FAQs for SPM TM-E-1 “Risk Management of E-banking” (V.2~~1~~ – 19~~24~~.04~~10~~.24~~19~~) [CONFIDENTIAL]

FAQ No.	Question	Answer
Subsection 1.2 – Types of e-banking		
1.	Are financial services provided to corporate customers via host to host connectivity, other than through the Internet or wireless network, regarded as e-banking services?	Financial services provided to corporate customers via host to host connectivity, other than through the Internet or wireless network, are generally not regarded as e-banking for the purpose of this SPM module.
Subsection 3.3 – Independent assessment and penetration tests		
1.	What criteria should AIs take into account when determining whether an e-banking enhancement is a major enhancement?	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.
2.	Who may conduct an independent assessment? Is the AI allowed to leverage on previous assessments or assessment reports provided by the relevant service providers of the outsourced activities when conducting the independent assessment?	So long as the assessors have the necessary expertise in the relevant risk management practices, and are independent from the parties that design, implement or operate the e-banking services, the assessors could be any function of the AI or its group, particularly the second line of defence (e.g. risk management function) or the internal audit function or, an external skilled person acceptable to the AI (e.g. including those independent assessors appointed by external service providers) or any other third-party consultants. 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. In addition, the assessors may leverage the results of previous independent assessments performed or independent assessment reports commissioned by external service providers, provided that the scope (e.g. controls, systems or processes) covered by such independent assessments is relevant to the new

		independent assessment, despite technology advancement or emergence of new threats. Whenever there is a need, the assessors should perform supplementary assessment to address any issues that have not been covered in the previous assessment or the outcome of the previous assessment may no longer be valid. The assessors should have a clear opinion on the e-banking initiative being assessed, regardless of whether or not the assessors may have taken into account the results of previous independent assessments.
3.	Can independent assessment reports be submitted by phases, in line with the phased rollout of e-banking initiatives?	It is acceptable for AIs to submit independent assessment reports by phases so long as the results submitted cover the e-banking services rolled out in a particular phase.
4.	What are the expectations on the scope of independent assessment from the fraud risk perspective?	The independent assessments of e-banking initiatives should cover an evaluation of the adequacy of the relevant controls (including fraud monitoring, customer authentication, and the relevant online processes and customer journeys) to manage the associated fraud risks, taking into account the latest fraud techniques and threats. In particular, the evaluation should evaluate whether the relevant online processes and customer journeys, etc. are adequate in preventing frauds and whether the AI’s fraud monitoring and remediation process are sufficient to promptly detect and follow up fraud attempts or actual fraud scenarios in a timely manner even after office hours. The evaluation should also cover areas such as the mechanism for monitoring emerging fraud techniques and threats, and retention and provision of sufficient information for law enforcement purpose. Although the latest fraud techniques and threats evolve over time, the assessment may need to cover the following fraud scenarios, among other fraud scenarios, based on past fraud threats: (i) A fraudster takes over a customer’s account by abusing certain processes of the e-banking services (e.g. online PIN reset and mobile phone number changing services) after the fraudster compromises

Commented [YPK1]: This revision aims to incorporate the requirements of the Operational and IT Incidents Watch “Recent developments in malware scams” dated 22 Dec 2023.

		the customer’s email account and obtains the customer’s personal information (e.g. mobile phone number). (ii) A fraudster is allowed to have many Internet banking login attempts to confirm the validity of user names and then get hold of a list of valid user names so that the fraudster can use the list to try compromising the customers' Internet banking accounts. (iii) A fraudster is permitted to have many attempts for answering the security questions in the password reset process and the answers can be easily guessed even randomly or available in public domain, social media or other sources. (iv) A fraudster takes advantage of a customer's mobile device being infected with malware to bypass authentication controls across various channels (e.g. phone banking, Internet banking and e-wallet).
Subsection 4.1 – Authentication of customers		
1.	For AIs allowing customers to use their account information (e.g. user ID) of social media platforms for receiving notifications sent by AIs via these social media platforms, whether two-factor authentication (2FA) is required if the customers are allowed to online register or change this account information?	In general, as a customer’s account information (e.g. user ID) of a social media platform may be used by an AI to send important notification to the customer, online registration or changes (including binding/linking of the social media platform’s account with the Internet banking account) of such information are regarded as high-risk transactions, which is subject to 2FA. That said, it may be acceptable if the AI adopts 1FA authentication method for this purpose provided that such a notification channel is only a supplementary channel, on top of the minimum notification requirements set out in the module. For the avoidance of doubt, if the channel subsequently becomes one of the channels to meet the minimum notification requirements, the online registration or changes of such information should then be subject to 2FA. Despite the above requirements, it is prudent that displaying the account information of these social media platforms on the Internet banking screens should still be regarded as high-risk transactions in all cases unless only partial information is disclosed. This is to help reduce the chance that such account information may be used by fraudsters to circumvent other security controls.

Commented [YPK2]: This revision aims to incorporate the requirements of the Operational and IT Incidents Watch “Recent developments in malware scams” dated 22 Dec 2023.

2.	Given that online registrations of third-party payees for high-risk funds transfers are classified as high-risk transactions, which are subject to two-factor authentication (2FA). However, as AIs may regard small-value funds transfers as not being high-risk transactions, can a payee be online registered for small-value funds transfers without 2FA?	Given the inherent fraud risk associated with small-value funds transfers, the spirit of TM-E-1 is that multiple layers of preventive and detective controls (including effective notifications) should be put in place by AIs before they offer e-banking services that allow small-value funds transfers. If an AI intends to offer an e-banking service that allows an online "registration" of a payee for small-value funds transfers without 2FA and effective notification is not subsequently sent to notify the payer/transferor after a small-value funds transfer to that "registered" payee has been initiated, this service is not in line with the spirit of TM-E-1. As such a service will expose the payer/transferor to undue fraud risk, it should not be launched. Hence, the HKMA would like to clarify that any payee who has been "registered" online without 2FA (or the so-called "registration" has not been carried out via a secure channel) should be regarded as an "unregistered payee", and an effective notification sent to the payer/transferor should therefore be required after each small-value funds transfer is initiated.
3.	What is the expectation of the HKMA regarding risk management of biometric technologies?	Technologies for biometric authentication are evolving and varying standards/certifications may be adopted by different parties for evaluating biometric authentication technologies. Hence, AIs are expected to develop the required knowledge and keep abreast of the emerging threats and risk management practices before implementing biometric authentication methods. As a general principle, the use of biometric authentication should be commensurate with the risks of the relevant transactions and services (note 1) and AIs are expected to put in place effective risk management measures, particularly those for preventing the leakage of customers’ biometric data. Depending on the biometric indicators used and the technologies involved, AIs’ evaluation and implementation need to take into account, among others, the following matters. A. Maturity of the technologies

AIs should carefully consider factors such as the track records (e.g. fraud rates) of the technologies and the service providers, key security vulnerabilities or attacks (e.g. presentation attacks) and counter-measures that can be implemented (e.g. liveness detection, retry attempt controls), and any quantifiable indicators on the accuracy or error rates about the authentication results (e.g. false acceptance rate and false rejection rate). To this end, AIs should take into account the relevant test results, if applicable, and assessment performed by themselves or other parties with the necessary expertise.

B. Protection of biometric data

As biometric data are highly sensitive data of customers, AIs should ensure that those data are adequately protected during transmission to/from, and storage in, the AI’s internal system and network. AIs should choose those technologies that adequately minimise the risk of any leakage of customers’ biometric data, even if such data are stored in customers’ devices and then the devices are lost or compromised, say, by malware. The protection measures should generally include:

(i) Proper transformation of biometric data before being transmitted or stored such that even if the transformed data are leaked, it would be impracticable to reconstruct the biometric data of the customers concerned from the leaked data;

(ii) Safeguard of any customers’ biometric data stored in the AI’s internal system and network by measures that are as stringent as sound industry practices adopted for protecting customers’ other highly sensitive information (such as customers’ login credentials), unless the above-mentioned transformation process and related security controls (e.g. key management) are able to serve the same purpose. Relevant requirements include, among others, those

		stipulated in subsection 5.1.1 of the SPM module regarding the protection of customers’ highly sensitive information; and (iii) Other mitigating controls for reducing the risks arising from any leakage of customers’ biometric data, given that customers basically cannot change their biometric data. AIs also need to comply with any relevant codes of practice issued or approved by the Privacy Commissioner for Personal Data giving practical guidance on compliance with the Personal Data (Privacy) Ordinance (such as Guidance on Collection and Use of Biometric Data). For such compliance, AIs should seek clarification from the Privacy Commissioner for Personal Data whenever there is a need. C. Enrolment of and withdrawal from biometric authentication methods As biometric authentication methods entail the provision of highly sensitive biometric data by customers, AIs should allow customers to opt-in the enrolment of such a method only upon their consent after proper disclosure about the method, the associated risks (e.g. the risks and implication related to any leakage of biometric data) and precautions expected (e.g. customers may need to report loss of their mobile devices to AIs) to the customers. If the biometric authentication method will be subsequently used as one acceptable factor for authenticating the customer’s identity for effecting high-risk transactions of e-banking services, the enrolment or any change (if technically feasible to detect such change) of the biometric authentication method (note 2) (e.g. change of customers’ fingerprints used for authentication) should be classified as a high-risk transaction and hence subject to two-factor authentication (2FA) (note 3) and customer notification requirements, or through other secure channels with adequate identity check. This

		classification is intended to reduce the risk of unauthorized high-risk e-banking transactions effected after the enrolment or change of biometric authentication without the customer's consent. When a customer decides to withdraw from using the biometric authentication method, the AI should delete the customer's biometric data (including transformed formats) stored by the AI (including those in the AI's mobile App and internal system and network) in a timely and an effective manner, taking into account the AI's retention policy, if applicable and in line with the relevant data retention requirements (such as the Guidance on Collection and Use of Biometric Data). If the biometric data cannot be deleted by the AI (e.g. the biometric data are stored in the customer's device), the AI is expected to advise the customer so, the possible implications and suggested measures the customer can take, say, during the disclosure of the enrolment process and when the AI sends acknowledgement to the customer to confirm the withdrawal. Note 1: AIs should take into account of this FAQ when launching biometric authentication for different banking services (e.g. branch services). AIs should perform appropriate risk assessment before deciding whether biometric authentication should be implemented for other banking services. Note 2: The enrolment or any change of the biometric authentication may be effective immediately after the customer's identity has been properly authenticated by the AI, so long as the AI has assessed that this is commensurate with the risks of the relevant banking transactions. Note 3: For the avoidance of doubt, a biometric authentication method enrolled without 2FA and other controls applicable to high-risk e-banking transactions should not be generally regarded as one acceptable factor for authenticating the customer's high-risk e-banking transactions, including the aforementioned enrolment process.

4.	Display of full contact details (e.g. correspondence address) that may be used by customers to receive important information or monitor their accounts’ activities on the Internet banking screens would be regarded as high-risk transactions and subject to two-factor authentication (2FA). When an e-statement contains correspondence address, should AIs implement 2FA for the access of e-statements via Internet banking?	While the aforementioned 2FA requirement is to reduce the risk that fraudsters can intercept important documents or information, the banking industry is of the view that the display of correspondence address on the Internet banking screens is less sensitive and risky than other contact details. In this connection, the HKMA considers that it would be acceptable for an AI to allow its customers to access the e-statements containing correspondence address in Internet banking without 2FA (or only selected customers based on their preference) after the AI has assessed and managed the relevant risks.
5.	What are the specific security measures that need to be implemented by AIs for the use of one-time-password (OTP) or digital certificate as two-factor authentication (2FA)?	In general, AIs are expected to ensure that the authentication factors used are reliable, effective and secure. Specifically, AIs are suggested to implement the following security measures. (1) One-time password (OTP) (a) An OTP can be regarded as a second factor "something the customer has" for customer authentication only if the OTP will expire within a short period of time. AIs should ensure that the period of validity of the OTPs is reasonably short (i.e. sufficient but not excessive) and the OTPs solution is secure, taking into account the channels for communication and the risk that the OTPs could be intercepted. Hence, it would be acceptable for an AI to determine a reasonable period of validity of OTPs which is commensurate with the result of the AI's risk assessment, taking into consideration factors such as the nature and sensitivity of the transactions to be authenticated by the OTPs, nature of the OTPs adopted and other security

		controls implemented. As a reference, the banking industry participants have adopted for many e-banking transactions that the period of validity of SMS OTPs should not exceed 100 seconds based on their own risk assessment. (b) AIs are expected to implement sound key management practices to safeguard the secret codes (also known as "seed values") for generating the OTPs; (c) If the OTPs are sent to customers via SMS, AIs are expected to implement controls with the relevant mobile network operators in Hong Kong to deliver such SMS OTPs originating from the AIs to the registered mobile phones of the customers concerned regardless of whether the SMS forwarding service in respect of these mobile phone numbers has been activated; (d) With respect to the SMS message containing the OTP, AIs should ensure that the details of the transaction are prominently displayed before the OTP, including the transaction type, transaction amount and partial information about the account number or other identifiers of (e.g. mobile phone number) of payee if relevant. The customer should be reminded to review the accuracy of the transaction details prior to entering the OTP to initiate the high-risk transaction; (e) In cases where repeated invalid OTP authentication attempts are identified, AIs are expected to implement appropriate controls to prevent potential attacks (e.g. brute-force attacks); and (f) AIs should conduct regular assessment on the adequacy and effectiveness of the OTP adopted for customer authentication, taking into account the latest hacking techniques and security threats (e.g. SIM swap scam related to SMS OTP) and implement appropriate mitigating measures if needed. (2) <u>Digital certificate</u> AIs are expected to ensure that the digital certificate and its associated private key are non-duplicable and stored in a secure manner. For instance, as it would be more secure if the digital certificate is retrievable

		by a customer’s personal computer or mobile devices only when the customer needs to make use of the digital certificate for accessing e-banking services, AIs should avoid installing the digital certificate directly on the customer’s device unless adequate and effective measures are in place to ensure that the digital certificate is stored securely on the devices and impracticable to be replicated. In which cases, customers should be reminded to remove the media storing the digital certificate from their devices after the certificate is used for accessing the services.
6.	What is the expectation of the HKMA for opening an Internet banking account over the Internet and changing contact details?	AIs should ensure that effective controls are in place to minimise the risk that Internet banking accounts are opened by fraudsters without the knowledge of the genuine customers. If customers are allowed to open Internet banking accounts over the Internet, the controls should be effective in authenticating the identity of the person opening the account against the customer he or she claims to be and facilitating early detection of unauthorized opening of such an account by the customer concerned, taking into account possible and latest fraud techniques. In cases where a customer is allowed to input the PIN of the customer’s credit/ATM cards or phone banking account, and credit card/account number for opening an Internet banking account over the Internet, the AI should implement adequate controls over the resetting or reissuing of the PIN and controls for addressing the risk of repeated unauthorized attempts by fraudsters to open Internet banking accounts. AIs should be cautious when mailing important documents (e.g. new passwords) to a recently changed correspondence address. AIs should implement effective monitoring mechanisms to detect any suspicious online transactions shortly after a change of the customer’s contact details.
7.	Apart from high-risk funds transfers and transactions set out in subsection 4.1.4 of SPM	Apart from high-risk funds transfers and transactions set out in subsection 4.1.4 of SPM TM-E-1, high-risk transactions also include:

	TM-E-1, are there any other examples of high-risk transactions?	(i) online registrations of third-party payees or– high-risk merchants for high-risk funds transfers; (ii) online binding of an e-banking account with a social media account (which include an instant messaging account) of the customer so that the customer can make use of his or her social media account for receiving important notifications from AIs or acting as one factor of customer authentication when accessing the customer’s e-banking account (note 1); (iii) online binding of a customer’s bank account or payment card with his or her contactless mobile payment App; (iv) increases of the transaction limit(s) through online channels; (v) online changes of contact details (e.g. e-mail address, correspondence address, mobile phone number or other contact phone numbers) that are used by the customer to receive important information (e.g. one-time password (OTP) or notifications sent by AIs) or monitor the activities in the customer’s accounts; (vi) display of the above-mentioned contact details on the screens (e.g. screens for Internet banking) unless (a) only partial information is disclosed, as such information may assist fraudsters in circumventing other security controls; or (b) only correspondence address is disclosed (note 2); and (vii) administration of Internet banking user accounts (e.g. user account creation) in business Internet banking. Note 1: AIs should assess and evaluate whether adequate and effective controls are implemented in the relevant social media platform against potential fraud scenarios (e.g. account-takeover frauds) before relying on the binding of the social media account as a factor of customer authentication. Note 2: AIs may choose to allow Faster Payment System (FPS) payees to generate a QR code containing the payees' contact details (e.g. email address, mobile number) via their mobile banking Apps so that a

		payer can scan the QR code to facilitate the input of the payee contact details for FPS payments. If the contact information embedded in the above-mentioned QR code could be easily retrieved by a standard QR code scanner, there is a risk that a fraudster can gather a customer's email address/mobile number in the event that he or she has already obtained the customer's Internet banking user ID and password. Under this circumstance, this type of QR code generation function should be considered as high-risk transaction in principle. Having said that, an AI planning to launch such a QR code generation function may adopt alternative control arrangements so long as it can effectively mitigate the above-mentioned risk.
8.	What is the expectation of the HKMA for using device binding as an authentication factor?	One of the industry practices for device binding involves the binding of one or more unique and hard-to-spoof identifier(s) (e.g. a unique cryptographic key) associated with the customer’s identity (i.e. the customer’s Internet banking account) with the customer’s device such that the identifier(s) is/are stored securely on the device and hence the device bound with these identifiers could be recognised by the AIs’ system(s) for authenticating the customer. For the purpose of this FAQ, these unique and hard-to-spoof identifiers are called “binding elements”. The controls over device binding process and the protection of the binding elements should be effective. Depending on the design of the device binding solution and the technologies involved, AIs are generally expected to adopt the practices listed below. AIs may also implement other control measures that the AIs consider to be as effective as those listed below: (a) Adequate controls should be in place to minimise the risk where a fraudster impersonates a customer to bind the fraudster’s own device, instead of the customer’s device, with the binding element(s) associated with the customer. Hence, AIs should implement proper controls to authenticate a customer’s identity before the binding element(s) is/are bound with the device

		designated by the customer, and to reduce the risks of interception by fraudsters and leakage of sensitive customer data or binding elements; (b) AIs should also inform customers of the steps to be taken by customers to “unbind" their devices (e.g. due to change or loss of devices, withdrawal from binding the devices). Controls should be in place for revoking the binding between the binding element(s) and the customer’s device in a timely manner to reduce the risk that the device would be used by fraudsters for accessing the relevant e-banking services before the binding is revoked; and (c) If the binding process can be done online and the device bound with the binding element(s) will be used as one acceptable factor for authenticating the customer’s high-risk e-banking transactions, the binding process itself should be classified as a high-risk transaction and hence subject to 2FA, the relevant customer notification requirements and other applicable control requirements. In addition, AIs should implement effective measures to strengthen the security of device binding taking into account phishing and other relevant risks. These measures, include, among others, (i) deferring the execution of the binding/re-binding of devices for a reasonably long period, (ii) adding an extra layer of authentication (e.g. SMS OTP) for the first (and even a few subsequent) high-risk transaction(s) after the deferred period, and/or (iii) adopting authentication factors less vulnerable to phishing (e.g. facial recognition for device binding). This safeguard is intended to reduce the risk of unauthorized high-risk e-banking transactions effected after a fraudster binds his device through online binding process~~ without 2FA~~. Effective measures should be in place to protect the security of the binding elements. These measures normally include:

Commented [YPK3]: Explanatory Note

This revision aims to incorporate the requirements of the Operational and IT Incidents Watch “Staying vigilant against phishing attacks” dated 10 Feb 2023 in relation to phishing attacks involving unauthorized device binding and fund transfers.

		(a) AIs should adopt binding element(s) that is/are unique in nature and can be uniquely associated with the relevant customer’s identity; and (b) The binding element(s) should be hard-to-spoof, stored securely on the devices and impracticable to be replicated for use, so as to reduce the risk that the binding element(s) is/are replicated or transferred out of the bound device by fraudsters for use on another device owned by fraudsters. AIs should take into account risks associated with specific types of devices (e.g. security vulnerabilities, the risk of malware and malicious Apps that might potentially capture binding elements stored on the devices) to determine whether only certain types of devices are allowed for device binding. It would also be prudent for AIs to adopt the controls (e.g. jailbreak/root detection, checking of device platforms) stipulated in the E-banking SPM in their binding solutions involving mobile devices regardless of whether high-risk transactions are allowed through the mobile devices.
9.	Are there any sound practices on security controls for AIs allowing the use of soft token on customers’ mobile devices?	As there are different methods in the market for developing soft token, AIs are expected to duly assess the technical features and security controls (e.g. jailbreak/root detection, anti-tampering capability, sandboxing feature, cryptographic mechanism, device binding, etc.) prior to implementing the soft token and periodically thereafter, having regard to the emerging cyber threats (e.g. malware attacks targeting customers’ devices, malware attacks that exploit legitimate features or permissions, say, screen mirroring, recording, overlay, accessibility service, etc., for malicious usage). The use of soft token on customers’ mobile devices also exposes AIs and customers to similar risks as using SMS OTPs, especially in case of compromised OTP seed or generation algorithm. In this connection, AIs allowing the use of soft token on customers’ mobile devices should also implement additional security controls applicable to OTP where appropriate as set out in FAQ #5 of subsection 4.1.

		Apart from the aforementioned control principles, AIs are expected to put in place device binding controls (See FAQ #8 of subsection 4.1) when implementing soft token.
10.	What is the technology-risk-related expectation of the HKMA for remote customer on-boarding services offered by AIs?	Before an AI engages in remote account onboarding services via technology solutions, the senior management should recognise that any ineffective remote account opening mechanism would expose the institution various risks including, among others, to a higher level of money laundering / terrorist financing risk (note 1) and fraud risk (e.g. fraudsters syndicating remotely-opened accounts). In this connection, in using technology to facilitate remote customer on-boarding process, senior management of AIs are expected to ensure effective technology risk management controls are implemented over these processes, including the adequacy of their customer identity verification mechanisms and the robustness of the technologies employed. In particular, AIs are expected to put in place the following controls, or other similarly effective alternative controls. A. <u>Governance</u> Governance process should be in place to ensure that the remote account onboarding processes are duly reviewed and approved by the senior management of the AI, demonstrating clear accountability of the senior management and well-defined responsibilities of the relevant functions (e.g. the business line or technology function) with regard to the robustness of the remote account onboarding services. Any material limitations of the related technologies (including material gaps as compared with ordinary account onboarding processes, such as in terms of robustness of identity verification) should be clearly communicated with the AIs’ senior management, and the risks associated with these limitations should also be assessed by the senior management. In case an AI makes use of technology solution provided by an external service provider, it is expected that proper due diligence should be conducted by the AI

		to ensure that the service provider is capable and that the solution provided by the service provider is reliable and robust. B. Validation and testing AIs should effectively test the remote account onboarding processes, taking into account, among others, potential cyber-attacks and frauds (e.g. malware attacks, parameter tampering, vulnerabilities that may allow identity verification controls to be bypassed, systemic loopholes that may lead to large-scale deficiencies in identity verification). As for technologies provided by service provider(s), AIs are still accountable for the reliability of the technologies. Hence, the responsible management team members of the AI should satisfy themselves that the technologies have been adequately tested and the testing approach and methodology are rigorous and robust. The AI should conduct its own testing whenever there is a need and it should not simply rely on the testing and assessment results provided by the service providers. In addition, the testing methodology and results should be reviewed by an independent assessor acceptable by the AI as part of the AI’s risk governance process. C. Validation of identity documents Where customers’ identity documents are being validated during the remote customer on-boarding processes, AIs should ensure that the authenticity of these documents is effectively validated, taking into account, among others, the maturity of the technologies used for the validation, the effectiveness of the security feature validation mechanism (as compared with the similar validation processes carried out physically at branch counters), and the accuracy / error rates or any other objective measures/metrics of the reliability of the validation process. Although certain technology solutions may support the validation of different identity documents issued by multiple jurisdictions, AIs should ensure that the types of identity documents allowed by the remote customer on-boarding services are well supported by the effectiveness of the technology solutions.

		D. Recognition of customers Where facial recognition technologies are adopted for identity verification, AIs should ensure the effectiveness of the technologies, taking into account, among others, the effectiveness of the liveness detection (i.e. determining whether the facial images used for the identity verification are captured from a living person instead of a facial replica or a digital reproduction) and the overall accuracy of the facial recognition solution, including the false acceptance rates and false rejection rates or any other objective measures/metrics. E. Proper coding Given that service providers are usually involved in the development of identity verification solutions, AIs should establish effective mechanisms to address the risk that the application developed by the services providers contains malicious codes or material deficiencies, which could lead to a higher risk of systemic loopholes in the remote customer on-boarding process. For example, an AI could specify clearly in the terms and conditions with its service providers, where applicable, that the service providers should adopt effective software development controls. The AI should satisfy themselves that proper controls are in place within the service providers as part of the relevant software development process (e.g. requiring its service providers to provide independent assessment reports and/or relevant evidence to show that source code review has been performed). F. Risk mitigating measures AIs should implement additional risk mitigating measures (e.g. quality assurance checking of actual remote on-boarding results, collection and monitoring of customers’ relevant digital footprints to identify

		unusual or suspicious activities) whenever there is a need to address the risk of falsely on-boarded customers who might have evaded the technological measures of the remote on-boarding solutions. G. Periodic assessments AIs should conduct regular assessments to ensure ongoing reliability of the technology solutions (particularly for solutions using artificial intelligence, where their effectiveness may change over time depending on the actual data processed by the solutions) and to identify and assess if emerging fraud schemes or attacks would impose new or heightened risks to the remote customer on-boarding services. Note 1: AIs should assess the money laundering and terrorist financing risk associated with the remote customer on-boarding process and ensure compliance with the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions), HKMA’s circular on “Remote on-boarding of individual customers” (dated 1 February 2019) and other relevant guidance issued by the HKMA from time to time, as well as the requirements set out by the relevant regulatory bodies and overseas jurisdictions concerned.
11.	What is the expectation of the HKMA in relation to security controls for resetting the Internet banking password because a customer forgets the password?	AIs should carry out adequate identity checks (e.g. two-factor authentication, identity verification at branch) and any other appropriate measures when any customer requests resetting the customer’s Internet banking password, so as to effectively address the risk of fraudsters resetting and obtaining the reset password without the knowledge of the genuine customers. If security questions are used in the password reset process, the questions should be carefully designed. In particular, the questions should be designed in such a way so that answers would not be easily guessed even randomly or available in public domain, social media or other sources. AIs should also implement appropriate controls so that it would be impracticable for fraudsters to have unlimited attempts for answering

		the security questions, even with automatic means. The use of security questions should be supplemented by other means of authentication controls (e.g. other factor of authentication) whenever there is a need to adequately authenticate the identity of the person who tries to reset the password. Moreover, AIs should not simply send a hyperlink to the customers via email or mobile phone for resetting the internet banking password, because a fraudster could then reset the password if he or she has compromised the customer’s email account or has access to the hyperlink on the customer’s mobile phone. In addition, AIs should conduct regular risk assessment on the adequacy and effectiveness of the password reset controls taking into account the latest hacking techniques and security threats (including whether the answers to the questions may be leaked to fraudsters during data breach incidents that happen from time to time).
12.	What is the expectation of the HKMA in relation to the controls against attacks attempting to log in to Internet banking services using automated tools (e.g. brute-force attacks or “credential stuffing” attacks)?	AIs should implement effective measures to guard against automated brute-force attacks and credential stuffing using automated tools during Internet banking login if 2FA is not used for logins of Internet banking services. Such measures may include a challenge response test (e.g. CAPTCHA) and AIs should avoid giving an indication whether a particular user ID is valid or not before the correct login credentials are input. In any case, AIs should implement appropriate controls so that it would be impracticable for fraudsters to have unlimited attempts for similar automated attacks. In addition, internet banking service that authenticates customer by user name and password during the login process may be subject to a higher fraud risk if the design of the login process allows a fraudster to have many or even unlimited attempts to confirm the validity of user names (e.g. if the bank's login page indicates whether a user name entered is valid or not). This might allow the fraudster to get hold of a list of valid user names and hence the fraudster could use the list to try compromising the customers' Internet banking accounts (e.g. by more targeted social engineering or phishing attacks using email addresses

		similar to the valid user names). Hence, AIs should implement measures to ensure that their internet banking services are not subject to the above risk. AIs should conduct regular risk assessment on the adequacy and effectiveness of the login controls taking into account the latest hacking techniques and security threats to address the cyber-attacks aim at fraudulently gaining access to customer accounts.
Subsection 4.2 – Notifications sent to customers		
1.	If an AI does not have the customers' specific contact information for the notification channel(s) adopted by an AI to facilitate customers' timely detection of unauthorized transactions, should the AI reject the relevant transactions initiated by those customers?	If an AI has adopted a particular channel (e.g. SMS message, email, instant message services or outbound call) for the purpose of notifying its customers of important matters, the AI should make practically reasonable effort to collect the relevant contact information from the customers and explain to them the risk implication and any impact on the service if such contact information could not be obtained from the customers. If the AI is still unable to obtain the relevant contact information for notifying a customer when the customer initiates a transaction that is considered as of higher risk, the AI is expected to make timely attempt to notify the customer via other available contact information provided by the customer to the AI. In any case where the AI cannot reach the customer, the AI should consider applying any additional control measures (e.g. delaying the execution of the relevant transaction until the AI obtains the confirmation from the customer) when the AI decides to accept the transaction.
2.	With reference to section 4.2.1 of the SPM on Risk Management of E-banking, it is stipulated that "AIs, should, as far as practicable, notify customers immediately via an effective channel	SMS OTP and effective notifications serve different purposes. While SMS OTP is intended for authenticating a customer before proceeding a transaction, an effective notification serves to notify the customer when the transaction has been proceeded/made after the successful authentication of the customer. Based on some Internet banking fraud cases reported to the HKMA, effective notifications sent for high-risk Internet banking

	once the customers initiate transactions that are considered as of higher risk." When a customer initiates a high-risk transaction, the AI would send him/her an SMS OTP. As the SMS OTP also contains the transaction details, can we treat the SMS OTP as the notification as well so that another notification is not required to be sent to customers? For the purpose of interpreting the quoted requirement, can I consider the stage where customers have inputted the transaction details (which leads to sending of SMS OTP) as "initiating" the transaction?	transactions have been useful to promptly inform a customer of potential fraudulent transactions that might have been authenticated by the customer, say, due to social engineering attack or fake Internet login screen. As such, we consider that it remains important for such notifications to be sent out after customer authentication of the relevant transactions has been carried out. Taking into account the above, SMS OTP should not be considered as an effective notification at this stage, although the HKMA would continue to review the relevant developments going forward.
3.	As set out in section 4.2 of the SPM on Risk Management of E-banking (TM-E-1), AIs are required to notify customers immediately via an effective channel once the customers initiate high-risk transactions. From a service quality perspective, customers may, from time to time, request AIs to opt out from such notifications. In this situation, we would like to seek clarification from the HKMA on whether those opt-out requests could be entertained and whether reconfirmation from the said customers should be obtained on a regular	It would be acceptable for an AI to entertain such a request from a customer, as an exception, provided that the following conditions can be met: - the AI has clearly explained to the customer the potential risks and any other service implications if no effective notification is sent to the customer, and the customer confirms his or her understanding of the risks and implications and he or she still determines to opt out from receiving such notifications; - the AI has properly authenticated the identity of the customer to ensure that the request is from the genuine customer; - the AI has offered other alternative notification channels to the customer (note 1); - the AI allows the customer to opt in if requested; - the AI maintains proper records related to the above-mentioned process; and - the opt-out by the customer does not affect the responsibilities of the customer and the AI as set out in the Code of Banking Practice, including customers' and AIs' liability for loss.

	interval thereafter, say annually or once every two year.	The AI may decide whether reconfirmation from the customer will be obtained on a regular interval, and if so, it should explain to the customer. Note 1: For the avoidance of doubt, if the customer does not agree to adopt any one of the notification channels offered by the AI, the AI can still entertain such a request from the customer on an exceptional basis, provided that the conditions listed above are met.
4.	If AIs allow customers to apply for or activate small-value funds transfer service via Internet Banking, are AIs required to send a notification to customers for the activation or application (i.e. enrollment) of such service?	To mitigate the risk that fraudsters activate the small-value funds transfers service on behalf of an AI's customer without the knowledge of the customer, controls should be in place by AIs so that only customers who choose to use the service will be able to effect small-value funds transfers transaction without 2FA. In other words, the small-value funds transfer service should be by default not given to customers (i.e. disabled) or pre-set to zero transaction limit(s) until customers apply for or activate such service. As activation of small-value funds transfer service via Internet banking may increase the risk of unauthorized fund transfers, AIs should send notifications to customers for the activation or application (i.e. enrollment) of such service. AIs can determine what channel(s) to be used for sending such kind of notification to their customers provided that the channel(s) chosen is/are commensurate with AIs' risk assessment.
5.	What is the expectation of the HKMA for sending customer notification messages to facilitate timely detection of unauthorized e-banking transactions and activities?	To facilitate prompt detection of unauthorized e-banking transactions and activities, customer notification messages should be effective and, at a minimum, include the following types: (i) timely notifications (note 1) for high-risk transactions conducted via Internet banking or phone banking;

		(ii) timely notifications for card-not-present (CNP) ~~credit~~payment card transactions that (a) involve high-risk merchants with transaction amount exceeding certain threshold value (note 2) or (b) use contactless ~~credit~~payment cards and no additional authentication is required (note 3); and (iii) timely notifications for the following types of transactions: (a) online activation of small-value funds transfer service and small-value funds transfers to unregistered payees; (b) all CNP ~~credit~~payment card transactions or those CNP ~~credit~~payment card transactions exceeding a transaction amount threshold if specified by the relevant customer, other than those covered in (ii) above; (c) overseas credit card point-of-sale transactions that are considered as high-risk by the AI, taking into account factors such as the nature or amount of the transactions; and (d) overseas ATM cash withdrawal transactions and EPSCO transactions (including payment and cash withdrawal transactions) that are considered as high-risk by the AI. In addition, a timely notification should be sent to a customer who signs on the Internet banking services offering funds transfer services without using 2FA for the login process. Although such notifications could be streamlined commensurate with the risk associated with the login process, AIs should aim at reducing confusion that it may cause to the customer about when such notifications will be sent out. For instance, AIs may send out such notifications when the customer accesses the Internet banking services from a device different from the device(s) which was/were recently used by the customer. The above-mentioned notifications should be sent to customers immediately via an effective channel commensurate with the risks associated with the transactions. While notifications set out in (i) and (ii) above are generally expected to be sent via SMS messages, AIs may make use of other channels (e.g.

		emails, in-App push notifications) if preferred by the customers so long as the AI has taken adequate measures to address the limitations associated with the relevant channels so as to ensure that its customers will be able to receive those notifications in a timely manner. In this connection, such measures generally include: (i) Explaining clearly to the customer the key limitations of the channels that could be chosen by the customer to receive such notifications; (ii) Putting in place arrangements such that the notifications can be delivered to and be received by the customers; (iii) Allowing changes of the notification channels by customers (where the change requests initiated by customers should be regarded as high-risk transactions); (iv) Including SMS message as one of the notification channels that can be chosen by the customers. Note 1: As regards business Internet banking which enforces dual authorization control (e.g. maker and checker controls) for each high-risk transaction, AIs have the flexibility to send the notifications by batch via emails. Note 2: AIs should conduct internal assessment to determine the predefined threshold transaction amount for each category of high-risk merchants. Note 3: AIs may consider allowing a customer to set a threshold below which notifications will not be sent to the customer. However, the customer needs to opt in for this arrangement and AIs need to allow the customer to choose a threshold limit which should not be greater than HK$5,000 (this threshold has been determined after consulting the banking industry associations) in any case.

6.	What is the expectation of the HKMA for SMS notifications sent by AIs to customers who have activated the SMS forwarding service?	AIs using SMS for the notifications required in the SPM should implement controls with the relevant mobile network operators in Hong Kong to deliver SMS notifications related to CNP credit card transactions sent by the credit card issuing banks to both the pre-registered mobile phone numbers and any Hong Kong mobile phone numbers to which SMS notifications are being forwarded (if the SMS forwarding service has been activated). In addition, AIs should conduct risk assessment to determine whether such control needs to be adopted for other types of online transactions.
7.	Are AIs allowed to send messages (e.g. emails, SMS messages) to their customers with embedded hyperlinks?	AIs should adopt appropriate measures to safeguard against social engineering techniques for obtaining customers' information such as e-banking user IDs and passwords via fake or suspicious emails, SMS messages, websites and Internet banking mobile applications (Apps) or impersonating AIs' staff or the Police. AIs should not send messages (e.g. emails or SMS messages) to the customers with embedded hyperlinks (including those presented as QR code) to the transactional websites or Internet banking mobile Apps. In addition, AIs should also remind their customers not to access bank websites through hyperlinks embedded in emails.
Subsection 5.1 – Confidentiality and integrity of information		
1.	Are there any specific controls that should be implemented if there is a need for a decryption process at some point between the customers' devices and the AI's trusted internal networks for the transmission of an Internet banking password?	If there is a need for a decryption process at some point (e.g. at the web server) between the customers' devices and the AI's trusted internal networks for the transmission of an Internet banking password, any cryptographic process (i.e., decryption and re-encryption) should ideally be performed in a secure environment that is highly tamper-resistant. At a minimum, that cryptographic process should be performed in the same server and the decrypted passwords should not be stored or cached in the server after the cryptographic process is completed and the password is re-encrypted for transmission to continue.
Subsection 5.2 – Internet Infrastructure		

1.	Are there any sound practices on security controls for the Internet infrastructure implemented by AIs?	AIs should make reference to sound industry practices and put in place Internet infrastructure which is commensurate with the risks associated with Internet banking. At a minimum, AIs should implement the controls mentioned below. (1) Demilitarized Zone (DMZ) (a) The DMZ, situated between the Internet and AIs’ trusted internal networks, normally houses various kinds of servers and other relevant devices (e.g. network and security devices). Given the exposure of these devices to potential attacks via the Internet, no confidential data (including encrypted login passwords) should normally be stored or cached in these devices; (b) To protect the devices in the DMZ, there should be "external firewall(s)" (the term firewall(s) also covers other related network equipment such as router(s) for the purpose of this section) to control the traffic between the Internet and the devices housed in the DMZ so that only acceptable communication methods for connecting to these devices would be allowed. No sensitive or system information should be unveiled when the firewalls respond to malicious network traffic from the Internet; and (c) In ensuring that only permissible network traffic can pass from the devices in the DMZ to the AIs' trusted internal networks, AIs should install another tier of "internal firewall(s)" to control the traffic between the DMZ and the AIs' trusted internal networks. Any direct dial-up connections or other network connections with third parties bypassing the firewalls should generally be prohibited. If a dial-up connection is necessary for a specific task, this connection should be properly approved, monitored and removed immediately after completion of the task. In addition, if two or more tiers of firewalls are used, AIs may consider using firewalls of different brands/models to prevent similar security vulnerabilities from being exploited in different firewalls. (2) Configuration and protection

		(a) AIs should formulate formal policies for the configuration, monitoring and maintenance of their firewalls and servers as well as any other relevant devices of the Internet infrastructure, so that all changes to the configuration are properly controlled, tested and tracked. AIs should also perform frequent reviews and timely updates of the configurations of these devices to enhance protection from newly identified vulnerabilities; (b) Any unused programs and computer processes of firewalls, servers and any other relevant devices should be deactivated or removed. AIs should establish accountability for the timely review, testing and application of appropriate patches to these devices. Moreover, security software should be installed and updated on these devices. Only the minimum number of user accounts that are necessary for the operation of these devices should be maintained; (c) The programs and other information kept in the firewalls, servers and any other relevant devices should be updated only by strongly authenticated user accounts or authorized computer processes. These devices should also be subject to stringent change control procedures. AIs should use appropriate scanning tools to identify any potential security issues relating to these devices on a regular basis. Periodic integrity checks on important programs and static data (e.g. configuration) kept in these devices should be conducted to validate that they have not been altered; and (d) All access to the firewalls, servers and any other relevant devices using privileged or emergency accounts (e.g. system administrator or "super user") should be tightly controlled, recorded and monitored. If these devices are administrated remotely, strong authentication and encryption of system information should be in place to protect them from unauthorized access. (3) Intrusion detection (a) AIs should identify with care the information necessary to detect an intrusion in their Internet banking system or related network. This information will facilitate the determination of what audit

		logs of firewalls, servers and any other relevant devices should be enabled and retained, and what other data (e.g. system resources utilisation, network traffic) should be monitored; (b) Appropriate controls should be in place to protect and backup the audit logs, and to ensure that the clocks of the systems generating the logs are synchronised. Audit logs should generally be reviewed on a timely basis. Since log files are typically voluminous and difficult for humans to process, AIs should consider the use of automated tools to help analyse the audit logs and collect information that is relevant but unavailable from the audit logs. AIs should configure the automated tools to facilitate their active response to any potential intrusion detected; (c) In selecting automated tools, AIs should consider whether the tools are able to cope with evolving patterns or techniques of attack (e.g. whether the vendors can offer timely updates of attack signatures for IDS/IPS). AIs should also assess the potential impact of the tools on the Internet infrastructure (e.g. system performance, or whether the installation of the tools would in turn introduce potential security loopholes); and (d) The tools should be carefully tested and fine-tuned periodically to improve their effectiveness while reducing false alarms. A formal process should be in place to ensure that the relevant support staff will respond to important alerts generated by the tools on a 24 hours a day, 7 days a week basis.
Subsection 5.3 – Application system security		
1.	What is the expectation of the HKMA for the application system security controls implemented by AIs?	AIs should implement, among others, the following controls: (i) When AIs select system development tools for the purpose of developing their Internet banking systems, including Internet banking Apps, they should evaluate the security features that can be provided by different tools to ensure that effective application security can be implemented. In any

		consideration of the selection of an Internet banking system developed by a third-party vendor, AIs should assess the application security of the system. (ii) Comprehensive and effective validation of input parameters should be performed (e.g. checking to detect/prevent any tampering with a payee’s account number input by the customers). This prevents intentional invalid input parameters from being used to launch an attack by embedding malicious commands to be executed by the Internet banking system. Moreover, the Internet banking system should operate with the least possible system privileges. (iii) Error messages or information (e.g. HTML code) produced by the Internet banking system should not reveal sensitive details of the system and errors should be appropriately logged. (iv) The mechanism for managing an Internet banking session should be secure. In particular, a session should be terminated after a defined period of inactivity, while sensitive information generated or used during the session should not be cached in the customers’ devices, including in the temporary files of the browsers. Moreover, the Internet banking system should ideally prohibit the browsers from memorising or displaying the Internet banking user IDs and passwords previously entered by customers and the Internet banking pages previously accessed by customers. (v) The Internet banking system should also implement appropriate means for the customers’ browsers and Apps to validate the identity and genuineness of the Internet banking website accessed by the customers. (vi) Appropriate controls should be implemented (e.g. inspection of traffic flowing from customers’ devices to the Internet banking system) to detect common web application attacks. (vii) Hidden directories that contain administrative pages or sensitive information should be removed from the production server of the Internet banking system or protected by effective authentication and access control mechanisms. Back-up files and sensitive files should be removed from the servers. Alternatively, the structure of the relevant file directories should be securely protected to

		prevent access to these files by potential attackers. Adequate controls should be implemented to ensure that all sensitive files of the Internet banking system are appropriately protected.
Subsection 6.1 – Funds transfers		
1.	Are there any specific controls that should be implemented for high-risk funds transfers and small-value funds transfer to unregistered payees?	AIs should implement, among others, the following controls to minimise the risk of unauthorized high-risk funds transfers and small-value funds transfers to unregistered payees: (i) transaction limit(s) for such funds transfers should be implemented. Customers should only be allowed to increase the transaction limit(s) through secure channels; and (ii) consideration should be given to deferring the execution of online registration of payees and funds transfers assessed by AIs as higher risk (e.g. high-value funds transfers) by an appropriate period of time after sending notifications to the customers. AIs’ prudent cap(s) on the transaction limit(s) for small-value funds transfer transactions to unregistered payees should not exceed the ceiling per Internet banking account as stated in the relevant guidelines of the HKMA issued from time to time. Given that small-value funds transfer transactions are not regarded as high-risk transactions and hence do not require 2FA, AIs should implement additional risk mitigating measures as appropriate. For instance, if the AIs have doubt on the genuineness of small-value funds transfer transactions, they should implement measures such as: (i) re-authenticating the customers’ identity using 2FA; or (ii) deferring the execution of the small-value funds transfer transactions depending on the transaction amount.

		Alternatively, AIs may choose to implement 2FA controls for authenticating small-value funds transfer transactions.
Subsection 6.3 – Account aggregation service		
1.	Are there any regulatory requirements and security control requirements that should be observed by AIs offering account aggregation service (AAS)?	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 log in 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: (i) 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; (ii) Section 92 in respect of any advertisements posted on the Internet for soliciting deposits from members of the public in Hong Kong; (iii) 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 (iv) 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. 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. 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. 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. 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. 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.

		To address the increased security risk, the AI should satisfy, among others, the following requirements: (i) 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 SPM module 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) to address the risk that fraudsters might impersonate the customer via the partnering institution; (ii) 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 (iii) 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. Please refer to FAQ #2 under subsection 3.3 for further guidance.
Subsection 7.1 – Internet banking accessed via mobile devices		
1.	Are there any common security controls that are expected to be implemented to address the risks associated with Internet banking accessed via mobile devices?	Taking into account the evolving risks associated with mobile malware and vulnerabilities of mobile devices, AIs should adopt multi-layers of defence to manage the risks. In cases where Internet banking services accessed via mobile devices allow high-risk transactions, the following security controls are expected to be implemented to address the relevant risks:

		(i) conducting assessment to determine whether any mobile platforms should be “blacklisted” or “whitelisted” for accessing their Internet banking services, having regard to factors such as the capacity of the platforms to address security vulnerabilities and plausible attacks from malicious Apps; (ii) restricting the device from accessing the services if there is a reasonable doubt that (i) the mobile device used by the customer has been compromised (e.g. rooted/jailbroken devices~~) or~~), (ii) the device contains mobile Apps installed via unofficial sources with excessive permissions (e.g. accessibility service or full control) and not on AIs’ whitelist (i.e. list of mobile Apps assessed as legitimate by AIs), or (iii) the device belongs to any mobile platforms blacklisted by the AI. ~~Alternatively, the AI~~AIs should ~~clearly warn~~ also alert customers to the ~~customer of the potential security~~relevant risks ~~associated with~~ and offer guidance on how to configure their devices (e.g. remove the unofficial Apps) to resume the ~~device before allowing the customer to~~ access ~~the~~to Internet banking services~~ via the device;~~; (iii) performing a formal code review of the Internet banking App to ensure that the App does not contain security loopholes;~~ and~~ (iv) implementing measures to ensure that customer data are not stored or cached in the mobile devices after normal or abnormal termination of the Internet banking session whenever practicable~~.~~; and ~~(iv)~~(v) putting in place adequate security measures against malware attacks, including but not limited to the relevant controls mentioned in FAQ #9 under subsection 4.1. In addition, it would also be useful if the following sound practices could be adopted to strengthen the security of the Internet banking App: (i) conducting other checks regarding any signs of malware on the customer’s device before the device can be used to access the Internet banking services; and

Commented [YPK4]: Explanatory Note

This revision aims to incorporate the requirements of the Operational and IT Incidents Watch “Recent developments in malware scams” dated 22 Dec 2023.

Commented [YPK5]: Explanatory Note

This revision aims to remind AIs to put in place adequate security measures against malware scams (including those anti-malware controls applicable to soft token in FAQ #9 under subsection 4.1).

		(ii) performing code obfuscation to increase the difficulty of examination by potential fraudsters through reverse engineering of the App. For a business customer that does not adopt a dual authorization control (e.g. maker and checker controls) or for a personal customer, AIs should immediately send an additional notification to the customer through a notification channel that is different from the original notification channel if the original notification is generally accessible by mobile devices once the customer initiates a high-risk transaction or a small-value funds transfer to an unregistered payee.
2.	Are there any security control requirements for AIs using SMS OTP or soft tokens as 2FA for accessing the Internet banking services?	The effectiveness of OTP may be weakened if the same mobile device can be used for accessing Internet banking and receiving / generating the OTPs while in the event that the mobile device has also been controlled or compromised by a fraudster. In cases where a customer is able to initiate a high-risk transaction with the use of such OTP only for the purpose of 2FA, AIs should implement additional risk mitigating measures, including the following controls: (i) As a customer's mobile phone number for receiving SMS OTP is a crucial piece of information in the context of the relevant security controls, changes of those mobile phone numbers should be permitted only through secure channels with adequate identity checks, other than using 2FA via SMS OTP. (ii) For a business customer that does not adopt a dual authorization control (e.g. maker and checker controls) or for a personal customer, the AI should put in place the following extra security measures: (a) online registration of a payee should take effect only after a delay of at least 6 hours or else the funds transfers to the newly registered payees via the same mobile device should be subject to deferred execution for a period of time commensurate with the risk and value of the transaction;

		(b) in principle, a high-risk funds transfer transaction via the same mobile device with an amount exceeding a threshold determined by the AI should only be effective after an appropriately prudent delay that is commensurate with the relevant risks and the AI’s fraud monitoring capability. In general, the delay should be at least 6 hours for high-risk fund transfers involving a relatively high value based on the threshold determined by AIs. Moreover, AIs should use a risk-based arrangement to call back the relevant customers to confirm or follow up those transactions as needed; and (c) for high-risk funds transfers, AIs should consider setting additional prudent transaction cap(s) (e.g. per day or over a period of time) commensurate with their own risk appetites. Any online increase of the transaction limit(s) via the same mobile phone should take effect only after a delay of at least 6 hours. The use of OTPs generated from customers’ mobile devices such as soft tokens also exposes AIs and customers to similar risks as using SMS OTPs. In principle, AIs allowing customers’ mobile devices to generate OTPs should also implement the controls set out in this FAQ, where applicable. However, AIs using soft tokens as 2FA may have some flexibility of not requiring deferred execution and the related controls so long as a regular assessment is undertaken to confirm the robustness of the implementation of soft tokens and to identify any residual risks, and effective risk mitigating measures (e.g. confining the waiver of deferred execution to transactions under a certain threshold) are taken to address these residual risks.
Subsection 7.3 – Self-service terminals		
1	What security controls are AIs expected to implement in relation to self-service terminals?	AIs should implement, among others, the following security controls in relation to self-service terminals: (1) Authentication

		(a) implementing adequate controls covering the issuance, activation, replacement and loss of cards used in the terminals; (b) enforcing chip-based authentication on chip cards issued by AIs for local ATM transactions (note 1); and (c) installing encrypting PIN pads in those terminals which require customers to input PIN for transaction authentication. (2) <u>System security</u> (a) installing application whitelisting solutions in the personal computers (PCs) inside the terminals to prohibit the execution of unauthorized programs. Unauthorized program executions and other exceptions identified by the whitelisting solution should be promptly followed up by the AI. In addition, proper security controls should be in place to protect the whitelisting solution against unauthorized changes or deactivation; (b) reviewing the application whitelist on a regularly basis to ensure that only necessary programs are maintained in the list; (c) implementing security hardening process to secure the PCs inside the terminals, hosts, servers and backend systems which connect to the terminals; (d) adopting strong encryption to secure the data transmission between the hosts, terminals and cash dispensers. Proper authentication controls should be implemented between the terminal PCs and the cash dispensers to guard against cash dispensation instructions from unauthorized sources; (e) prohibiting terminals from booting up via external devices and removing unnecessary external devices from the terminals; and (f) securing the basic input/output system (BIOS) of the personal computers inside terminals from unauthorized access.

		(3) Physical security (a) installing keypad covers and anti-skimming devices (note 2) in those terminals that involve the use of cards for authentication of customers’ identity and require customers to input PIN for transaction authentication; (b) undertaking frequent patrols of terminals in order to check the physical security of the terminals and to discover any abnormal status in respect of the terminals. Adequate measures should also be implemented to reduce the chance of, and deal with, scenarios resulting in “unattended banknotes” being dispensed from the terminals; (c) providing adequate physical safeguards and proper access controls over terminals’ connections to peripheral devices (e.g. prohibiting unauthorized devices from being connected to and communicated with the terminal via USB ports , disabling the USB auto-run function of the terminals); (d) providing adequate physical access controls to the terminals and the PCs inside. For example, some stringent physical access controls of the vault inside terminals may involve installation of a lock that requires one-time password; and (e) retaining sufficient audit trails (including system records and footage from closed-circuit television (CCTV (note 3))) of customers’ transactions conducted through the terminals. (4) Banknote handling (a) implementing adequate measures and effective arrangements related to replenishment or collection of banknotes in or from the terminals; (b) performing careful assessment and selection of terminals which allow deposit of banknotes, having regard to, among other factors, their capability in detecting counterfeit banknotes and related test results. System controls or alternative arrangements should be in place to facilitate

		timely installation of system updates for enhancing the capacity of the terminals in detecting counterfeit banknotes; and (c) implementing proper procedures and dual controls to reconcile the banknotes in the terminals against the records in the AIs’ systems. (5) Other security and operation controls (a) implementing proper network segregation between networks related to self-service terminals and other networks of the AIs; (b) providing sufficient guidance and training to staff handling disputes with customers; and (c) giving adequate consideration to customers’ experience and expectation (e.g. response time of the terminals) when designing and implementing the relevant system processing related to self-service terminals so as to reduce the chance of confusion and customer disputes. AIs should keep abreast of emerging ATM attacks and take appropriate measures to address the risks. For terminals that allow cardless cash withdrawal, AIs should ensure that the authentication control needed before a customer withdraws cash still requires proper 2FA and that other mitigation controls are in place. Even if a cardless cash withdrawal involves only a smaller amount and the withdrawal is initiated by the relevant bank account holder via an e-banking channel, it is still prudent that such initiation is subject to 2FA or other compensating controls, in the light of the inherent risks of such transactions. Note 1: In cases where 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 before any

		overseas ATM cash withdrawal can be conducted. Customers are also given an option to set a lower withdrawal limit for overseas ATM cash withdrawal transactions. Note 2: These include, for instance, fraudulent device inhibitors (FDI) to prevent attempted installation of skimming devices in the terminals. For terminals subject to higher risk, AIs should implement more effective anti-skimming solutions that can effectively detect, and/or interfere with, any skimmers including micro-skimmers (e.g. those that can be attached on the card insertion slot). Note 3: 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.
Subsection 7.4 – Phone Banking		
1.	Are there any sound practices on using challenge questions to authenticate customers' identity during phone banking services?	For AIs that ask challenge questions to authenticate customers' identity during phone banking services, they should also put in place adequate controls to minimise the risk that fraudsters are able to answer the questions based on information about the customers available from public sources or data leakage incidents from different types of organisations happening from time to time. Moreover, AIs should also implement controls in order to address the risk that their staff or service providers who have access to the answers of the challenge questions could impersonate the customer concerned using the information. Those staff or service providers should only be given access to information about the customers on a need-to-know basis. This may include only a very limited set of challenge questions and answers (e.g. only those selected randomly by the system and raised to the customers) and the answers should be as dynamic as possible, while their access to the questions and answers is properly recorded and retained for future investigation if needed. Challenge questions could be more effective if the following sound practices are adopted:

		(i) the sets of challenge questions could be created with answers which are not easily available in public domain, social media or affected by relevant data breach incidents happening from time to time, or can be easily guessed by the fraudster even without any access to customers’ information; (ii) a series of more difficult questions with static answers or dynamic questions could be asked during the customer identity authentication process; (iii) different sets of challenge questions could be used to authenticate customers between different phone banking authentication sessions; and (iv) suitable arrangements to prevent fraudsters from engaging repeated attempts of guessing the challenge questions. AIs should periodically re-assess the effectiveness of the challenge questions in the light of emerging risk, and data breach incidents from time to time that may weaken the effectiveness of certain questions. In cases where phone banking services allow high-risk transactions, AIs should implement effective 2FA mechanisms to authenticate the identity of the customers. As an alternative to 2FA, AIs may call back the customer via a pre-registered telephone number provided by the customer to ask certain additional challenge questions, particularly dynamic questions (e.g. details of recent transactions), and confirm such a high-risk transaction. If the phone banking service allows funds transfers to unregistered payees, AIs should implement controls that are similarly effective as those set out in this SPM module.
Subsection 7.5 – Contactless mobile payments		
1.	What is the expectation of the HKMA on the implementation of contactless mobile payment service?	AIs should implement effective controls to address the specific risks of contactless mobile payment service as stipulated in section 7.5 of the SPM. In particular,

		(i) Sensitive data required for making contactless mobile payments should be stored in a highly secure location where the data security and access controls adopted to protect the data should comply with the relevant international/industry standards. Moreover, unnecessary information (such as cardholder names, card CVV/CVC/CVN) should not be stored in the relevant secure location. (ii) In cases where a credit card account is used for providing a contactless mobile payment service, such credit card account should be prohibited from conducting CNP credit card transactions unless the card information (e.g. card number, expiry date) is not readable by a contactless reader through electronic pick-pocketing. (iii) Adequate and effective security controls should be implemented to guard against potential and emerging attacks (e.g. relay attacks (note 1)) on the service. (iv) Adequate and effective procedures should be in place to prevent and detect unconfirmed/incomplete transactions and facilitate a timely refund to the customers. Note 1: Relay attacks refer to a modus operandi where the attacker forwards a request from the point-of-sale (POS) terminal to the victim's mobile device and relays back its answer to the POS in real time, in order to carry out a contactless mobile payment using the victim's credit card information by pretending to be the owner of the victim's device.
Subsection 8.1 – Fraud and incident management		
1.	Are there any control examples and sound practices on the fraud monitoring mechanisms implemented by AIs?	In general, AIs' fraud monitoring mechanisms should be capable of detecting, for instance, the following possible scenarios under a risk-based approach: (i) Internet banking login and transactions initiated from an Internet Protocol (IP) address indicated as potentially suspicious by internal or external sources;

		(ii) Internet banking login from a device different from device(s) which was/were recently used by the customer; (iii) overseas cash withdrawals using ATM/credit cards performed shortly after local transactions conducted by the card(s) belonging to the same customer; (iv) funds transfers made to payees who have been regarded as possibly suspicious or doubtful by internal or external sources; (v) frequent or multiple cash withdrawal transactions, funds transfers (including small-value funds transfers and direct debit transactions) or funds transfer attempts made to the same payee or set of payees within a short period of time; (vi) a large-value funds transfer conducted shortly after online registration of the payee(s) via Internet banking; (vii) change of a customer's important contact details (such as correspondence address) shortly followed by activities which may indicate potential fraudulent activities such as the opening of an Internet banking account online, a request for important documents to be mailed to any changed address, online increase of funds transfer limits via Internet banking, or a sudden increase of funds transfers made to unregistered payee(s); and (viii) change of a customer's mobile phone number for receiving SMS notifications or OTPs, shortly followed by potentially suspicious activities such as (i) large-value funds transfers to unregistered payee(s); and (ii) online registration of third-party payee(s) subsequently followed by large-value funds transfers to the same payee(s).
Subsection 8.2 – Incident response and periodic drills		
1.	What is the expectation of the HKMA on the incident response and management procedures established by AIs?	AIs should establish incident response and management procedures that allow AIs:

		(i) to find out quickly the possible root cause of the incident and assess the potential scale and impact of the incident; (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 where feasible via any cyber intelligence sharing platform or forum; (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. AIs are expected to proactively notify the customers affected, or likely to be affected, through the most effective means and inform them of the key facts relating to the incident and the steps that customers may take. Where the incident involves a disruption of critical e-banking service and may last for a prolonged period of time, AIs should consider making a press release where the situation so warrants.
Subsection 9.4 – System resilience		
1.	What is the expectation of the HKMA on contingency and fallback measures for new technologies adopted by AIs?	Similar to other critical banking services, there should be contingency and fallback measures for new technologies (e.g. soft token) adopted by AIs against cyber threats that may impact the effectiveness of the technologies, if applicable. If a technology in use is vulnerable to a material threat newly identified, the AIs concerned should have the ability to devise effective mitigating controls quickly to minimise the associated risk. For example,

		(i) lowering the limits of the transactions (if any) that rely on the technology for customer authentication; (ii) strengthening the fraud monitoring mechanisms; (iii) putting in place an alternative mechanism (and the related contingency plans) when the technology solution in use is compromised; or (iv) restricting the functions that could be accessed by platforms that are vulnerable to the threat.
Subsection 9.5 – Coping with system disruptions		
1.	What distributed denial-of-service (DDoS) controls are AIs expected to implement?	In general, AIs with heavy reliance on Internet for delivery of banking services or 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 expected to implement more advanced controls that are capable of dealing with more serious or different types of distributed denial-of-service (DDoS) attacks (e.g. volumetric network floods that saturate an AI's Internet pipe and attacks targeting SSL-secured services) that may target AIs directly or any other websites (e.g. those of the same banking group) hosted by AIs’ Internet infrastructure. Depending on AIs’ Internet infrastructure and their assessment of DDoS attacks relevant to them, typical controls may include: • periodically assessing the potential areas in the systems and infrastructure components that could be susceptible to DDoS attacks and determine the capability of anti-DDoS mitigation required, taking into account the latest DDoS attack trends and techniques, and the normal usage of the AIs’ Internet banking services and corporate websites; • clean pipes (note 1) with sufficient capacity; • purpose-built appliances (note 2) with anti-DDoS services provided by upstream vendors or Internet service providers (ISPs); • considering the need for engaging multiple vendors or service providers to further reduce the

		risk if a particular vendor / service provider may not have capacity to handle simultaneous DDoS attacks at its clients; and • controls for protecting the supporting systems (e.g. Domain Name System and the AI’s corporate website). Where the ISPs are engaged to mitigate DDoS attacks in the upstream networks, AIs are expected to establish an incident response plan and relevant communication protocol with their ISPs to strengthen their capability in effective DDoS mitigation. Note 1: Clean pipes protect an institution against volumetric DDoS attacks by redirecting the institution's inbound traffic to the service provider's scrubbing centers when a DDoS attack is detected. The scrubbing centers apply DDoS filtering to block the malicious traffic and route the legitimate traffic back to the institution. Note 2: These refer to dedicated and specially designed devices which are usually deployed in AIs’ data centres to detect and mitigate DDoS attacks.
2.	Can the HKMA share some common root causes of system disruption?	According to the information provided by relevant AIs, some system disruptions of critical services by AIs were caused by problems in the actual implementation of some conventional IT controls including: (i) lack of end-to-end testing which simulated the production environment and the actual transaction volume before launching system changes into the IT production environment; (ii) inadequate testing, including performance test of exceptional scenarios and the implication of holidays for the system behaviour (e.g. surges in customer logins);

		(iii) incorrect instructions leading to changes for testing environment mistakenly applied to the production environment; (iv) insufficient staff training and absence of dual control to prevent human errors during implementation of system changes; (v) inappropriate scheduling of changes to fall on business hours; (vi) failure of applying system/configuration changes to all the areas required (e.g. changes were made only to the primary system/equipment but not the backup system/equipment), causing problems in disaster recovery or system resilience; and (vii) inadequate contingency arrangement and fall back plan in the event of unsuccessful implementation of system changes. Therefore, AIs should also take appropriate measures having regard to these lessons learnt from these system disruptions.