Guideline on AI-to-AI Information Sharing for the Detection or Prevention of Crime

November 2025

CONTENTS

Chapter 1 – OVERVIEW

1.1	This Guideline is issued under section 68AAL of Part XIIAA of the Banking Ordinance (Cap. 155) (BO). References to section numbers are to those in Part XIIAA of the BO (Part XIIAA) unless otherwise stated. It should be read in conjunction with Part XIIAA, the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) (AML/CFT Guideline), and other relevant Guidelines and Guidance Papers issued by the HKMA from time to time.
1.2	Terms and abbreviations used in this Guideline should be interpreted by reference to the definitions set out in the Glossary. Where the Guideline discusses obligations, requirements or provisions of other ordinances (e.g. Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO), Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)), the terms used in describing those obligations, requirements or provisions should, absent any indication to the contrary, be interpreted by reference to the definitions in those ordinances.
1.3	This Guideline describes the statutory framework and regulatory expectations relating to the voluntary sharing of information among authorized institutions (AIs) for the purposes of detecting or preventing prohibited conduct (information sharing mechanism).
1.4	This Guideline is intended for use by AIs and provides: (a) general guidance on the scope of information sharing; circumstances under which information may be shared; types of information that may be shared; thresholds that must be met; confidentiality and record-keeping requirements; the circumstances in which the safe harbour under Part XIIAA will apply to protect information sharing; the use to which shared information may be put and the need to avoid indiscriminate de-risking; correction of inaccurate information; and complaint handling; and (b) practical guidance to assist AIs and their senior management in designing and implementing their own policies, procedures and controls relevant to the information sharing mechanism.

1.5	This Guideline will be kept under review and it may be necessary to issue amendments from time to time.
1.6	For the avoidance of doubt, the use of the word "must" or "should" in relation to an action, consideration or measure referred to in this Guideline indicates that it is a mandatory requirement.
1.7	A failure to comply with any provision of this Guideline may reflect adversely on whether the Monetary Authority (MA) continues to be satisfied that the AI has adequate systems of control for the purposes of section 68AAH of Part XIIAA; or whether an AI has met any condition imposed by the MA under section 68AAB(4)(b), 68AAC(6)(b), 68AAD(5)(b) or 68AAE(4)(b). Such failure may also reflect adversely on whether an AI continues to comply with the authorization criteria set out in the Seventh Schedule to the BO, particularly paragraph 10 of the Seventh Schedule which requires an AI to maintain on and after authorization adequate accounting systems and systems of control. The HKMA is empowered to exercise various provisions under the BO in case of non-compliance with the requirements set out in this Guideline.

Chapter 2 – THE LEGAL FRAMEWORK AND SYSTEMS OF CONTROL

Part XIIAA of the BO	
2.1	Part XIIAA sets out a legal framework for the voluntary sharing of information among AIs for the purposes of detecting or preventing prohibited conduct. AIs should familiarise themselves with the detailed provisions in Part XIIAA and note the following in particular.
2.2	Definitions: while a number of terms are defined by reference to existing legislation, including the AMLO, section 68AA introduces or defines certain terms specifically for the purposes of Part XIIAA. In particular: ***entity*** means a natural person, a body of persons (incorporated or unincorporated) or a legal arrangement, and includes – (a) a corporation; (b) a partnership; and (c) a trust. ***relevant entity,*** in relation to an AI, means – (a) an entity with which the AI maintains or has maintained a business relationship (i.e. a customer or former customer of the AI); or (b) an entity for which the AI has conducted or been requested to conduct an occasional transaction. ***platform*** includes an electronic system and any other mechanism. ***prohibited conduct*** means – (a) money laundering; (b) terrorist financing as defined by section 1 of Part 1 of Schedule 1 to the AMLO; or (c) financing of proliferation of weapons of mass destruction as defined by section 2(1) of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526).

	The scope of offences in relation to which AIs may share information is prescribed in the definition of prohibited conduct. ***money laundering*** – (a) means dealing[1] with any property that is the proceeds of – (i) an indictable offence; or (ii) any conduct that would constitute an indictable offence if it had occurred in Hong Kong; and (b) includes money laundering as defined by section 1 of Part 1 of Schedule 1 to the AMLO. Sub-paragraph (a) has been included in the definition of "money laundering" to capture payments that might not be caught by the "disguise" element of the "money laundering" definition in the AMLO. For example, an initial payment by a bank customer who may be a victim of fraud to a fraudster's account (sometimes referred to as a "victim payment") might not meet the "money laundering" definition in the AMLO because, at this stage, there is no act intended to have the effect of making the property (funds) not to appear to represent proceeds of an indictable offence. However, where a fraud has been committed, the funds are already proceeds of an indictable offence and receiving or acquiring (dealing) them is covered by the information sharing mechanism.
Safe harbour	
2.3	Section 68AAG(1) provides legal protection in certain circumstances for AIs disclosing information under the relevant provisions of Part XIIAA, provided that they act in good faith and with reasonable care and do not disclose the fact that information has been disclosed. The terms "reasonable care" and "good faith" are not defined but are well established legal terms and the subject of case law. Examples of reasonable care would include AIs ensuring, as far as is reasonably practicable, before disclosing any information, that: (a) the conditions for disclosure under the relevant provisions of Part XIIAA are met;

[1] ***dealing*** is separately defined in Part XIIAA.

	(b) the information is as accurate as possible by reference to information available at the time of disclosure; and (c) unless the MA's consent has been obtained for disclosure via another channel (see Chapter 5 on Off-Platform Sharing), information is only disclosed via a designated platform to an AI that has the MA's written approval under section 68AAH. An example of good faith in this context would be for an AI to ensure that information is only disclosed for the purposes of detecting or preventing prohibited conduct and not for any other purpose.
2.4	There is also a safe harbour for an AI which receives information under the information sharing mechanism in that section 68AAG(4) provides that the AI's disclosure of information under section 68AAF(3)(a) or use of information under section 68AAF(3)(b) is not to be treated as a breach of any obligation owed by the AI.
2.5	AIs should note that a breach of the requirements under Part XIIAA, such as disclosure to an entity that is not an AI or an AI that does not have the written approval of the MA under section 68AAH, or for a purpose other than detecting or preventing prohibited conduct (e.g. marketing), could result in an AI losing the protection of the safe harbour and being in breach of restrictions on disclosure of information imposed by any common law obligation of confidentiality or by any contract or any enactment or rule of conduct and consequently being potentially liable in damages for any loss arising out of the disclosure.
Systems of control	
2.6	Section 68AAH(1) provides that in order to obtain written approval from the MA to access a designated platform for sharing information under Part XIIAA, the MA should be satisfied that the AI has adequate systems of control for ensuring its compliance with the requirements under Part XIIAA.
2.7	An AI should develop and maintain policies, procedures and controls governing, among other things: (a) decisions to request and/or disclose information;

	(b) access to designated platforms; (c) handling and use of information disclosed/received (such as reviewing results and taking any follow-up actions to mitigate the money laundering and terrorist financing (ML/TF) risks); and (d) maintaining related records.
2.8	Policies, procedures and controls in relation to the sharing of information among AIs should be approved by senior management, and subject to effective oversight, regular review and revision to ensure they remain effective.
2.9	Policies, procedures and controls in relation to the sharing of information among AIs should include reporting of any breach of confidentiality in relation to the shared information to the HKMA and, where appropriate, to the relevant platform operator and, where the information includes personal data, to the Office of the Privacy Commissioner for Personal Data (PCPD).
2.10	An AI should implement policies, procedures and controls in relation to the sharing of information among AIs having regard to the nature, size and complexity of its businesses. It should also refer to Chapter 3 of the AML/CFT Guideline for general requirements on the policies, procedures and controls of an AI.
Common law & contractual obligations	
2.11	AIs are subject to common law confidentiality obligations and contractual provisions, generally included in an AI's terms and conditions entered into at the time of establishing a business relationship and amended from time to time. The safe harbour provision in section 68AAG (see above) gives legal protection in certain circumstances to AIs from (among other things) claims of breach of confidentiality obligations or breach of contractual disclosure restrictions where the AIs disclose information in accordance with the relevant provisions of Part XIIAA. A receiving AI's use of information in accordance with section 68AAF(3) is also not treated as a breach of any confidentiality obligation owed by the AI. AIs may also consider it prudent to review their Terms and Conditions to ensure that they are compatible with the statutory framework and make any necessary amendments.

Interaction with the PDPO	
2.12	While Part XIIAA provides a standalone framework for information sharing among AIs, it does not override or modify the PDPO, which remains relevant. Indeed, much of the language of Part XIIAA intentionally reflects that used in parts of the PDPO. AIs should note the following sections of the PDPO in particular.
Applicability of Data Protection Principles (DPPs)	
2.13	In providing a statutory framework, Part XIIAA authorizes the sharing of personal data within the parameters set out in the law. Part XIIAA does not override the PDPO but in specifically authorizing data sharing it engages section 60B of the PDPO which exempts personal data from the provisions of DPP3 (use of personal data) if the use (which includes disclosure or transfer) of the data is "authorized by or under any enactment". Further, given that the objective of information sharing under Part XIIAA is the detection or prevention of crime, section 58 of the PDPO is also relevant.
2.14	Section 58(1) of the PDPO exempts personal data held for the purposes of, among other things, the prevention or detection of crime,[2] and the prevention or preclusion of significant financial loss arising from unlawful or seriously improper conduct, or dishonesty or malpractice, by persons[3] from the provisions of DPP6 (access to personal data) and section 18(1)(b) (data access request). Section 58(2) of the PDPO exempts data used ("used" includes "disclosed" or "transferred") for, among other things, the detection or prevention of crime from the provisions of DPP3 (use of personal data) whether or not the data is held for that purpose and where the application of DPP3 would be likely to prejudice, inter alia, the detection or prevention of crime. Please also refer to paragraphs 14.4 to 14.8 below.

[2] PDPO section 58(1)(a).

[3] PDPO section 58(1)(e)(ii).

Chapter 3 – SCOPE

Institutions	
3.1	The information sharing mechanism provided for in Part XIIAA applies only to AIs, i.e. institutions authorized by the MA under the BO to conduct banking business or a business of taking deposits in Hong Kong.
3.2	The definition of "entity" (which is used in relation to the subjects in respect of which information can be shared) is intentionally widely drawn. Information may be shared in respect of individuals, legal persons and legal arrangements, including corporations, partnerships and trusts.
3.3	The statutory framework in Part XIIAA intentionally avoids restricting the types of information that may be shared. This is because types of information that may be relevant are evolving continuously. For example, digital footprint and device ID data have become increasingly important in recent years. However, AIs should note that information requested or disclosed under the information sharing mechanism set out in Part XIIAA must be relevant and may only be requested/disclosed for the purposes of detecting/preventing prohibited conduct. These requirements are linked to the "safe harbour" in section 68AAG. AIs should establish effective procedures to ensure that information is only requested/disclosed when all relevant requirements are met. In particular, AIs must not request/disclose information for any collateral purpose (e.g. marketing) or engage in "fishing expeditions" i.e. requesting information that is not related to or is broader than is necessary for a specific inquiry aimed at detecting/preventing prohibited conduct.
3.4	"Prohibited conduct", in respect of which information may be shared, covers money laundering, terrorist financing and financing of proliferation of weapons of mass destruction (WMD). Money laundering is defined in section 68AA to include dealing in proceeds of an indictable offence (or conduct committed outside Hong Kong which, if committed in Hong Kong, would constitute an indictable offence). As noted at paragraph 2.2, this is intentionally somewhat wider than the definition in the AMLO in order to capture "victim payments" and is not dependent on there being an attempt to disguise any

	property, including funds, as something other than proceeds of an indictable offence.
3.5	The money laundering definition is not tied to any specific predicate offence and in principle covers any indictable offence.

Chapter 4 – SHARING VIA DESIGNATED PLATFORMS

Designation criteria	
4.1	Under section 68AAM of Part XIIAA, the MA may designate platforms for the purposes of the information sharing mechanism and, in so doing, must identify the operator of such platforms. The term "**platform**" includes an electronic system and any other mechanism, which allows for non-electronic platforms to be used. However, in practice, it is likely that all designated platforms will be electronic.
4.2	The key criteria that the MA will take into account when deciding to designate a platform include: (a) the identity of the participants in the platform; (b) the manner in which the platform is operated and, if applicable, the person who operates the platform; (c) the arrangements and protocols relating to the security and confidentiality of information transferred through or accessed on the platform; and (d) any other matter the MA considers relevant.
Financial Intelligence Evaluation Sharing Tool (FINEST)	
4.3	FINEST is the primary platform used for "own-initiative" sharing under section 68AAC(4) and onward disclosure under section 68AAD(2). It is operated by the HKPF, and the HKMA has access to the platform.
ICLNet	
4.4	ICLNet is a platform operated by HKICL Services Limited (HSL)[4]. ICLNet is a highly secure network platform and is the primary platform for the "request and response" procedure under sections 68AAB(1) and 68AAC(1).
Access to designated platforms	
Participating AIs	
4.5	Under section 68AAH, the MA may give written approval to an AI to access a designated platform for the purposes of information sharing under Part XIIAA, provided the MA is satisfied that the

[4] HSL is a wholly-owned subsidiary of Hong Kong Interbank Clearing Limited (HKICL), which is a private company jointly owned by the HKMA and the Hong Kong Association of Banks (HKAB).

	AI has adequate systems of control for ensuring its compliance with the requirements under Part XIIAA. An AI may only access a designated platform for the purposes of information sharing under Part XIIAA if the MA's approval is in force. The requirement to have adequate systems of control is a continuing one and the HKMA will review such systems of control as part of its supervisory work from time to time.
4.6	In determining whether the AI has adequate systems of control, the MA will take into account the AI's: (a) information technology and other arrangements for accessing designated platforms; (b) internal systems of control for safeguarding the security and confidentiality of information shared, including information disclosed to and received from other AIs under the Part XIIAA information sharing mechanism, and for ensuring that such information is only accessed by specialist staff of the AI (generally those engaged in financial crime compliance, audit or other relevant functions), although it may be shared with other staff when necessary for the conduct of their duties; (c) internal systems of control for ensuring that information is only disclosed, and information received is only used, for the purposes of detecting or preventing prohibited conduct; and (d) governance arrangements, including senior management oversight, for ensuring the controls are properly implemented and kept up-to-date.
Hong Kong Monetary Authority (HKMA)	
4.7	The HKMA has access to both FINEST and ICLNet. The HKMA will use this access primarily for supervisory purposes, including monitoring usage of the systems for information sharing and, where necessary, following up on complaints. The HKMA will not access the information shared except for the purposes of carrying out the MA's functions under the BO.
Joint Financial Intelligence Unit (JFIU)	
4.8	Under section 68AAJ(1), JFIU officers may access information disclosed under sections 68AAC(4) (own-initiative disclosure) or 68AAD(2) (onward disclosure). JFIU does not have access to

	information shared under the request and response procedure. If the AI(s) involved in a request and response procedure decide that the activity they have become aware of reaches the threshold for suspicious transaction report (STR) filing and subsequently file an STR(s), JFIU will have access to the information disclosed under section 25A of the Organized and Serious Crimes Ordinance (OSCO) (Cap. 455) and equivalent provisions of the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) (Cap. 405) and the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) (Cap. 575).
4.9	Section 68AAJ(1) is included because there may be occasions when an AI needs to share information via FINEST urgently before it has been able to file an STR. In such cases, JFIU requires swift access to the information but would not yet have such access under the relevant provision of OSCO, DTROP or UNATMO.
Platform operators	
4.10	Under section 68AAJ(3), the operator of a designated platform (e.g. HSL for ICLNet) may also have access (subject to any conditions imposed by the MA) for the purpose of operating the platform.

Chapter 5 – OFF-PLATFORM SHARING

5.1	Requests and disclosures must be made on designated platforms unless the MA has given written approval for a request or disclosure to be done by other means, in accordance with any conditions he may impose[5]. The intent of the relevant provisions is to cater for exceptional circumstances where it is necessary or expedient for AIs to share information "off-platform".
5.2	Examples could include situations where: (a) an AI that is a participant in a designated platform (e.g. FINEST) becomes aware that funds that have been transferred to its accounts may be involved in prohibited conduct, but those funds have already been transferred to another AI that is not a participant in the designated platform; (b) a non-participating AI becomes aware that one of its relevant entities may be involved in prohibited conduct and that there is a nexus to one or more other AIs (which may or may not be participating AIs) and wishes to alert them; or (c) an AI that is a participant in a designated platform needs to share information with one or more other participating AIs urgently and doing so off-platform will, in the particular circumstances of the case, be quicker. In such cases, it may be necessary or expedient for information to be shared other than via a designated platform, although this should generally only be done where there is a clear reason, e.g. in cases involving particularly large or frequent transfers, or where an urgent alert is necessary to facilitate the freezing of funds.
5.3	Where such a situation arises, the AI that wishes to pass information off-platform should approach the HKMA. The HKMA will consider whether approval should be granted and, where appropriate, liaise with the AI to which the information is to be sent (receiving AI). The MA may consider giving a general, non-case specific, approval to AIs participating on a given designated platform, subject to any conditions the MA considers

[5] See sections 68AAB(4), 68AAC(6), 68AAD(5) and 68AAE(4).

	appropriate, to cater for unusual situations such as those envisaged in paragraph 5.2(c).
5.4	In many cases, it may be possible to use ICLNet for such sharing and the MA may consider giving the disclosing and/or receiving AI temporary approval to use ICLNet for the purposes of Part XIIAA. In other cases, it may be necessary to use other means such as paper correspondence, a secure email channel, face-to-face meetings facilitated by the HKMA or a combination of these. In such cases, the primary consideration will be to ensure the confidentiality of the information passed and the MA may impose conditions to ensure that this is achieved.
5.5	There remains a need to comply with section 68AAJ(1) for off-platform sharing. This may be achieved by copying correspondence, via ICLNet or otherwise, to JFIU. It may also be expedient to inform other AIs which have provided or received related information via FINEST that the information has been passed to a non-participating AI off platform.
5.6	It is expected that off-platform sharing will be more relevant for own-initiative sharing (section 68AAC(4)) and onward sharing (section 68AAD). However, if an AI is of the opinion that it needs to make a request under section 68AAB(1) off platform, it may approach the HKMA to seek approval.

Chapter 6 – REQUEST AND RESPONSE

6.1	Section 68AAB(1) allows an AI (institution A) to request information from another AI (institution B) in relation to an entity or associated account or transaction as further described in paragraphs 6.5 to 6.9 below. Institution A is not required to obtain the consent of the entity to which the request for information relates if institution A has reasonable grounds to believe that seeking such consent would risk prejudicing its conduct of inquiries for detecting or preventing prohibited conduct.
6.2	Section 68AAC(1) permits an AI that receives a request for information made under section 68AAB(1) (requested AI) to disclose to the institution making the request (requesting AI) any information that relates to an entity, account or transaction identified in the request, or subject to section 68AAC(3) (see paragraph 6.4 below), any information that relates to an entity, account or transaction not identified in the request.
6.3	Section 68AAC(2) sets out the circumstances under which a response to a request may be made. These are that the requested AI has reasonable grounds to believe that the disclosure may assist the requesting AI in its inquiries and that seeking consent of any entity to which the information relates would risk prejudicing the requesting AI's conduct of such inquiries.
6.4	Section 68AAC(3) provides that a requested AI, in responding to a request under section 68AAB(1), may only disclose information relating to an entity, account or transaction that is not identified in the request if it has reasonable grounds to believe that such entity, account or transaction is associated with an entity, account or transaction that is identified in the request.
Making requests under section 68AAB(1)	
6.5	Section 68AAB(2) sets out the circumstances in which a requesting AI (institution A) may make a request for information from a requested AI (institution B). These include, among other things, that institution A becomes aware of activity that, in the opinion of institution A, warrants inquiries for assessing whether an entity or associated account or transaction may be, or may have been, involved in or associated with any prohibited conduct; and that institution A knows that institution B has information, or has

	reasonable grounds to believe institution B is likely to have information, relating to the entity or associated account or transaction that may assist in institution A's inquiries for detecting or preventing prohibited conduct. "Reasonable grounds to believe" in this context will in practice usually mean that there is a transaction nexus linking the customer or account of institution A (that institution A believes warrants inquiries), with a customer or account at institution B. AIs should not make general or "fishing expedition" requests.
6.6	Institution A is not required to seek the consent of its own relevant entity (customer), an associated entity of its relevant entity or a relevant entity of institution B or an associated entity of such relevant entity of institution B that is the subject of the request provided institution A has reasonable grounds to believe that seeking such consent risks prejudicing the conduct of its inquiries. This is likely to be the case where there are questions as to whether the customer, account or transaction may be involved in or linked to prohibited conduct based on fraud typologies observed and there is a risk of "tipping off" someone potentially engaged in such conduct. This may also be the case if, in a particular given circumstance, there is a need to conduct inquiries very quickly in order to prevent the occurrence of potential imminent prohibited conduct and the requesting AI (institution A) is unable to contact a particular customer quickly enough to obtain consent. This will be a question of fact in each case and there can be no general assumption that the possibility of delay in going through the process of seeking consent will always be sufficient to prejudice the conduct of inquiries.
6.7	As noted at paragraph 2.2, the definition of ***"money laundering"*** covers payments by potential victims, so that the relevant entity of institution A may be a victim of fraud or other crime. There may therefore be circumstances where it is possible and practicable to seek consent, e.g. where institution A's customer may be a victim of fraud or other criminal activity. In such cases, the requesting AI should consider seeking the customer's consent to request information from another AI. However, there may be cases where the AI suspects that a customer may be a victim but the customer insists on proceeding with the transaction. There

	may also be a risk that the customer could alert the suspected criminal. In such cases, the AI may consider whether to make a request under section 68AAB(1) without seeking the customer's consent since, if the customer refuses consent, this would prejudice the conduct of the requesting AI's inquiries.
6.8	In each case, AIs should consider whether seeking consent would risk prejudicing the conduct of inquiries, keep a record of any decision made and be prepared to make such record available to the HKMA on request.
6.9	Requests for information by an AI under section 68AAB(1) (which should include the items specified in section 68AAB(5)) may relate to (i) a "relevant entity" of institution A, i.e. a customer or a person with whom the AI maintains or has maintained a business relationship, or for whom the AI has conducted or has been asked to conduct an occasional transaction; (ii) an entity, account or transaction associated with such relevant entity of institution A or with an occasional transaction that institution A has conducted or has been requested to conduct for such relevant entity; (iii) a relevant entity of institution B; or (iv) an entity, account or transaction associated with such relevant entity of institution B or with an occasional transaction that institution B has or may have conducted for such relevant entity. Association need not be a formal association as between individuals in a legal arrangement or between corporate entities, but may include links such as common directors, beneficial owners or signatories; shared postal or IP addresses; or other digital footprint information.
6.10	The request and response procedure is likely to take place before an STR has been filed. Institution A will have become aware of activity that gives rise to questions and will seek information from institution B to assist it in assessing whether there is a risk of prohibited conduct in relation to the relevant entity, account or transaction. Institution A will then decide whether or not to file an STR taking into account any information received from institution B.
6.11	That said, the legislation does not preclude requests for information being made after an STR has been filed if institution A is satisfied that the activity it has observed already meets the

	threshold for filing an STR, but has reasonable grounds to believe institution B may have information that will assist it in its inquiries, which may lead to further or supplemental STRs.
Responding to requests under section 68AAB(1)	
6.12	Where AIs receive requests made under section 68AAB(1) (requested AI) , the requested AI is expected to: (a) acknowledge receipt immediately; (b) respond substantively wherever possible and as soon as reasonably practicable provided the circumstances in section 68AAC(2) are met; (c) identify in its response the information that is disclosed for the purposes of Part XIIAA; and (d) give an interim response within 3 working days if unable to provide a substantive response earlier. The interim response should indicate a timeframe for a substantive response if possible. In accordance with section 68AAC(6), disclosures in response to requests under section 68AAB(1) must be made via a designated platform (unless the MA has given prior written approval for off-platform sharing). To avoid possible errors, AIs are encouraged to conduct all of steps (a) to (d) above via the designated platform on which the request was received. Requested AIs should keep a record of decisions on whether to respond to requests and any responses provided and be prepared to make such record available to the HKMA on request.
6.13	Section 68AAC(2) sets out the circumstances in which disclosure in response to a request may be made. These include that the requested AI has reasonable grounds to believe that: (a) disclosing the requested information may assist the requesting AI in its inquiries referred to in section 68AAB(2)(b). "Reasonable grounds to believe" in this context will include the fact that there is a transaction nexus or other substantive link between the relevant entity, account or transaction of the requesting AI and the entity, account or transaction of the requested AI referred to in the request; and

	(b) seeking the consent of any entity to which the information relates would risk prejudicing the requesting AI's conduct of inquiries.
6.14	Section 68AAC(1)(b) also permits the requested AI to disclose information relating to an entity, account or transaction that is <u>not</u> identified in the request, provided that it has reasonable grounds to believe that the entity, account or transaction is associated with the entity, account or transaction identified in the request. Indicators of association that would constitute reasonable grounds to believe could include: (a) transaction nexus; (b) common directors, signatories, trustees, beneficiaries, etc. (for legal person or arrangements); (c) common IP addresses, devices or other digital footprint data; (d) other information or characteristics indicating that the entities, accounts or transactions are linked or may be controlled or operated by the same person(s) or form parts of a network, e.g. of mule accounts.
6.15	The requested AI is not expected to conduct its own investigation of whether the requesting AI's reasons for requesting the information are justified, and in most cases it will not be in a position to do so.

Chapter 7 – OWN-INITIATIVE SHARING

7.1	Section 68AAC(4) allows an AI (disclosing AI) to disclose information to another AI (receiving AI) at its own initiative (i.e. not in response to a request under section 68AAB(1)) relating to a relevant entity of the disclosing AI; or an entity, account or transaction associated with such relevant entity; or with an occasional transaction that the disclosing AI has conducted or been requested to conduct for the relevant entity. It is worth noting that such disclosure can be made to more than one AI.
Circumstances under which information may be shared	
7.2	Section 68AAC(5) sets out the circumstances under which own initiative disclosure can be made under section 68AAC(4). These include that the disclosing AI has become aware of activity by a relevant entity or associated entity, or in relation to an associated account or transaction, that (i) it has reasonable grounds to believe indicates involvement in or association with prohibited conduct; (ii) the disclosing AI is of the opinion that the information may assist the receiving AI in detecting or preventing prohibited conduct; and (iii) the disclosing AI has reasonable grounds to believe that seeking consent of any entity to which the information relates would risk prejudicing the receiving AI's detection or prevention of prohibited conduct.
7.3	An AI (disclosing AI) may disclose information relating to a relevant entity (i.e. customer) or an entity, account or transaction associated with such relevant entity or an occasional transaction the disclosing AI has conducted or been requested to conduct for the relevant entity.
7.4	An AI disclosing information on its own initiative is also likely to file an STR in respect of the entity or account to which the disclosure relates, although own initiative information sharing under section 68AAC(4) is not conditional on having filed an STR. In many cases, the AI will have received intelligence from law enforcement in Hong Kong or, potentially, outside Hong Kong (e.g. via group entities). In other cases, the AI itself will have observed activity that raises significant red flags indicating possible involvement in or associated with prohibited conduct, or received complaints from purported victims or their representatives. In any case, AIs should not wait until STRs are

	filed before sharing information as the STR filing process may take some time.
7.5	"Reasonable grounds to believe" in the context of involvement in or association with prohibited conduct would include: (a) intelligence or other information from law enforcement, possibly related to requests for information; (b) intelligence or information from group entities; (c) information from scam victims or persons acting on behalf of scam victims; or (d) activity observed by the AI, indicating possible involvement, directly or indirectly, in prohibited conduct or links to entities, accounts or transactions known or reasonably believed to be involved in prohibited conduct.
AIs with which information may be shared	
7.6	In these circumstances, the AI (disclosing AI) may disclose information to another AI (receiving AI) if it is of the opinion that the information may assist the receiving AI in detecting or preventing any prohibited conduct. Information may be disclosed to more than one AI and it is not necessary in each case for there to be a transaction nexus linking the entity or account that is the subject of the disclosure, or any associated entity or account, to an entity or account held by the receiving AI.
7.7	Information shared at the AI's own initiative will be posted on FINEST and should generally only be disclosed to AIs that participate in FINEST. Any AI that believes it is necessary or expedient to share information with an AI that is not a participant in FINEST should approach the HKMA (see Chapter 5 on Off-Platform Sharing).
7.8	A disclosing AI should consider whether the information is likely to assist the receiving AI in detecting or preventing prohibited conduct. In some cases, this may only apply to one AI or a distinct group of AIs, e.g. where the activity relates to a specific case in which the suspicion arises from a clear transaction nexus with any entity or account of one receiving AI or a distinct group of receiving AIs, in the absence of apparent involvement of other

	AIs. In other cases, the information may relate to a person or legal entity that is believed to be part of a money-laundering network, and may support the detection or prevention of prohibited conduct, by enabling receiving AIs to apply enhanced monitoring and surveillance on entities with which a business relationship has been or is going to be established. In each case, the disclosing AI should consider whether to disclose the information to one or a group of AIs or to all AIs participating in FINEST.
7.9	Before making a disclosure without the consent of the entity to which the information relates, the disclosing AI must have reasonable grounds to believe that seeking consent would risk prejudicing the receiving AI's detection or prevention of prohibited conduct. As the disclosing AI must already have reasonable grounds to believe that identified activity indicates possible involvement in prohibited conduct, potential for prejudice might be perceived in relation to the risk of "tipping off" through the seeking of consent, causing a subject to take steps to evade further investigation or conceal their activity. In the own-initiative information sharing scenario, the subject of the information is also less likely (than in the request and response procedure) to be a potential victim. Notwithstanding the above, in each case the disclosing AI should assess the likelihood that seeking consent would risk prejudicing the objective of detecting or preventing prohibited conduct before making a decision whether or not to do so, keep a record of the reasons for the decision and be prepared to make the record available to the HKMA on request.
Onward sharing	
7.10	Section 68AAD allows onward sharing of information. This provision is designed for cases where an AI has received information disclosed under section 68AAC(4) (own-initiative sharing), and the receiving AI becomes aware that there is a nexus to another AI and is of the opinion that the information may assist that further AI in detecting or preventing prohibited conduct. Examples include cases where the receiving AI receives information that funds believed to be proceeds of crime have been transferred to one of its accounts, but those funds have already been transferred to another AI (further AI).

7.11	In such cases, the receiving AI may disclose the relevant information to the further AI without having to obtain the consent of any entity to which the information relates, provided it has reasonable grounds to believe that (i) any entity, account or transaction to which the information relates may be, or have been, involved in prohibited conduct, and (ii) seeking such consent would risk prejudicing the further AI's detection or prevention of any prohibited conduct. Any such disclosure should identify the information disclosed for the purposes of Part XIIAA.
7.12	The fact that the entity, account or transaction has been named in information disclosed by the original disclosing AI may be treated by the receiving AI as a significant, but not definitive in itself, factor in determining whether there is possible involvement in or association with prohibited conduct, before deciding whether to disclose information to the further AI. The receiving AI may consider seeking further information from the original disclosing AI via a request under section 68AAB(1) if the conditions for such a request in section 68AAB(1) and (2) are met.
7.13	Under section 68AAD(4), the receiving AI should not disclose the name of the original disclosing AI or any information that may identify it, without the disclosing AI's prior consent.
7.14	Similar considerations apply regarding the seeking of consent from entities to which information relates, as are discussed in paragraph 7.9.

Chapter 8 – CIRCUMSTANCES UNDER WHICH INFORMATION SHOULD NOT BE SHARED

8.1	There will be cases where sharing information is not appropriate. These include, but are not limited to, the following categories. AIs will need to exercise judgment in such cases and should consult either the HKMA or the relevant law enforcement agency if in doubt.
Sensitive cases	
8.2	There are some types of offence where information sharing is not appropriate or is unlawful. Separate guidance will be issued by the HKMA from time to time as required on the types of offence in respect of which information should not be shared without first seeking guidance/approval from the relevant law enforcement agency.
Non-AIs	
8.3	As noted in paragraph 3.1, information sharing under Part XIIAA is only permitted among AIs. AIs should not request information from or disclose information to any entity that is not an AI under the relevant provisions of Part XIIAA. Disclosure of information to a non-AI will not be covered by the "safe harbour" provided under section 68AAG.
Cases that may be subject to non-Hong Kong data privacy or other confidentiality requirements	
8.4	The safe harbour provision only has effect within Hong Kong. AIs should consider taking competent legal advice as necessary, for example whether they may be bound by data privacy or other confidentiality requirements in other jurisdictions in respect of certain customers, e.g. where business relationships are managed in Hong Kong but the relevant bank accounts or transactions are booked elsewhere with non-local affiliates of the AIs.

Chapter 9 – CORRECTION OF INACCURATE INFORMATION

Duty to correct inaccurate information	
9.1	AIs are expected to exercise reasonable care to ensure that information is accurate at the time it is shared. Nevertheless, it is possible that incorrect information may be shared, although such cases should be rare. It is also possible that information may change, or additional information is obtained, after the original disclosure. Given that receiving AIs are likely to act on information received and the potential consequences of such actions for those affected, it is important that any inaccuracies are corrected as soon as reasonably practicable. In addition, disclosing AIs are expected to update or amend information if they become aware that any information disclosed previously has changed or become outdated, and provide any additional information they become aware of subsequent to the original disclosure that is, in the disclosing AI's opinion, relevant and may assist receiving AIs in detecting or preventing prohibited conduct.
9.2	Section 68AAE(1) imposes a duty on an AI which discloses information to correct any inaccuracy in that information as soon as reasonably practicable after becoming aware of such inaccuracy. This applies to disclosure made in the course of making a request under section 68AAB(1), in response to such a request, as part of an own-initiative disclosure or via onward disclosure. Similarly, under section 68AAE(2), if an AI becomes aware that any correction made under subsection (1) is itself inaccurate or has become inaccurate, it must correct the inaccuracy as soon as reasonably practicable.
9.3	A correction of inaccurate information should be sent to all AIs to which the original information was sent using the same channel (i.e. designated platform or off-platform) as was used for the original disclosure. Any information that is disclosed for correcting an inaccuracy must be identified as such for the purposes of Part XIIAA.
9.4	The AI is not required to obtain consent from any entity to which the information relates. There is no reasonable grounds threshold in the case of disclosure for the purpose of correcting inaccuracy

	as the AI has already assessed whether seeking consent would risk prejudicing the detection or prevention of prohibited conduct, or in the case of a request under section 68AAB(1) the AI's conduct of inquiries, when making the original disclosure or request.
9.5	The duty to correct inaccurate information also applies to AIs that have made an onward disclosure under section 68AAD. Such AIs, on receiving a correction from the original disclosing AI, should pass on the correction to any AI to which an onward disclosure has been made as soon as reasonably practicable after receiving the correction.
9.6	If a requested AI that receives a request made under section 68AAB(1) and decides to respond substantively under section 68AAC(1) is aware that any information contained in that request is inaccurate, it is encouraged to inform the requesting AI of the inaccuracy in its response or as soon as reasonably practicable after becoming aware of the inaccuracy.
Treatment of corrected information	
9.7	Treatment of corrected information will depend on the nature of the inaccuracy: (a) In cases where the disclosing AI becomes aware that the information disclosed via FINEST was wholly inaccurate, e.g. where the wrong person has been named, the AI should arrange to delete the information from FINEST. A statement that the information has been found to be inaccurate and deleted should be posted in its place. (b) Disclosing and receiving AIs should update their own records, in particular any monitoring and screening systems, to reflect any correction of inaccuracies. However, it is acceptable to retain the original information in the AI's internal records if necessary to explain what changes have been made and the reasons for doing so for audit trail purposes, provided such information is stored in accordance with the AIs' internal policies and procedures regarding confidentiality. (c) Where information disclosed via FINEST is found to have become outdated or needs to be changed in light of events that the AI has become aware of since disclosure, it is acceptable to retain the original information on FINEST

	together with the correction and any supplementary information.
9.8	In all cases, when correcting inaccurate information, AIs should consider the possible adverse consequences for the interests of any persons affected and take appropriate steps to avoid or reduce such consequences where necessary, including deleting information where appropriate.

Chapter 10 – USE OF INFORMATION RECEIVED

10.1	Information shared under Part XIIAA may only be used for the detection or prevention of prohibited conduct. AIs receiving information must not use it for any other or collateral purpose (e.g. marketing).
Purposes for which information may be used	
10.2	A receiving AI may use information received for the following purposes: (a) to trigger a review of whether there is any reason to suspect that any of its customers or accounts may have received funds that are proceeds of an indictable offence and, if so, in determining what action to take, including whether to file STRs to the JFIU where appropriate[6]; (b) as a basis for implementing enhanced monitoring and surveillance of any customer or account where appropriate; (c) to trigger a review of existing customer due diligence (CDD) records of any customer and determine whether any further action is warranted as a result; and (d) as a factor in deciding whether to establish or maintain a business relationship bearing in mind paragraph 10.5 below.
10.3	In addition to entities, accounts or transactions identified in the disclosure received, receiving AIs may use information received for the purposes above in respect of any other entity, account or transaction that is associated with an entity, account or transaction identified in the disclosure received. Examples of association in this context include, but are not limited to: (a) where the AI finds that it has an account in the name of a person named in the disclosure that is not the account named in the disclosure or other accounts in different names that are associated with the person named in the disclosure; (b) where a corporate entity shares a beneficial owner, shareholder, director, or person purporting to act on behalf of the entity with an entity named in the disclosure; or (c) other forms of association such as shared mailing or IP addresses, device IDs or other digital footprint indicators.

[6] Where an STR is filed, the AI may include a note that the STR is based on intelligence received through FINEST.

10.4	When taking any of the actions set out in paragraph 10.2, a receiving AI is expected to make its own assessment, taking into account all available information, before deciding the appropriate course of action in accordance with its own policies and procedures. The fact that a receiving AI has received information disclosed under Part XIIAA may be considered as part of such an assessment, but should not be the sole basis for taking any action.
Avoidance of de-risking	
10.5	The information sharing mechanism under Part XIIAA is not intended to create "blacklists" or lead to automatic or indiscriminate "de-risking" or the exclusion of persons or classes of person from the banking system. The fact that an entity has been named in an information request under section 68AAB(1) or in any disclosure should be considered along with other information available to the AI when considering whether to exit a business relationship with that entity. Similarly, the fact that an entity has been identified in a request or disclosure should not be taken in insolation as a reason for declining to enter into a business relationship with that entity but rather it should be considered in conjunction with all other information available to the AI from various sources including information provided by the prospective customer.

Chapter 11 – CONFIDENTIALITY REQUIREMENTS

11.1	Although Part XIIAA permits the disclosure and use of information, including personal data as defined in the PDPO, for defined purposes, such information must be treated as confidential and only be disclosed as permitted by the relevant provisions of Part XIIAA or other legislation.
11.2	Section 68AAF specifically prohibits an AI from disclosing the fact that it has disclosed information in accordance with the relevant provisions of Part XIIAA to anyone except a JFIU officer, the MA or the operator of a designated platform. This is analogous to the "tipping off" provisions in OSCO, DTROP, etc., since revealing that information has been shared would obviously risk undermining the purposes of detecting or preventing prohibited conduct.
11.3	Section 68AAF(3) provides that a receiving AI may only disclose information disclosed to it as required or permitted by law or when ordered by a court, and may only use such information for detecting or preventing prohibited conduct.
11.4	The overall effect of these provisions is that AIs disclosing or receiving information should treat such information, and the fact that they have disclosed or received it, as confidential. Information should be subject to at least the same level of confidentiality as other customer information, in particular personal data, held by the AI. AIs should note that the provisions of the PDPO still apply to personal data.
11.5	Access to information to be disclosed and information received should be subject to specific protocols and in general should be limited to authorised staff whose duties include handling/investigating suspected financial crime. These staff will often also be those who have access to designated platforms. Access to information should only be granted to other staff where necessary for the conduct of their duties.
11.6	AIs should ensure that specialist staff designated to deal with disclosure of information and information received have appropriate training and experience, including in dealing with personal data and the provisions of the PDPO.

Chapter 12 – RECORD KEEPING REQUIREMENTS

12.1	Section 68AAI imposes a duty to keep records of any request for information under section 68AAB(1) that an AI makes or receives as well as any information that it discloses or receives under Part XIIAA: (a) in relation to a customer, throughout the business relationship and for at least five years from the end of the business relationship; (b) in relation to any other entity, for at least five years from the date when the request or disclosure is made.
12.2	Under section 68AAI(3), the MA may extend the period if he is satisfied that the record is relevant to an ongoing criminal or other investigation or any other purpose as specified by the MA.
12.3	These requirements are based on those in Part 3 of Schedule 2 to the AMLO so AIs are already subject to similar requirements with regard to CDD information. AIs may therefore find it convenient to keep records to meet the two sets of requirements in the same systems.
12.4	While information disclosed on FINEST will be available on the platform, it will generally be archived after 5 years and will then not generally be available to AIs. Since ICLNet is a network, secure emails transmitted are not stored on the platform. AIs are required to keep an "audit trail" of records relating to decisions to request or disclose information and to take action (if any) on the basis of information received. This type of information will generally not be posted on or shared via a designated platform. Storage in the designated platform will therefore not be sufficient to meet the record-keeping requirements in many cases.
12.5	AIs should also note that, where information comprises personal data, DPP2 (accuracy and duration of retention of personal data) under the PDPO continues to apply and AIs should establish and maintain policies, procedures and controls to ensure that personal data is not kept for longer than is necessary.

Deletion of Intelligence Sharing Reports (ISRs)	
12.6	AIs should establish and maintain procedures for deleting ISRs[7] in line with the record-keeping requirements in section 68AAI and the requirement to correct inaccurate information under section 68AAE, taking into account the provisions of DPP2 of the PDPO.

[7] ISRs are the means by which information is shared on FINEST in accordance with the relevant provisions of Part XIIAA.

Chapter 13 – RELATIONSHIP WITH THE SUSPICIOUS TRANSACTION REPORT REGIME

ISR is not an STR	
13.1	The information sharing mechanism under Part XIIAA is not intended to modify or replace the STR regime. In particular, an ISR does not count as an STR and posting information to a designated platform does not relieve an AI of its obligation under the relevant legislation to file STRs. AIs should keep in mind the need to file STRs as soon as reasonably practicable to ensure that relevant information is passed to the JFIU in good time.
Not tipping off	
13.2	Section 68AAG(3) provides that disclosure of information under the relevant sections of Part XIIAA does not constitute an offence under the "tipping off" provisions of DTROP, OSCO or UNATMO. Nevertheless, AIs disclosing or receiving information should exercise appropriate care not to reveal that an STR has been filed.

Chapter 14 – COMPLAINT HANDLING AND DATA ACCESS REQUESTS

Complaints	
14.1	Customers of AIs in respect of whom information is shared under Part XIIAA will generally not be aware of that fact. Indeed AIs are barred under section 68AAF(1) from disclosing that information has been shared except in very limited circumstances.
14.2	However, customers will be aware of the existence of the information sharing mechanism and the designated platforms. It is therefore likely that customers whose accounts are suspended or closed, or whose applications to open accounts are declined, may lodge complaints with AIs alleging that their information has been shared. Such complaints require careful handling and AIs should establish and maintain policies, procedures and controls for doing so in line with the HKMA SPM IC-4 as part of their general complaint-handling processes. In responding to such complaints, AIs should avoid confirming whether or not information has been shared under Part XIIAA. Any confirmation that it has would contravene section 68AAF(1). Confirmation that information has not been shared would risk implying that information has been shared in other cases where a different reply is given, which could indirectly contravene section 68AAF(1).
14.3	Whether or not a customer alleges in a complaint that information has been shared, an AI receiving a complaint relating to suspension, closure or refusal of a business relationship should check whether information was in fact disclosed or received under the provisions of Part XIIAA and this was a factor in the decision to take any action. If this was the case, the AI should review decisions made and whether they were appropriate in accordance with its usual complaint handling procedures and HKMA SPM IC-4.
Data access requests	
14.4	Section 20(3)(ea) of the PDPO provides that a data user may refuse to comply with a data access request if the data user is entitled under the PDPO or any other Ordinance not to comply with the request. Section 68AAK of Part XIIAA of the BO

	provides that an AI, the MA, a JFIU officer or a designated platform operator is entitled not to comply with a data access request in relation to any information disclosed under section 68AAB(3), 68AAC(1) or (4), 68AAD(2) or 68AAE(3) of Part XIIAA of the BO for the purposes of section 20(3)(ea) of the PDPO.
14.5	However in such circumstances section 21(1) of the PDPO will require that a notice of the refusal to comply with the data access request (refusal notice) be given to the requestor and that this notice should include reasons for the refusal.
14.6	Alternatively, under section 58(1) of the PDPO where personal data is held for the purposes of the prevention or detection of crime it is exempt from DPP6 (access to personal data) and from the obligation (under section 18(1)(b) of the PDPO) to supply a copy of any data held in response to a data access request, in circumstances where to grant access or supply such copy would likely prejudice the prevention or detection of crime. This might, depending upon the circumstances, cover personal data in the hands of a receiving AI under the information sharing mechanism in Part XIIAA insofar as: (i) the data has been received and is held by the recipient solely for assessing involvement in, or assisting in the detection or prevention of, prohibited conduct (i.e. crime); and (ii) disclosure of the data being in the receiving AI's hands could in turn reveal or prompt suspicion that the information has been shared between AIs for the detection or prevention of prohibited conduct and thus potentially provoke prejudicial evasive action to conceal activities or avoid further investigation.
14.7	Where a data access request relates to personal data which is exempt from section 18(1)(b) of the PDPO by virtue of section 58 of the PDPO – section 63 of the PDPO may provide a further exemption from the obligation under section 18(1)(a) of the PDPO to inform a requestor, in response to a data access request, whether any personal data is held in respect of that individual in circumstances where such disclosure would likely prejudice the prevention or detection of crime. Section 21(2) of the PDPO will then permit a refusal notice just to inform the requestor that the data user has no personal data the existence of which it is required to disclose to the requestor (or words to like effect). In other words, no reason for the refusal has to be given if reliance can be

	placed on section 58 / 63 / 21(2) of the PDPO to refuse to comply with a data access request.
14.8	An AI wishing to avail itself of section 21(2) of the PDPO should note that it would be doing so under the PDPO regime, rather than Part XIIAA of the BO, and must meet all relevant criteria under the PDPO.

GLOSSARY OF KEY TERMS & ABBREVIATIONS

Terms / abbreviations	Meaning
AIs	Authorized institutions
AML/CFT Guideline	Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions)
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
BO	Banking Ordinance (Cap. 155)
CDD	Customer due diligence
DPPs	Data Protection Principles
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
FINEST	Financial Intelligence Evaluation Sharing Tool
HKAB	The Hong Kong Association of Banks
HKICL	Hong Kong Interbank Clearing Limited
HKMA	Hong Kong Monetary Authority
HKPF	Hong Kong Police Force
HSL	HKICL Services Limited, a wholly-owned subsidiary of HKICL
ICLNet	HKICL Network, a secure network platform operated by HSL
ISR	Intelligence Sharing Report
JFIU	Joint Financial Intelligence Unit
MA	Monetary Authority
ML/TF	Money laundering and terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
Part XIIAA	Part XIIAA of the BO
PCPD	Office of the Privacy Commissioner for Personal Data
PDPO	Personal Data (Privacy) Ordinance (Cap. 486)
SPM	Supervisory Policy Manual issued by the HKMA
STR	Suspicious transaction report
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
WMD	Weapons of mass destruction