical presence or any required licence.

2.3 Risks associated with underlying financial services

2.3.1 Apart from the risks driven mainly by the use of technologies or the electronic channels used in e-banking, AIs also face the risks associated with the underlying financial services delivered through e-banking. For instance, a lending function offered through Internet banking will expose AIs to the relevant credit risks. Similarly, AIs are subject to essentially the same risks (such as operational, reputation and legal risk) arising from a securities brokerage function if they offer such function via Internet banking.

2.3.2 Among the risks related to the underlying financial services delivered through e-banking, AIs should pay particular attention to the possible implications of the increased popularity of e-banking services for their liquidity risk management. Specifically, e-banking services may allow customers to transfer large sums of funds to bank accounts in other institutions more easily compared to the traditional way of banking (e.g.

where a customer needs to be physically present in an AI's branch). This could result in potentially different customer behaviour, especially in times of stress.

3. Risk governance of e-banking

3.1 Board and senior management oversight

3.1.1 It is the primary responsibility of AIs to ensure that the risks posed by e-banking are properly managed and to educate and protect their customers. In the light of the inherent operational, reputation and legal risk as well as potential liquidity risk associated with e-banking, an AI's Board[7], or its designated committee, and senior management should exercise effective oversight of the risk management processes undertaken by both relevant business lines and support functions (especially the IT function) relating to e-banking in order to ensure that:

(i) the change in risks associated with e-banking are fully understood and that adequate risk management measures are taken when introducing or enhancing e-banking and thereafter, as there might be changes in risk over time especially as technologies evolve. In this connection, the AI's Board and senior management should attach priority to defining clear ownership of risks and promoting a strong risk culture, and devote sufficient financial resources in maintaining adequate staffing resources and expertise to manage the risks inherent in e-banking. In the event that the AI does not have the required resources or expertise to implement the required risk management controls, it should not launch or offer e-banking;

(ii) the AI complies with all relevant supervisory

[7] For the purpose of this module, the responsibility for the oversight of e-banking in respect of the Hong Kong operations of an overseas incorporated AI would rest with its local senior management, under the monitoring of its head-office or regional head-quarters, especially if its e-banking requires material support and involvement of the AI's overseas offices.

requirements/guidance issued by the HKMA or other relevant authorities as well as industry associations from time to time, including the risk management principles and practices set out in this module and other relevant modules, when introducing or enhancing its e-banking; and

(iii) the AI has an adequate system of checks and balances. Where material control deficiencies are identified, appropriate follow-up actions should be considered and monitored by the Board or senior management.

3.2 Accountability and staff competence in the three lines of defense

3.2.1 Since risk management in relation to e-banking is generally complicated and evolving (especially in respect of operational risk), it is vital for an AI to ensure that:

(i) the management and staff of the relevant business lines and support functions (i.e., the first line of defense) are accountable for, and competent in, assessing and monitoring the relevant risks and implementing the required risk management controls; and

(ii) in addition, the AI should clearly specify the accountability of the management and staff of its second line of defense (e.g. risk management function, compliance function) in evaluating the adequacy of the risk management controls implemented by the first line of defense, as well as the role of the third line of defense (normally the internal audit function) in auditing the relevant risk management controls. It is important for the AI to support the development of the technical competence and knowledge required by the second and third lines of defense for such check and balance functions accordingly.

3.3 Independent assessment and penetration tests

3.3.1 As part of the risk governance for e-banking, AIs' senior management should establish clear policies and accountability to ensure that stringent independent assessment is performed before the launch of any new electronic delivery channel of e-banking service, or a major enhancement [8] to existing services, and periodically thereafter so that there is a greater assurance that sufficient risk management controls are actually in place in relation to the service or enhancement concerned. In this connection, the AI's policy framework for independent assessment should ensure that, among others:

(i) the senior management designate which function(s) (e.g. the main business line sponsoring the e-banking service, the risk management function or the internal audit function) to be responsible for the quality of, and undertaking proper follow-up actions arising from e-banking independent assessment. All issues with material risk and associated impact identified by independent assessment should be satisfactorily resolved or accepted by senior management with sufficient justifications before the launch of the service or enhancement. For issues with material risk but accepted by senior management, they should be subject to a mechanism of periodic re-evaluation so as to ascertain whether the acceptance remains appropriate;

(ii) the scope of independent assessment covers, at a minimum, an objective evaluation (which may be risk-based) of whether adequate risk management controls have been implemented for the e-banking service in question, including those applicable controls set out in this module (focusing on relevant controls under

[8] A major enhancement may refer to, for instance, a modification of the functionalities (e.g. the introduction of an ability of conducting high-risk transactions, which are not available in the existing e-banking channel or service) or system features (e.g. the underlying technologies, or the Internet infrastructure) of an e-banking service that could lead to a material increase of the associated risks particularly the security risk and system availability of the service.

subsections 4 to 9) and other applicable HKMA and industry guidelines and circulars that are relevant to the underlying financial services and the electronic delivery channel concerned. Where relevant, the independent assessment should cover all relevant systems or processes outsourced to service providers within or outside the banking group. That said, the scope of the independent assessment could be appropriately adjusted if certain controls, systems or processes have been assessed or audited within a reasonable period of time prior to the independent assessment with respect to the risks involved;

(iii) independent assessment are performed by trusted assessors with the necessary expertise in the underlying financial services and/or electronic delivery channel, and who are independent from the parties that design, implement or operate the e-banking service. Moreover, the assessors should be able to report their findings freely and directly to the Board (or its designated committee(s)) and senior management of the AI whenever there is a need. So long as these conditions can be met, the assessors could be any function, particularly the second line of defense (e.g. risk management function) or the internal audit function of the AI or the banking group, an external auditor acceptable to the AI (e.g. including those appointed by outsourcing service providers) or any other third-party consultants. Where multiple assessors are needed in the independent assessment (e.g. when the assessor for assessing a third-party service provider is different from the assessor who reviews the AI's own systems and controls), the responsible function(s) as defined in subsection 3.3.1(i) should ensure that there is no gap among the scope of assessment performed by different assessors. In general, items to be reported in the independent assessment should cover, at a minimum, the

areas specified in Annex A, and the report should be submitted to the HKMA upon request; and

(iv) formal risk assessment is conducted periodically by, for instance, the function(s) designated by the senior management under subsection 3.3.1(i) above or an independent party (such as the assessor), to determine whether any independent assessment should be performed during the year, and if so, the scope of such independent assessment. Such formal risk assessment should be carried out at least on an annual basis for Internet banking and financial services delivered over the Internet or via a wireless network. The risk assessment should take into account objective analysis of any material change to the risk profile of the financial services being provided or the AI's e-banking system, emerging vulnerabilities and other risks related to the electronic delivery channels concerned, etc. The party responsible for performing such risk assessment should have sufficient expertise in the emerging risks posed by the e-banking service concerned so as to ensure that the need for independent assessment would not be underestimated. Moreover, the AI's policy framework or related procedures for independent assessment should require the risk assessment to be endorsed by designated senior officer(s) and depict the minimum frequency with which independent assessment should be conducted for different e-banking services/channels.

3.3.2 If an AI's policy framework for independent assessment does not include penetration tests[9], the senior management should further ensure that regular

[9] In general, a penetration test refers to the use of a variety of manual and automated techniques to simulate attacks on an institution's technological security controls, particularly attacks from malicious outsiders. For the avoidance of doubt, "vulnerability assessment" as set out in subsection 5.4.2 is not regarded as penetration tests for the purpose of this module.

penetration tests are performed by qualified independent parties (the functions/firms or individuals conducting the tests should have proven experience and/or relevant professional qualifications). For the purpose of this module, a penetration test should assess, at the minimum, the AI's Internet banking and any financial services delivered over the Internet or via a wireless network (covering enquiry-only services and relevant outsourced systems) annually. Penetration tests should be carefully planned and carried out so as not to unduly disrupt the AI's production systems/channels.

4. Customer security

4.1 Administration of Internet banking accounts

4.1.1 If AIs allow a customer to open an Internet banking account over the Internet, a reliable authentication method should be adopted to verify the identity of the customer.

4.1.2 Moreover, AIs should perform adequate identity checks when any customer requests a change to the customer's Internet banking account information (including resetting or reissuing of Internet banking password) or contact details (e.g. e-mail address, correspondence address or contact phone number) that are used by the customer to receive important information (e.g. one-time password [10] (OTP) delivered via Short Message Service (SMS)). AIs should also monitor the activities of the customer's accounts concerned. In particular, AIs should take measures to prevent and detect possible malfeasance or frauds related to these changes.

4.2 Authentication of customers

4.2.1 AIs should select reliable and effective authentication

[10] OTP is a password that is valid for authentication of a single access attempt only so that even if this one-time password is captured by a fraudster, the password cannot be reused for subsequent authentication.

techniques to validate the identity and authority of their e-banking customers. In general, two-factor authentication [11] (2FA) of customers should be implemented for e-banking channels (e.g. self-service terminals, Internet banking, phone banking or even contactless mobile payments) that allow high-risk transactions (e.g. withdrawal of customers' funds from self-service terminals or funds transfers to unregistered third-party payees). If a password (including a Personal Identification Number (PIN)) is used as one factor of authentication, AIs should put in place adequate controls related to the strength of the password (e.g. minimum password length) and disallow repeated login attempts using invalid passwords. Depending on AIs' risk assessment and any trend in potential attacks that could compromise customers' passwords, consideration should also be given to enforcing periodic changes of Internet banking passwords by relevant customers. Moreover, AIs should implement appropriate segregation of duties and security measures to ensure any password generated, re-issued or reset by AIs would not be disclosed or leaked during the generation and delivery[12].

4.2.2 For Internet banking, AIs should require 2FA [13] to re-authenticate customers' identity before performing each high-risk transaction. High-risk transactions

[11] Two-factor authentication refers to the use of two out of the three types of factors (i.e. (i) something a customer knows; (ii) something a customer has; and (iii) something a customer is)).

[12] For example, sending default or new passwords to customers via emails in clear text is not considered as a secure way of delivery.

[13] Where user IDs and passwords are used as the basic factor (i.e., something a customer knows) of authentication, examples of the second factor, in terms of "something a customer has", for authentication include (i) OTP generated by a token/device that is in the customer's possession and associated with the customer's bank account; (ii) OTPs generated by AIs' security systems and delivered to customers via SMS; and (iii) digital certificates stored in a smart card or other devices in the customer's possession. However, a mere registration of the customer's device may not be stringent enough to be regarded as "something a customer has" for 2FA purpose. If the second factor for authentication makes use of "something a customer is", this may include biometric identifiers such as fingerprint, face, iris or voice recognition provided that the identifiers are credible. In any case, AIs should evaluate the possible technologies carefully (including whether they are sufficiently mature and to what extent the method remains secure such as even if the device in the customer's possession is compromised, say, by malware) and implement the 2FA solution that is commensurate with the risks associated with the types of transaction involved.

should cover, at least, high-risk funds transfers, which include:

(i) funds transfers to payees specified by third-party bank account numbers (or unique identifiers other than bank account numbers) that have not been registered by the customers;

(ii) bill payments to merchants that have been classified by AIs as high-risk merchants[14] but where the payees' accounts have not been registered by the customers; and

(iii) transactions that effectively allow online transfers[15] of customers' eligible monetary or non-monetary benefits or interests (e.g. credit card rewards points), directly or through conversion/redemption (including via AIs' corporate websites), to third parties other than the customers themselves or those parties registered by the customers through secure channels (e.g. at a branch, by post, via Internet banking after 2FA).

4.2.3 AIs should ensure that registration of a payee's account or unique identifier in a high-risk transaction should only be allowed through secure channels (e.g. at a branch, by post or via Internet banking after 2FA) with adequate identity checks conducted by AIs. However, AIs may regard small-value funds transfers (see subsection 6.1.1 below) as not being high-risk transactions. In any case, AIs have the flexibility of applying more stringent 2FA (e.g. transaction signing using information specific to the transaction) to those high-risk transactions that they consider as more sensitive (e.g. high-risk funds transfers). Customers

[14] AIs should establish an effective and proper due diligence process to assess and determine whether a merchant should be classified as a high-risk merchant (e.g. credit cards lenders and other money lenders, securities brokers, money changers and the Telebet services). Regular assessment should also be conducted on these merchants to ensure that the assigned categories remain appropriate.

[15] It is acceptable that no 2FA is used to authenticate a customer's identity when the monetary value related to a transfer does not exceed the AI's prudent cap(s) for small-value funds transfers via Internet banking (see subsection 6.1.1).

who choose not to adopt 2FA should be restricted from conducting any high-risk transactions via Internet banking.

4.3 Notifications sent to customers

4.3.1 To facilitate customers' timely detection of unauthorized transactions that may arise as a result of fraudulent activities related to e-banking channels, AIs should, as far as practicable, notify customers immediately via an effective channel once the customers initiate transactions that are considered as of higher risk. Each such notification message should contain the transaction details, including among others, the transaction type, partial payee account number/unique identifier and transaction amount, if the information is available and relevant.

4.3.2 Given the growing fraud risk related to online credit card transactions, AIs should also send timely notifications for all CNP credit card transactions (except for recurring payments), or those CNP credit card transactions exceeding a transaction amount threshold if such a threshold can be specified by the relevant customers to the AI concerned.

4.3.3 If AIs are aware of any notifications that cannot be delivered to the customers concerned, they should use a risk-based approach to following up those situations (e.g. AIs should consider notifying the customers concerned via other alternative means).

4.4 Security advice for customers

4.4.1 AIs should warn their e-banking customers of the customers' obligations to take reasonable security precautions to protect the devices they use in e-banking and keep the passwords they use for accessing e-banking secure and secret. AIs should also observe the relevant provisions set out in the Code when providing e-banking services to personal customers. Moreover, AIs should periodically provide advice to their e-banking customers regarding precautionary security measures. Such advice

should be easy-to-understand, prominently displayed and regularly reviewed and updated. The advice should be delivered through multiple effective channels (e.g. via AIs' corporate websites, messages on e-banking login screens, email reminders, printed notifications). AIs should ensure that sufficient advance guidance and training are given to officers who handle customers' enquiries related to the security precautions of e-banking.

4.4.2 In addition, AIs should manage the risk associated with fraudulent websites, phishing emails or similar scams (which may involve Internet banking mobile applications (Apps)) which are designed[16] to trick their customers into revealing sensitive customer information such as account numbers, Internet banking passwords, OTP or credit card information. In particular, AIs should search the Internet and Apps stores regularly for fake or suspicious websites or Apps. Whenever AIs become aware[17] of fake or suspicious emails, websites, Apps or similar scams that might give the public the false impression that they originate from the AI or that their Apps can be downloaded from unofficial sources, or cases involving suspicious Internet banking login screens (e.g. pop-up windows requesting customers to input their credit card information) affecting multiple customers within a short period of time, AIs should consider and decide in a timely manner how to inform their customers and the public more widely and report the matter to the Hong Kong Police Force (the "Police"). If it is considered to be in the best interests of their customers, AIs should notify promptly their customers through issuing press releases (or other similarly effective means), and

[16] For instance, fraudulent websites (e.g. purporting to be AIs' corporate websites, AIs' pages or groups created in social media platforms or other portals) can look genuine by using different techniques such as (i) copying the genuine graphics from an AI's website; (ii) redirecting customers to the real website so that customers are communicating with the real AI concerned without knowing that their sensitive customer information may be passing through the fake website; and (iii) using a website address which is very similar to that of an AI, or which may be regarded as that of an AI.

[17] AIs may be aware of fake or suspicious emails, websites, Apps or phone banking services through their search activities or through advice/enquiries received from other sources.

report the matter to the HKMA[18]. Besides, AIs should make attempts to remove the fake or suspicious items where practicable.

4.5 Customer protection

4.5.1 AIs should seek to protect the interests of all types of customers when offering e-banking services to them. In particular, AIs should respect the spirit of the Code and the Treat Customers Fairly Charter (TCF) when offering e-banking services to their personal customers. For instance, AIs should set out and explain clearly the key features, risks and terms of their e-banking services to customers. Moreover, the terms and conditions of an AI's e-banking services should provide a fair and balanced description of the relationship between the customer and the institution. Unless a customer acts fraudulently or with gross negligence, he or she should not be responsible for any direct loss suffered by him or her as a result of unauthorized transactions in relation to the use of e-banking services. As regards business customers, AIs should ensure that there are clear terms and conditions provided to them, which should cover customers' risks and responsibilities, precautionary security measures, procedures for handling customer disputes and liabilities in relation to unauthorized transactions. Customers should be made aware of these terms before they are provided with e-banking services.

4.5.2 Separately, AIs are reminded of the need to comply with the Personal Data (Privacy) Ordinance and any relevant codes of practice / guidelines or guidance issued or published by the Privacy Commissioner for Personal Data or the Office of the Privacy Commissioner for Personal Data from time to time. For example, AIs should comply with the Privacy Commissioner for Personal Data's recommendations

[18] In general, AIs are expected to issue their press releases as soon as practicable (say, within 1 day) after they become aware of the scams, and report the cases to the HKMA immediately after the press releases are issued. After receiving a report from an AI, the HKMA will post on its website the hyperlink to the AI's press release for ease of reference by members of the public.

on best practices with respect to online tracking and use of cookies on their websites (including Internet banking websites and Apps).

5. System and network security for Internet banking

5.1 Confidentiality and integrity of information

5.1.1 AIs should adopt secure and internationally-recognised strong encryption algorithms[19] to protect the confidentiality of customers' information transmitted over external networks including the Internet, and highly sensitive information (e.g. this refers mainly to customers' login credentials such as e-banking passwords) kept in storage or sent over internal networks. Sound key management practices should also be in place to safeguard the relevant encryption keys. As the strength of encryption could be affected if outdated or weaker algorithms technologies are used, AIs should carefully evaluate the implementation of relevant encryption controls for e-banking from time to time, and improve or update the implementation whenever there is a need.

5.1.2 AIs should also implement sufficient controls to maintain and verify the integrity of the information processed by their Internet banking systems. For example, AIs should implement checks and controls in the application systems so as to reconcile data file balances after transaction updates and to check the integrity of data transmitted between different systems.

5.2 Internet infrastructure

5.2.1 AIs should establish a secure Internet infrastructure (including the design of the demilitarized zone and configuration of the relevant devices, as well as

[19] If it is not practicable to implement internationally-recognized strong encryption algorithms, AIs should still implement similarly stringent encryption algorithms as an alternative and the algorithms should be subject to independent assessment.

intrusion detection controls) to support their Internet banking system. Moreover, AIs should implement adequate security measures for the internal networks and network connections to external parties, and proper patch management procedures for systems and infrastructure components.

5.3 Application system security

5.3.1 AIs should put in place an adequate level of application system security in respect of their Internet banking system, including any Apps, covering at least application design and development, testing and implementation. In this connection, AIs should make reference to industry sound practices[20] on application system security.

5.3.2 Before launching any Internet banking system or system changes, an adequate application system source code review, which could be risk-based, should be performed. The review should aim at identifying any non-compliance with the relevant application security standards, any source codes that may potentially pose or create security threats/loopholes or whether any malicious code has been embedded in the application system. Such review should be conducted by an appropriate party[21] with relevant expertise and the party should also be independent of the staff who developed the application system.

5.4 Threat monitoring and vulnerability assessment

5.4.1 AIs should establish a systematic monitoring process (such as subscribing to reputable sources for online security news/alerts including information relating to latest attack techniques; documenting the monitoring

[20] An example is the Open Web Application Security Project (www.owasp.org).

[21] It would be acceptable if the code review is a peer review, assisted by relevant automated tools, performed by another designated member of the system development team so long as the reviewer appropriately documents the scope, approach and outcome of the peer review. If the application system is developed by a third-party vendor, the AI should be satisfied that the vendor has put in place an adequate code review process. Otherwise, the AI should conduct a code review of the application system provided by the vendor.

and analysis works performed, etc.) to closely monitor emergent security threats that are relevant to their Internet infrastructure, application systems and other relevant system components and operations.

5.4.2 AIs should also utilize automated tools (supplemented by manual techniques if needed) to perform periodic vulnerability assessment [22] to detect security vulnerabilities in their Internet infrastructure and relevant Internet banking systems.

5.4.3 AIs should adopt a risk-based approach to addressing the risks arising from the security threats or vulnerabilities identified.

6. Controls related to services offered via Internet banking or the Internet

6.1 Funds transfers

6.1.1 AIs should implement 2FA to re-authenticate the customer's identity before effecting a high-risk funds transfer transaction (see subsection 4.2.2). Nevertheless, AIs also have the flexibility to offer a service where small-value funds transfer transactions to unregistered payees' accounts or unregistered payees with unique identifiers ("unregistered payees") can be effected without re-authenticating the customers' identity using 2FA. In this case, those small-value funds transfers have to be subject to at least a transaction limit defined by the customer concerned in terms of the maximum aggregate rolling total value of such transactions over a period of time. The transaction limit(s) for small-value funds transfers should be bound by prudent cap(s) determined by AIs, having regard to factors such as their fraud monitoring capability. AIs should also clearly communicate to customers (e.g. suitable illustrations may be used if appropriate) the risk implications of the transaction limit(s) especially when AIs provide such small-value

[22] Vulnerability assessment is the process of identifying and assessing security vulnerabilities in a system or network.

funds transfer service to customers, or when customers set or increase the limit(s). To further prevent frauds from making use of such a service without the knowledge of the customers, AIs should put in place controls[23] so that only customers who choose to use the service will be able to effect small-value funds transfer transactions without 2FA.

6.1.2 In any case, AIs should put in place prudent policies and effective safeguards including a proper structure of transaction limits to minimise the risk of unauthorized high-risk funds transfers to unregistered payees. These cover, among others:

(i) funds transfer functions should be disabled or the relevant transaction limit(s) for high-risk funds transfers should be pre-set to zero when a new Internet banking account is first opened. Furthermore, the function or the limit(s) should also be reset to zero if they have not been used for a period of time (such period should not normally exceed 18 months); and

(ii) consideration should be given to offering the option of dual authorization control (e.g. maker and checker controls) for business customers.

6.1.3 Where funds transfer services via Internet banking (or other e-banking channels) allow an AI's customers, on aggregate, to transfer large sums of funds away from the AI to bank accounts (which may or may not be their own accounts) maintained in other institutions within a short period of time, the AI should ensure that its systems and controls for liquidity risk management remain effective in assessing, monitoring, controlling and managing the increased liquidity risk during both business as usual operations and in any periods of stress.

6.2 Online submission of information

[23] For instance, AIs may require customers to apply for or activate, via a secure channel (e.g. at a branch, by post, via Internet banking after 2FA) such a service beforehand. Alternatively, small-value funds transfer functions may be disabled or the relevant transaction limit(s) may be pre-set to zero initially.

6.2.1 AIs that allow customers to submit information (e.g. applications for financial products/services) via the Internet (e.g. their corporate websites) should assess the risks and establish appropriate controls, including:

(i) ensuring that adequate encryption mechanisms and other controls are in place to protect the confidentiality and integrity of any sensitive information and documents submitted by the customers via the AIs' corporate websites;

(ii) implementing system controls to detect and guard against malware attacks through any documents submitted;

(iii) considering asking the customer to provide supporting documents and conduct additional checks assessed by AIs as appropriate to validate the identity of the customer; and

(iv) posting prominent notices on the relevant part(s) of the websites for the attention of the customers who use the channel if the channel is not for urgent submission of information (e.g. reporting of fraud or suspicious transactions).

6.3 Account aggregation service

6.3.1 In general, there are two types of account aggregation service (AAS[24]) that can be offered by an AI via Internet banking:

(i) In the first type, customers are only given access to the statements of their specific accounts maintained in other institutions, in circumstances where there is no direct connection between the computer systems and networks of the institutions involved and the transmissions of the information in the statements are carried out via proven interbank

[24] When an AI offers AAS, it generally allows its customers to access their accounts maintained in other institutions (which could be in overseas jurisdictions) through the AI's Internet banking without requiring the customers to separately login to the Internet banking service of those institutions.

financial messaging networks (e.g. SWIFT); and

(ii) In the second type, customers are able to operate their specific accounts maintained in other institutions (e.g. perform balance enquiries, effect funds transfers), even on a real-time basis. This type may require a direct connection between the computer systems/networks of the two institutions, or otherwise the use of proven interbank financial messaging network for transmission of instructions between the institutions.

6.3.2 An AI offering AAS as described in subsection 6.3.1(i) should establish a policy on what types of institutions would be covered by the service, having regard to factors such as the possible reputation or legal implications. Proper disclosure to customers about the risks and limitations of the service should also be made. In principle, the AI should not have possession of the customers' authorization or Internet banking login credentials required by the other institution(s) to share the customer statements with the AI. If an AI is requested to share its customers' statements with another institution offering AAS, the AI should also formulate a policy setting out the circumstances where such request would be accommodated.

6.3.3 Where an AI intends to offer AAS as described in subsection 6.3.1(ii), it should ensure that adequate controls are in place before partnering with other institutions to launch the service. These include controls (see Annex B for more details) to ensure that, among others:

(i) the relevant business models are acceptable so as to mitigate the relevant reputation and legal risk involved;

(ii) legal reviews are performed to ensure that any applicable local or overseas legal and regulatory requirements have been observed, especially if AIs partner with overseas

institutions. Separately, adequate safeguards against the risk of money laundering and terrorist financing are in place if cross-border funds transfers can be conducted;

(iii) legal due diligence is performed if AAS involves personal data privacy concerns (e.g. when a customer's personal data needs to be transmitted to, or stored by, another institution especially if it is outside Hong Kong) so as to identify any need for disclosure or obtaining of customer consent. Moreover, appropriate controls should be implemented for customer protection such as when handling any cross-border customer complaints and apportionment of liability for any financial loss of customers that may be caused by fraud cases or system failures involving the partnering institution; and

(iv) sufficient security controls are implemented and independent assessment is performed to minimise the risk of intrusion to AIs' systems and networks through any connections with the partnering institution (e.g. due to less-stringent controls at the partnering institution or even security loopholes in its systems).

6.3.4 For the avoidance of doubt, controls similar to the above should be implemented by an AI if it partners with another institution offering AAS similar to that in subsection 6.3.1(ii).

6.4 Provision of other online financial services

6.4.1 As technological and product innovations evolve, AIs may introduce other or new financial services via Internet banking or the Internet. Under Principle 1 of the TCF Charter, the services should be designed to meet the needs of customers. In all cases, AIs should carefully assess the risks (e.g. credit risk,

market risk[25], reputation and legal risk) associated with the underlying financial services and how the use of electronic channels (especially if the financial services could be accessible from outside Hong Kong) may have shifted or amplified those risks. Among these risks, AIs should take into account whether their customers are able to transact with them directly using market prices indicated in their Internet banking systems. If so, AIs should review and strengthen corresponding controls where appropriate, including controls to ensure the timeliness and accuracy of the market prices indicated online, even amid periods of unusual market volatility.

6.4.2 If the online financial services offered by an AI involve activities regulated by the Securities and Futures Commission (SFC) (such as allowing AIs' customers to make use of their online platforms for investment in money market funds), AIs should have regard to the relevant regulatory requirements (see also "SB-1 Supervision of Regulated Activities of SFC-Registered Authorized Institutions") and ensure the requirements can still be fulfilled even if the delivery of the regulated activities involves one or more electronic channels.

6.4.3 If AIs intend to offer "crowdfunding"[26] services, they should note that this kind of service is still evolving and it is possible that certain risks involved might not as yet be adequately identified or understood. Hence, AIs should be prudent and very cautious in analyzing and managing the associated risks. Moreover, AIs that wish to become involved either directly or in cooperation with third parties in similar services should make sure that they identify and manage relevant risks, including credit, reputation, legal and operational

[25] For instance, market risk may arise if the customers are able to conduct financial transactions through electronic channels with an AI as the counterparty at prices that materially deviate from the prevailing market prices.

[26] "Crowdfunding" is generally regarded as an Internet platform that efficiently matches multiple investors with financiers (who may be natural persons and/or companies) seeking equity or debt financing (or borrowing). While one typical case is "peer-to-peer" (or P2P) lending involving lenders and borrowers, it should be noted that the business models may vary widely and a service provider may play different roles in such service.

risks and risks associated with anti-money laundering and counter-financing of terrorism, and that all necessary regulatory approvals are in place.

7. Security controls in respect of specific e-banking channels

7.1 Internet banking accessed via mobile devices

7.1.1 Apart from the risks generally applicable to Internet banking accessed via personal computers, Internet banking accessed via mobile devices entails certain specific risks such as (i) security vulnerabilities associated with mobile platforms, which may be different from those of personal computers; (ii) the risk of malware or malicious Apps that might potentially capture sensitive customer information, re-direct SMS notifications or OTPs sent by AIs, or mislead customers into carrying out unauthorized funds transfers; (iii) the risk of loss or theft of mobile devices; and (iv) customers' security awareness when using mobile devices may be lower than when using personal computers.

7.1.2 As such, AIs should identify and assess the specific risks of the mobile channel (including the relevant mobile platforms) they use and formulate relevant security measures to address these risks, in addition to other controls applicable to Internet banking accessed via personal computers.

7.1.3 Effective customer education programmes tailored for the use of mobile devices should be in place as well as ongoing efforts to identify fake Internet banking Apps, if applicable, and notify customers promptly.

7.1.4 Additional security controls should be implemented for AIs allowing their customers' mobile devices to receive or generate OTPs as the effectiveness of the 2FA may be weakened if the same mobile device could be used for (i) accessing Internet banking and (ii) receiving or generating OTPs.

7.2 Internet banking accessed via social media platforms or

other portals

7.2.1 When Internet banking can be accessed via social media platforms (including instant messaging services) or other portals, AIs may be exposed to risks such as (i) the risk of leakage of customer data due to insecure system interfaces or connections between the AIs' systems and those of the platforms/portals; (ii) the risk of system intrusion through any direct connections with the systems or security loopholes in the platforms/portals; (iii) reputation risk in any case where there are operational problems caused by the platforms/portals, thereby affecting the AIs' Internet banking; (iv) lack of clarity and potential confusion when handling customer disputes which may involve both the usage of Internet banking and the platforms/portals; and (v) potential cross-border issues if the platforms/portals are subject to laws, regulations or supervisory standards of overseas jurisdictions.

7.2.2 Before partnering with such platforms/portals, AIs should ensure that, among others:

(i) legal due diligence is undertaken to ascertain that any applicable local or overseas legal or regulatory requirements have been complied with (especially if AIs partner with overseas platforms/portals), including those relating to personal data privacy if customers' personal data would be transmitted to, or stored in, the platforms/portals. In addition, appropriate arrangements should be in place for ensuring customer protection such as when dealing with customer complaints and apportionment of liability for any financial loss of customers that may be caused by problems involving the platforms/portals; and

(ii) adequate security controls (e.g. in the areas of authentication, confidentiality, integrity, customer data protection and malware attacks) are implemented and independent assessment is performed so as to minimise the risk of intrusion into AIs' systems and networks through the

connections with the platforms/portals, and the risk of leakage of any customer data transmitted between the AI and the platforms/portals.

7.3 Self-service terminals

7.3.1 Among the various risks related to self-service terminals, the key operational risks relevant to AIs include:

(i) card skimming attacks;

(ii) fraudsters taking control of the terminals, such as by tampering with the terminals and/or implantation of malware, particularly on terminals using end-of-support software;

(iii) failure to detect and handle counterfeit banknotes for terminals (e.g. CDMs) allowing deposits of banknotes; and

(iv) disputes with customers caused by possibly confusing system processing of customer transactions [27] or incidents [28] related to transactions involving banknotes.

7.3.2 In order to mitigate the relevant risks, AIs should put in place, at the minimum, the following risk management measures:

(i) if cards are used as one of the factors for customer identity authentication in using the terminals, adequate security and controls should be implemented covering the issuance, activation, replacement[29] and loss of cards. In

[27] For instance, it might be confusing if a customer's account balance will be credited for some time even if no cheque has actually been deposited in a cheque deposit machine.

[28] These include, for instance, (i) when a customer leaves the ATM without taking the banknotes he or she has withdrawn; and (ii) when banknotes are stolen from a customer right after being dispensed from the terminal.

[29] For instance, if there is a change of the network operator(s)/card association(s) associated with the cards during the card replacement process, AIs should put in place appropriate arrangements to deal with possible enquiries from customers.

addition, chip-based authentication on chip cards[30] issued by AIs should be enforced for local ATM transactions. So long as the magnetic stripe is retained on a chip card to allow customers to use ATM services in locations outside Hong Kong that have not adopted chip-based ATM technology, the overseas ATM cash withdrawal capability for the chip card should be pre-set as deactivated and customers should be required to activate the capability and specify the activation period through appropriate channels (e.g. local ATMs, Internet banking, phone banking) before any overseas ATM cash withdrawal can be conducted. In addition, customers should also be given an option to set a lower withdrawal limit for overseas ATM cash withdrawal transactions;

(ii) keypad covers and anti-skimming devices (if the use of cards is needed) should be installed in terminals that require customers to input PIN for transaction authentication. Frequent patrols of terminals should be undertaken both during and after office hours in order to check the physical security of the terminals and to discover any suspicious devices attached to, or other abnormal status in respect of, the terminals. Furthermore, enhanced security measures should be implemented in response to information obtained about the techniques used in the latest threats related to card skimming, tampering with, or intrusion into, terminals;

(iii) for terminals allowing deposit of banknotes, careful assessment and selection of terminals should be performed having regard to, among other factors, their capability in detecting counterfeit banknotes and related test results. As vendors of these terminals would make

[30] These include pure debit cards, combo cards (i.e., credit cards linked with bank accounts) and pure credit cards. All the pure debit cards and combo cards issued by AIs have already been chip-enabled to support local ATM transactions. For pure credit cards, AIs should complete the replacement of non-chip-enabled cards by end-2015.

available system updates from time to time to enhance the capability of the terminals in detecting counterfeit banknotes, AIs should also put in place system controls or alternative arrangements to facilitate the timely and proper installation of these updates in all relevant terminals whenever there is a need;

(iv) sufficient audit trails (including system records and footage from closed-circuit television (CCTV[31])) of customers' transactions conducted through the terminals should be retained. Proper procedures and dual controls should also be implemented to reconcile the banknotes in the terminals against the records in the AIs' systems, and investigate any disputes with customers related to the use of the terminals. Sufficient guidance and training should also be given to staff handling disputes with customers so that appropriate responses will be given to customers, taking into account the relevant facts or investigation results. In addition, there should be adequate measures and effective arrangements related to replenishment or collection of banknotes in or from the terminals;

(v) AIs should adopt a risk-based approach to determining whether additional physical access controls should be implemented in unmanned service centres of self-service terminals so that only relevant customers would be generally given access into those centres. There should also be adequate measures to reduce the chance[32] of, and deal with, scenarios resulting in "unattended banknotes" being dispensed from the terminals; and

(vi) adequate consideration should be given to

[31] In general, AIs should install CCTVs for ATMs which are not located in secure areas such as lobbies of bank branches and any other locations assessed by AIs as low risk.

[32] For instance, AIs may consider the practicality and usefulness of measures suggested by the Police from time to time. These measures may include implementing notification alerts (e.g. flashing light, sound alert and advisory sticker) and standardizing the cash withdrawal sequence.

customers' experience and expectation when designing and implementing the relevant system processing related to self-service terminals so as to reduce the chance of confusion and customer disputes.

7.4 Phone banking

7.4.1 AIs should implement adequate customer identity authentication controls in their phone banking operations. When a customer calls in to inquire about the customer's bank account (e.g. balance or transaction history) or perform a transaction via the account, AIs should either use phone banking PIN or ask effective "challenge" questions to authenticate customers' identity. In general, "challenge" questions with answers that are readily available in the public domain (e.g. social networking websites) are less effective. Instead, AIs should consider asking a series of more difficult questions with static answers[33] or dynamic questions during the customer identity authentication process. Further, an authentication mechanism that uses different challenge questions between different phone banking authentication sessions, without disclosing all the questions in one session, is considered to be more effective. In addition, adequate controls should be implemented to minimise the risk that AIs' staff (or service providers) who ask the challenge questions and have access to the related answers of a customer would be able to impersonate the customer concerned using the information.

7.5 Contactless mobile payments

7.5.1 Given that payments are provided via contactless channels, contactless mobile payments usually entail certain specific risks such as (i) the risk of leakage of

[33] For example, customers are allowed to select "challenge" questions in advance from a list of available questions prepared by AIs and pre-set an answer for each of the selected "challenge" questions. In such cases, AIs should use a risk-based approach to following up cases of repeated failed attempts to address the risk of unauthorized access by fraudsters.

the customer's personal or credit card information through electronic pick-pocketing or eavesdropping in respect of the contactless/wireless traffic between the customer's mobile device and the payee; and (ii) the risk of loss or theft of the customer's mobile device, leading to fraudulent transactions.

7.5.2 In view of the above specific risks associated with contactless mobile payments, AIs should carefully assess the security risks of their proposed service and formulate relevant security measures before launching the service. At the minimum, AIs should ensure the service complies with any relevant minimum security standards issued by the banking industry associations from time to time as well as other relevant controls.

8. Fraud and incident management

8.1 Fraud monitoring and continuous intrusion detection

8.1.1 AIs should have a robust and effective automated fraud monitoring mechanism in place to detect, in a timely manner [34], suspicious Internet banking transactions and unusual activities ideally after taking into account their customers' Internet banking usage and behavioural patterns. For e-banking services other than Internet banking, AIs should still implement an appropriate fraud monitoring mechanism that can detect promptly suspicious transactions.

8.1.2 AIs should closely monitor trends and developments in emerging fraudulent techniques related to the use of e-banking channels, and regularly enhance or adjust their fraud monitoring systems whenever there is a need. During the process, AIs should take into account any fraud intelligence gathered from internal or external sources (e.g. from the industry, the Police or information security service providers).

[34] AIs with Internet banking services that are more important to the members of the public or the functioning of the financial systems of Hong Kong are generally expected to have a better capability of detecting potential Internet banking frauds in a timely manner.

8.1.3 AIs should assign sufficient designated staff with relevant expertise to promptly handle the alerts generated by their fraud monitoring mechanism if significant suspicious e-banking transactions or unusual activities are detected during or after office hours. AIs should also ensure that proper procedures and processes are in place for such designated staff to ascertain whether in fact any fraud might actually be being perpetrated via the suspicious transactions or activities identified. These processes may involve suspending the transactions temporarily and/or contacting the customers concerned through a reliable channel to verify the transactions or activities.

8.2 Incident response and periodic drills

8.2.1 Given that the risk of adverse incidents related to e-banking services cannot be completely eliminated, AIs should put in place formal incident response and management procedures for timely reporting and handling of different kinds of incidents (including suspected or actual security breaches, cyber attacks, frauds or service interruptions) affecting their e-banking services both during or outside office hours. The incident response and management procedures (which could be procedures applicable to the entire organization or specific to individual e-banking services) should allow AIs:

(i) to find out quickly the possible root cause of the incident (such as whether it arises from weaknesses in the AI's security controls) and assess the potential scale and impact of the incident (e.g. whether the incident is likely to affect other customers or even the customers of other AIs);

(ii) to, as soon as practicable, rectify or contain the damage to the AI's customers assets, data and reputation. The top priority should be to protect the interests of customers who have been or may be affected by the incident;

(iii) to escalate the incident promptly to the senior

management especially if the incident may result in reputation damage or material financial loss;

(iv) to notify promptly the affected customers and other affected AIs (so that they can in turn notify their affected customers) where appropriate;

(v) to collect and preserve forensic evidence as appropriate to facilitate subsequent investigation and prosecution of offenders if necessary; and

(vi) to perform a post-mortem review of the incident, covering the identification of the root cause and the generation of action plans for rectification actions needed (e.g. preventive and detective controls, mitigating controls).

8.2.2 A communication strategy[35] should be formulated by the senior management to ensure that consistent and up-to-date messages are conveyed to all relevant parties (e.g. customers, media and business partners) on a timely basis. In particular, AIs should proactively notify the customers affected, or likely to be affected, through the most effective means (including considering the possibility of making a press release[36]) and inform them of the key facts relating to the incident and the steps that customers may take[37].

8.2.3 Where the incident involves a disruption of critical e-banking service and may last for a prolonged period

[35] When handling a significant incident affecting a substantial number of customers, the AI concerned is likely to receive a large number of customer and media enquiries. It is therefore essential for the AI concerned to deploy swiftly adequate resources and communication channels (e.g. customer service hotlines) to handle such enquiries.

[36] There could be other relevant factors (e.g. the need to keep the public informed may need to be weighed against the relevant legal considerations, including where appropriate whether a press release may prejudice any ongoing criminal proceedings or any investigation) that the AI should also take into account. The important point is that the actions taken to keep the customers and, where appropriate, the public informed of a significant incident should form an integral part of the incident response and management capability of AIs.

[37] For example, any estimated service resumption time and, where applicable, how customers can protect their interests (e.g. apply for compensation for any losses incurred by the disruption).

of time, AIs should consider making a press release where the situation so warrants, such as when such a press release will be a demonstrable faster or more effective communication means than individual notifications[38]. In particular, an AI is expected to issue a press release (or make a similarly effective notification) shortly after the commencement of any disruption to its critical e-banking service that could affect a significant number of customers if the AI does not have reasonable confidence that the service can be resumed in the near future.

8.2.4 AIs should formulate, and regularly undertake practice drills to test their incident response and management procedures to ensure sufficient management oversight, adequate capacity and effective incident management capability.

8.2.5 Once an AI becomes aware that a significant incident (including any suspected or confirmed fraud case relating to e-banking) has occurred, the AI concerned should notify the HKMA promptly in accordance with the relevant arrangements set out by the HKMA from time to time.

9. System availability and business continuity management

9.1 Service level of e-banking for customers

9.1.1 It is important that e-banking services are delivered on a continuous basis with reasonably fast response time, taking into account customers' general expectations. In this connection, AIs should ensure that resilience capability, capacity planning and performance monitoring process of their e-banking systems (particularly for those systems supporting time-critical services such as Internet securities trading services) are commensurate with the scale and nature of their e-banking services.

[38] Individual notifications may include, for instance, calling the affected customers or sending SMS messages to the affected customers.

9.1.2 AIs should ensure that their controls relating to system resilience and their capacity planning for e-banking cover all systems (e.g. their Internet banking system and any connected core banking systems) and infrastructure components (e.g. Internet infrastructure, associated hardware, equipment and software used in relation to the networks and interfaces with the internal systems) within their institutions as well as those of any relevant service providers (whether within the same banking group or outside parties) to ensure stability, performance and continued system availability of e-banking to the relevant customers.

9.2 Capacity planning

9.2.1 A thorough review of the system capacity of the relevant systems and infrastructure should be conducted from time to time to identify any potential weaknesses that may affect the stability and performance of e-banking. Regular capacity planning and performance reports should be produced for senior management's attention. Any necessary enhancement measures to rectify the identified weaknesses should also be implemented promptly to avoid possible system instability.

9.2.2 Guidelines for capacity planning should be established, which clearly set out, among others, system utilization threshold and corresponding precautionary measures (e.g. to step up monitoring of system utilization and perform system upgrades when the peak utilization level reaches the predetermined capacity levels). A capacity planning methodology should also be developed to help estimate future capacity requirements (taking into account the trend analysis of system utilization, projection of customer growth and transaction volume, progress of system capacity upgrades, system performance issues encountered, etc.) and turn business requirements into IT capacity plans. The methodology should take into account capacity implications of any new business initiatives and anticipated growth of the utilization of the relevant e-banking services. In particular, for time-critical e-banking such as Internet securities trading services,

the capacity plan should take into account the possibility of a sudden upsurge in transactions during particular timing or situations.

9.2.3 It may be prudent that a fast-track software and hardware procurement process is formulated, which includes making prior arrangement with the related software and hardware providers to allow upgrading of system capacity within a short period of time when such a need arises. In any case, adequate end-to-end system stress testing should be conducted with adequate coverage of all relevant systems and infrastructure components to identify potential performance bottlenecks in advance.

9.3 Performance monitoring

9.3.1 Regardless of the scale of e-banking, an automated performance monitoring and alert system, which covers all critical systems and infrastructure components supporting e-banking, should be in place so that any potential system interruption or performance degradation (for Internet securities trading services, the monitoring should cover at least system capacity utilization and response time of critical user activities such as customer's identity authentication, stock holding enquiry and buy/sell order placements of securities) both during or after office hours could be detected and handled by designated staff in a timely manner.

9.4 System resilience

9.4.1 AIs should ensure that there is no single point of failure in the systems/infrastructure components (e.g. through proper implementation of high availability server clusters, multiple network connections, redundancy of critical hardware or equipment), nor unnecessary connections or dependency upon less critical systems. It is important that the actual effectiveness of the resilience of the system should be properly verified and tested.

9.5 Controls for coping with system disruptions

9.5.1 AIs' IT function should establish a service level agreement with business lines covering availability of e-banking systems. Against this system availability benchmark, AIs should maintain and service the relevant IT facilities and equipment in accordance with industry practices and suppliers' recommended service intervals and specifications. Moreover, AIs should formulate and undertake regular practice drills to test the relevant IT disaster recovery plan and procedures to ensure that their e-banking services can be resumed within a short period of time and in accordance with the AIs' business recovery requirements, taking into account the duration required for trouble-shooting, problem fixing and switching over to the back-up e-banking systems if needed.

9.5.2 AIs should take appropriate measures having regard to common issues that could lead to disruptions of e-banking. Moreover, AIs should implement proper precautionary measures before and during scheduled maintenance or drills (see Annex C for examples of precautionary measures).

9.5.3 Moreover, AIs should implement adequate controls to promptly detect and respond to the threats posed by distributed denial-of-service (DDoS) or other cyber attacks that could directly or indirectly cause disruptions to e-banking systems. These controls should be validated (e.g. testing at point of service activation or a production-like system environment) and periodically reviewed to ensure their ongoing effectiveness against any emerging techniques in DDoS attacks.

9.5.4 AIs should implement sufficient and effective alternative service delivery channels to ensure e-banking services can be provided continuously to customers as far as appropriate. In particular, if an Internet banking system is temporarily not accessible, AIs should ensure that their other service channels such as phone banking and branches have the capacity and related operational procedures to provide an acceptable level of service to their customers,

taking into account the anticipated customers expectation, in relation to critical functions (e.g. funds transfers, securities trading).

———————————

Contents	Glossary	Home	Introduction

Annex A: Items to be reported in independent assessment

A.1 In general, a report of independent assessment should cover at least the following items:

A.2 Period of assessment

A.2.1 The report should state when (a particular snapshot or a period of time) and at what stage of the preparation for the launch or major enhancement of e-banking service (e.g. design stage or testing stage of the e-banking system) the independent assessment was conducted.

A.3 Scope & approach

A.3.1 The report should describe the scope of, and approach adopted in, the assessment. In particular, the scope should mention the applicable subsections of this module and other applicable HKMA and industry guidelines and circulars that are relevant to the underlying financial services and the electronic delivery channel concerned, and the reasons for any material exclusion of applicable guidance. Furthermore, the report should set out what controls and system components, as well as what portion of the AI's internal networks and network equipment were covered in the independent assessment, against the scope as identified above.

A.3.2 The assessor should perform more thorough review and verification as appropriate on areas of higher risk. For AIs offering e-banking services of higher risk such as Internet banking and any financial services delivered over the Internet or via a wireless network (covering enquiry-only services and relevant outsourced systems), they should consider including in their independent assessment penetration tests.

A.4 Summary of assessment results

A.4.1 The report should include the following information:

- findings identified in the assessment, including any serious deficiencies identified during the course of the assessment even if such issues have been rectified before the report is issued. There should also be explanations of the risk implication of the findings, and the assessor's assessment of the level of risk associated with the findings;

- recommendations of the assessor to assist in addressing the findings; and

- management response to the findings and recommendations, including the actions taken or to be taken to address the findings, the target date for completing the actions, and any interim measures taken or to be taken (the management response may be included in a separate report).

A.4.2 If the management adopt alternative methods to address the weaknesses identified by the assessor or if the assessment discloses material weaknesses, the AI normally needs to request the assessor or another independent expert to perform a follow-up review of the matters concerned.

Annex B: Controls related to account aggregation service

B.1 Acceptable business models

B.1.1 In principle, an AI should ensure that any AAS partnering institution, which allows operation of its customers' accounts maintained in that AAS partnering institution, is a banking institution. Moreover, only the following types of bank account are allowed to be included in the AAS offered:

- for a personal customer, he or she can only aggregate bank accounts that belong to him/her individually or jointly with other individual(s), in the case of an "either one to sign" joint account; and

- for a business customer, it can aggregate only bank accounts of the same company, or of the companies within the same group, or of the same person/entity who owns all or part of such companies (including joint venture companies). Proper authorization such as a Board resolution should also be obtained from the relevant companies. If a business customer does not have any legal or affiliate relationship and it applies for AAS, AIs should carefully assess whether there is a genuine and legitimate business purpose for the service and satisfy themselves that the risk of abuse through the conduct of suspicious and illegal activities (e.g. money laundering or terrorist financing) is low.

B.1.2 In addition, AAS should only be provided by an AI in co-operation with a banking institution that is closely associated with it, which includes: (i) an overseas branch / its head office; and (ii) a local or overseas subsidiary, affiliated bank or the parent bank. As providing AAS in co-operation with other institutions which the AI does not have a close association involves complex legal issues, the AI should not provide AAS in those circumstances unless:

- there is no direct connection between the computer systems and networks of the institutions involved. Instead, data transmissions between the institutions are conducted via proven interbank financial messaging networks (e.g. SWIFT); and

- a proper bilateral agreement covering the rights and

obligations (including those related to the matters mentioned in this module) of both parties between the AI and the partnering institution is in place. Before entering into such an agreement, adequate due diligence should be conducted on the partnering institution and approval should be obtained from senior management before establishing the relationship with such an institution.

B.2 Compliance with all relevant local or overseas laws and regulations

B.2.1 If the AAS in question involves funds being taken from a local bank account of an AI and deposited into an overseas account of the partnering institution through the AI's Internet banking without requiring the customers to login to the overseas institution's Internet banking service, appropriate legal advice should be obtained to ensure that the service or the partnering institution will not contravene the Banking Ordinance, including among others:

- Section 12(1) in respect of prohibiting the carrying on of the business of taking deposits in Hong Kong by any entity which is not an AI;
- Section 92 in respect of any advertisements posted on the Internet for soliciting deposits from members of the public in Hong Kong;
- Section 97 in relation to the use of the term "bank" and section 97A in relation to the issuance of false statements as to authorized status; and
- Section 46 in relation to the establishment or maintenance of a local representative office in Hong Kong by an overseas bank. One relevant consideration, among others, is whether the AI undertakes so much of the representative, liaison and/or promotional functions of the overseas institution that it has become an office of the latter in Hong Kong.

B.2.2 In addition, the AI should check with the partnering institution whether it is required to obtain an approval from its regulatory authorities before AAS is launched. Effective risk management controls should be implemented to comply with all applicable relevant regulatory requirements especially if overseas jurisdictions are involved.

B.2.3 In addition, the AI should assess the associated money laundering and terrorist financing risk if AAS supports cross-border funds transfers, and ensure compliance with the Anti-Money Laundering Ordinance (AMLO), the AML Guideline and other relevant guidance issued by the HKMA from time to time, as well as the requirements set out by the overseas jurisdictions concerned.

B.3 Data privacy and customer protection

B.3.1 If AAS involves transfer of customers' personal data between local and overseas locations, the AI should ensure compliance with applicable data privacy laws and regulations in both the local and the overseas locations concerned. For instance, the AI should review whether it needs to obtain written consents from customers if their personal data are to be transferred to an overseas location and/or maintained overseas.

B.3.2 Due to the involvement of multiple parties in AAS, complications may arise in handling cross-border customer complaints, apportionment of liability and settlement of compensation claims for customers' financial loss arising from fraud cases and system failures, particularly for business models involving an overseas institution or an institution that is less closely associated with the AI. The AI should establish appropriate customer complaint handling procedures and internal guidelines for apportioning liability and settling any customers' claims for financial loss, in addition to issuing fair and balanced terms and conditions in relation to customer protection.

B.4 Security controls

B.4.1 AAS will inevitably tend to expose the AI to a higher security risk, as it will increase the number of access points to the AI's systems and network especially if the security controls of the partnering institution or the network connections between entities are inadequate.

B.4.2 To address the increased security risk, the AI should satisfy, among others, the following requirements:

- the security controls of the relevant systems and infrastructure of the partnering institution should be adequate, having regard to the AI's own baseline requirements on IT security. In cases where a customer is

able to initiate, through the partnering institution's Internet banking services, high-risk transactions or small-value funds transfers on the customer's bank account maintained in the AI via AAS, the partnering institution should comply with the applicable requirements stipulated in this module (particularly subsections 4.2, 4.3 and 6.1) as well as any other relevant HKMA guidelines, or similarly stringent requirements. If the partnering institution allows a customer to initiate, without appropriate 2FA authentication controls, funds transfers from the customer's bank account maintained in the AI to an aggregated bank account maintained in the partnering institution, the AI should implement mitigating controls (e.g. notifications sent to customers as per subsection 4.3) to address the risk that fraudsters might impersonate the customer via the partnering institution;

- effective controls should be established to ensure that the AI's customer data are kept confidential and will not be divulged to any person without the customer's consent. In particular, the AI's customer and transaction data should be properly segregated from those of the partnering institution and protected from unauthorized access by staff of that institution; and

- the independent assessment for evaluating the implementation of the above-mentioned requirements of the partnering institution should be performed by trusted assessors with the necessary expertise (see subsection 3.3.1(iii)). For instance, the assessment could be performed by the partnering institution's external or internal auditor acceptable to the AI.

Annex C: Examples of precautionary measures before and during scheduled system maintenance or drills

C.1 Management oversight and monitoring over the scheduled system maintenance/drills and related preparation/follow-up actions;

C.2 Proper preparation (e.g. proper maintenance/recovery procedures, testing of the changes with satisfactory results, well-tested fall-back procedures to cater for any exceptional and unexpected situations) before the maintenance/drills;

C.3 Live test after the scheduled system maintenance/drills to ensure the effective operation of the relevant services;

C.4 Adequate advance notifications to relevant customers about the service outage (e.g. the services that would be affected and the duration of the impact);

C.5 Arrangements that ensure prompt responses to customer and media enquiries that may arise during or after the affected period; and

C.6 Procedures for proper and timely escalation to senior management and public communication plans to cater for exceptional and unexpected situations (e.g. the scheduled system maintenance/drills cannot be completed in time and the services cannot be resumed as scheduled).