HONG KONG MONETARY AUTHORITY

GUIDANCE PAPER

Transaction Monitoring, Screening and Suspicious Transaction Reporting

Revised in February 2023

1 Introduction

Background and scope

1.1 This Guidance Paper replaces the "Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting", which the Hong Kong Monetary Authority (HKMA) first published in 2013 and updated in 2018. The updates in this Guidance Paper take into account changes in the use of data and technology, key observations from the HKMA's recent thematic reviews, enforcement actions, industry best practices, and feedback from the Joint Financial Intelligence Unit (JFIU) on quality and consistency of suspicious transaction reporting.

1.2 This Guidance Paper should be read in conjunction 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) (AML/CFT Guideline), other guidance issued by the HKMA and relevant competent authorities, and other applicable laws. The AML/CFT Guideline sets out relevant statutory[1] and regulatory requirements. While this Guidance Paper does not form part of the AML/CFT Guideline, it supplements the HKMA's principle-based requirements by providing practical guidance on the measures Authorized Institutions (AIs) can take, in the areas of transaction monitoring, screening and suspicious transaction reporting, to mitigate money laundering (ML), terrorist financing (TF), financial sanctions and proliferation financing (PF) risks.

1.3 The HKMA expects AIs to give consideration to adopting the practices this Guidance Paper describes, where appropriate, to improve their risk-based AML/CFT policies, procedures and controls (AML/CFT Systems), taking into consideration the nature, size and complexity of their businesses and the ML/TF risks that arise.

[1] The statutory requirements include obligations under the United Nations Sanctions Ordinance (UNSO), the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO), other ordinances with provisions requiring suspicious transaction reporting (i.e. the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405, and the Organized and Serious Crime Ordinance, Cap. 455), and the AMLO.

Use of technology and data

1.4 Transaction monitoring and screening are areas where AML/CFT technology application is comparatively mature; therefore, this Guidance Paper takes into account recent technological advances and good practices, the increased focus on data quality and integration of external data[2] as supporting pillars for effective AML/CFT Systems. AIs should make reference to other guidance and material[3] on the adoption and innovation of AML/CFT technology issued by the HKMA, and continue to review the use of technology to help make their systems and processes more effective and efficient on an ongoing basis.

[2] For example, AIs are encouraged to explore greater use of data from the Commercial Data Interchange (CDI) to help make systems for customer due diligence and data-driven risk assessment and monitoring more effective.

[3] To promote AIs' adoption of AML/CFT Regtech, the HKMA AML webpage has rolled out a section of AML/CFT Regtech, serving as the central repository and one-stop reference of AML Regtech-related information (https://www.hkma.gov.hk/eng/key-functions/banking/anti-money-laundering-and-counter-financing-of-terrorism/aml-cft-regtech/).

2 Transaction Monitoring

2.1 The AML/CFT Guideline provides principle-based guidance on how AIs should design and implement their transaction monitoring systems and processes taking into account various factors, and how the risk-based approach is adopted. Generally, transaction monitoring systems and processes cover the following core elements:

(a) a transaction monitoring system producing alerts or, in the case of very simple business models, relevant reports generated by management information system (MIS) (or a combination of both) to help identify suspicious transactions or abnormal transaction patterns; and

(b) processes to review those alerts or MIS reports, including examining the background and purposes of transactions, cross-checking the customer profiles, making enquiries if necessary and documentation of findings, outcomes and rationales for any decision made (e.g. closing the alert or escalating for further investigation) to provide a sufficient audit trail.

Systems used for Transaction Monitoring

System adoption

2.2 AIs should be able to demonstrate that their transaction monitoring systems and processes are effective taking into account the factors stipulated in Chapter 5 of the AML/CFT Guideline. For the majority of AIs, this may require some level of automation generally involving one or more rules-based or scenarios-based systems to produce alerts or MIS reports to aid identification of suspicious transactions for further examination. As stated in the AML/CFT Guideline, the design, degree of automation and sophistication of transaction monitoring systems and processes are institution-specific, and the appropriateness of systems is determined by a range of factors, including the AI's ML/TF risk exposure.

2.3 Before adopting a particular transaction monitoring system, AIs should conduct a comprehensive assessment and document the rationale for adopting the system, including how it meets the AI's needs and other relevant factors such as the appropriateness of the system vendor, compatibility of the new system with the AI's existing IT infrastructure, how system changes will be performed and managed, and any resource implications.

2.4 Adopting an off-the-shelf system provided by a vendor or head office without adequately taking into account AI's specific risks and context is unlikely to be sufficient for meeting relevant legal and regulatory requirements. The responsibility to mitigate ML/TF risks always lies with the AI, not with the system or its vendor.

2.5 In addition to automated systems, MIS reports may also be used for transaction monitoring, especially where the AI concerned is small in scale and the business model is comparatively simple. These may also be used to supplement rules-based or scenarios-based systems in monitoring specific risks or typologies. Where an AI solely relies on MIS reports, it should keep under regular review the need to adopt a more sophisticated automated transaction monitoring system especially when there is a material change to its business or risk exposure.

System design

2.6 No single transaction monitoring system will suit every AI, so the design of the system must be specific to individual AIs. A transaction monitoring system usually consists of various rules and scenarios based on common ML/TF typologies and transaction patterns or activities. These rules and scenarios should be relevant to an AI's identified ML/TF risks and its operations, and the rationales for adopting them should be well understood and documented by the AI.

2.7 A transaction monitoring system usually allows AIs to customise their own rules and scenarios and adjust underlying parameters and thresholds (e.g. monetary value, time period covered, count of transactions, etc.) based on different circumstances. It is important that the parameters and thresholds used are appropriate to effectively identify unusual or suspicious transactions and activities in the context of the AI's individual ML/TF risk profile. In addition, new or changed parameters and thresholds should be appropriately tested to ensure their proper functioning and that alerts are generated as intended.

2.8 A transaction monitoring system should have appropriate customer segmentation to allow the system to operate effectively, and generate more targeted, higher-quality alerts. In practice, AIs may group customers with similar characteristics into segments, taking into account factors including the business nature of the customers, products and services offered, and customer risk rating, etc. The same sets of parameters and thresholds are applied for each segment.

2.9 Customer segmentation and calibration of parameters and thresholds require skilled experts who have sufficient understanding of the AI's transaction monitoring systems and processes. AIs may consider employing technology or statistical tools and methods, e.g. above-the-line and below-the-line testing, to help identify the best configuration and calibration to reduce the number of false positive alerts. Factors to be considered include efficiency of existing rules, numbers of true hits, and false positives or negatives generated by the tests performed.

2.10 An AI should understand clearly how any model or mechanism (e.g. score deduction mechanism, hibernation model, etc.) works within the transaction monitoring system and its impact on optimising the monitoring capability. There should be appropriate validation and scrutiny to ensure that the level of optimisation is consistent with that intended and ensure that the system operates within the AI's risk appetite.

Data

2.11 Accurate data is a prerequisite for an effective transaction monitoring system. Validation of the integrity, accuracy and quality of data is imperative to ensure that complete and relevant data from core banking system and other source systems are used in the transaction monitoring system. Regular assurance testing on data quality and lineage should be conducted.

System oversight and review

2.12 Measures should be in place to ensure sufficient oversight by senior management of the development and implementation of the transaction monitoring system (including any models or mechanisms applied) to facilitate timely implementation of decisions and progress reviews. Senior management has a role in overseeing the ongoing enhancement of the system with a view to ensuring that the key ML/TF risks are appropriately mitigated. Major issues in system implementation should be promptly and appropriately addressed in the relevant management committee and escalated to senior management to ensure they are adequately resolved, with discussion and justification for decisions

properly documented.

2.13 Objectives and key performance indicators of the transaction monitoring system should be defined to facilitate monitoring of system effectiveness and efficiency. System performance should be subject to management oversight and appropriate detection controls (e.g. exception reports) can also help identify abnormalities which should be escalated for timely rectification.

2.14 AIs should periodically review the adequacy and effectiveness of the transaction monitoring systems and processes, including an assessment of the transaction characteristics the system monitors, risk factors, parameters and thresholds used (whether or not these generate alerts), and any alert prioritisation or discounting mechanism applied to ensure they remain optimal and address ML/TF risks, taking into account changes in business operations and new and emerging ML/TF typologies. This involves review of both outputs (e.g. the number of alerts) and outcomes (e.g. the actual cases warranting in-depth investigation and reporting). Where applicable, the transaction monitoring system should support integration of information and data from external sources as and when necessary to enhance targeting and mitigation of specific ML/TF risks[4].

Alert or MIS Report Handling and Documentation[5]

2.15 Robust alert review processes are required to effectively identify suspicious transactions for filing of suspicious transaction reports (STRs) to the JFIU. When reviewing alerts, AIs must be satisfied that the abnormalities identified can be explained before the alerts are cleared or closed.

2.16 Review of alerts relies heavily on specialised knowledge and expertise. Therefore, it is important to ensure the quality, accuracy and consistency of alert handling through clear and comprehensive policies and procedures, and adequate training. Staff responsible for review should be familiar with the design and operation of the transaction monitoring system.

---

4 For example, enhancing the scenario coverage of the transaction monitoring systems based on the latest typologies and risk indicators shared by law enforcement agencies including Fraud and Money Laundering Intelligence Taskforce (FMLIT) Alerts.

5 For the purpose of this section, alerts cover those generated from automated system and MIS reports. Reference should also be made to the guidance provided from paragraphs 3.12 to 3.15 on handling of alerts generated from the screening system as the same principles with regard to governance and oversight and documentation are applicable to transaction monitoring alert clearance process.

2.17 Staff responsible for reviewing alerts should refer to customer due diligence (CDD) profiles and record of previous alerts or reports on the customer. Where the existing information possessed by AIs is not sufficient for them to clear or close the alerts, AIs may need to approach the customer in order to understand the background and purpose of transactions identified by the system. While AIs are not expected to obtain supporting documents (e.g. invoices) of transactions in all cases, they should be critical and not accept at face value a simple but insufficient explanation provided by customers. Where necessary, AIs should ask further questions or request additional information.

2.18 Internet searches and checks against public or open-source information may also help explain unusual or abnormal transactions and activities. AIs may consider providing the responsible staff with commercial databases, solutions or tools to facilitate the review.

2.19 Appropriate mechanisms and procedures should be established to triage alerts which must be reviewed to enable AIs to make STRs as soon as it is reasonable to do so. Larger AIs commonly divide the review process into different levels. No matter how an AI designs its review processes, it should establish clear and reasonable internal timelines and procedures to monitor adherence.

2.20 There should be procedures for escalation and management of backlogs in alert review processes. Significant and prolonged backlogs may indicate ineffective transaction monitoring systems and processes; concerns regarding resourcing for alert handling; poor design of transaction monitoring rules, scenarios, parameters or thresholds; and/or inappropriate customer segmentation. Where significant backlogs or overdue alerts arise, senior management or the relevant risk committee should be informed and take appropriate measures to identify and address the root cause(s) and clear the backlog.

2.21 Sufficient documentation should be maintained to evidence the review of alerts, and determination of whether the transaction activities or patterns highlighted were suspicious or not. AIs should be cautious about using pre-defined answers for clearance of alerts. Generally, evidence of alert-by-alert consideration tailored to the specific circumstances of each customer and/or alert is expected.

2.22 AIs should establish an effective assurance programme to regularly and independently review the quality and consistency of alert clearance. The level of review should be commensurate with the circumstances including nature and size of business operations, complexity of review processes and procedures, and volume of alerts. Observations from such assurance reviews can also support enhancement of the transaction monitoring systems and processes.

3 Screening

3.1 Chapter 6 of the AML/CFT Guideline sets out the HKMA's expectations for AIs regarding TF, financial sanctions and PF, one of which is the establishment of effective sanctions screening systems and processes. These generally require:

(a) comprehensive and up-to-date screening databases;

(b) appropriate system setting and tuning;

(c) clear procedures for handling potential name matches; and

(d) processes to regularly review the effectiveness of the above elements.

3.2 The HKMA recognises that individual screening systems vary in degree of automation and sophistication, and there is no one-size-fits-all arrangement. These should be determined by each individual AI, through careful consideration of the nature, size and complexity of its businesses and an understanding of the risks to which it is exposed[6]. Additionally, there should also be clarity around ownership of, and accountability for, the relevant parts of the systems and processes, including which functions (e.g. compliance or IT unit or both) should manage them. These help to achieve system performance consistent with the AI's internal policies and risk appetite, and ensure compliance with relevant legal and regulatory requirements.

Maintenance of Screening Databases

3.3 Screening allows AIs to identify potential matches to persons sanctioned under Hong Kong law. This is usually achieved by cross-checking keywords that appear in an AI's normal course of business, such as in transactions or customer records, against names and identifiers[7] of persons designated under the UNATMO and the UNSO kept by the AI in form of databases.

[6] Such as customer type, the geographical regions where customers operate in, types of products and services provided by the AI, etc.

[7] Examples of such identifiers include nationalities, dates of birth, identification numbers, etc. (where applicable)

3.4 Regardless of whether the databases are maintained in-house or with support from a vendor (e.g. by subscribing to a commercial risk register), AIs should ensure the completeness and accuracy of the databases, and that these are updated in a timely manner. In addition, regular and frequent testing (such as periodic sample testing on names of newly added designations) should also be conducted.

3.5 A number of AIs rely on their head offices or other group entities to maintain and update the screening databases. It should be borne in mind that the ultimate responsibility for ensuring the accuracy and completeness of the databases rest with the AI, who should understand which lists and data are included in the screening databases and be able to explain any decisions made.

System Setting and Tuning

3.6 AIs should endeavour to strike the right balance between system effectiveness and efficiency[8] by applying appropriate system settings, which can be achieved by measures such as threshold tuning or monitoring levels of false positives. Examples of settings that can be applied to a screening system include thresholds of similarity for different identifiers such as names and dates of birth, or can take the form of algorithms which dictate conditions for which potential matches are flagged. These settings enable the screening system to identify alterations and variations commonly observed including the manipulation of names and keywords (e.g. re-ordering and swapping), as well as the use of different names with the same phonetics.

3.7 Given the importance of system tuning to performance, AIs should be able to demonstrate a clear understanding of the settings used in their screening systems, e.g. choices of configuration and how certain settings and filters are used, etc. AIs should ensure staff have relevant skills and knowledge to support deployment and ongoing maintenance. Upgrades or implementation of new screening systems should be appropriately tested and tuned prior to deployment, and should be subject to adequate oversight.

[8] Effectiveness refers in this context to the overall capability of the system in detecting / identifying a hit against a sanctioned person. Efficiency refers to the minimising of false positives.

3.8 Where optimisation functions or suppression lists (e.g. "good guy", "white" or exclusion lists) are used to enhance system efficiency, they should be subject to appropriate testing and oversight, which should occur before implementation of a new system or system enhancement. After implementation, AIs should regularly review the optimisation functions to ensure they remain valid and appropriate.

Handling of Potential Name Matches[9]

3.9 Policies and procedures should be in place to ensure appropriate and consistent handling and management of alerts generated from the screening systems. AIs should clearly identify the parties responsible for reviewing and clearing the alerts, and set out timelines for alert clearance. There should also be practical guidance to staff on situations where additional information from customers or respondent banks should be obtained to help better understand the background and purpose of the transactions or activities and support any further assessment. Conditions under which alerts must be escalated to higher review levels for more detailed analysis and approval authority required should be clearly documented in the AI's internal escalation policies and procedures.

3.10 The rationale for closing or escalating the alert should be documented in sufficient detail to provide an audit trail which demonstrates that the relevant legal, regulatory and internal requirements are being met. AIs should be cautious about using pre-defined answers for clearance of alerts.

3.11 Where business relationships, transactions or activities are assessed to be genuine hits, handling staff should escalate the case to a person with appropriate authority (e.g. senior management). Risk mitigating measures should be taken, and where appropriate, reports to the JFIU be made, as soon as it is reasonable to do so.

3.12 Where any part of the screening alert-handling is outsourced to servicing hubs of the AI's banking group (e.g. a regional specialist team or centre), the overall responsibility and accountability remains with the AI. AIs should ensure that the governance, systems and controls remain effective and adhere to both internal and local regulatory requirements.

[9] Reference should also be made to the guidance provided in paragraphs 2.15 to 2.22 on handling of alerts generated from the transaction monitoring system as the same principles with regard to governance and oversight and documentation are applicable to screening alert clearance process.

3.13 Based on their individual circumstances, AIs may choose to use automated, or other effective manual processes to handle names that use non-Latin script (including Chinese characters) or commercial codes. For example, they may use screening systems which are able to effectively generate alerts taking into account name variations from multiple Chinese Romanisation systems (e.g. Mandarin pinyin, Cantonese, Hokkien) and different types of Chinese characters.

Ongoing Review of the Screening Systems and Processes

3.14 Frequent and regular monitoring, tuning and testing should be conducted on all aspects of screening systems and processes, with testing results and analysis properly documented. AIs should also carry out regular independent review and quality assurance on screening systems and processes to provide adequate assurance.

3.15 Depending on the model adopted, AIs may rely on support from head office or other group entities to oversee the screening systems including maintenance and updating of the relevant databases. Senior management should have sufficient oversight of screening systems and processes to ensure their effectiveness and efficiency (including defining objectives and key performance indicators)[10]. Any system performance issues should be highlighted for senior management's attention to ensure they are promptly identified and rectified. Relevant staff of the AI are also expected to have adequate knowledge and understanding of the screening systems.

[10] Management information, such as information on volume of alerts, false positives and genuine hits, etc., should be made available to senior management, and be adequate to facilitate their understanding of the risks to which AIs may be exposed.

4 Suspicious Transaction Reports[11]

4.1 The AML/CFT Guideline provides guidance on the internal controls relating to filing STRs, including how to handle internal reports and post-STR reporting measures. This chapter provides further guidance on quality of STRs and how STRs can be prepared to better suit the needs of the JFIU leading to intelligence products, which can assist law enforcement agencies (LEAs) to disrupt ML/TF activities.

4.2 To enable the JFIU to extract useful information from STRs and make informed decisions quickly, it is important for AIs to ensure the quality and consistency of STRs. Every STR submitted to the JFIU should be accurate and complete with narratives which describe the scope and nature of the identified suspicion.

4.3 While AIs will have their own formats, STRs should have a structured format and contain all relevant information, based on the following principles:

(a) structure the content systematically (for easy comprehension by the JFIU);
(b) focus on the main subject and be concise;
(c) include digital footprints[12] related to online banking activities where relevant and available;
(d) ensure appropriate use of file attachments; and
(e) avoid providing non-editable transaction records to the JFIU.

4.4 While it is recognised that AIs may not be able to identify the exact nature of the underlying crime, they should report or select the categories of crime on a best-effort basis.

---

11 This document has been prepared by the HKMA, with input from the JFIU, to assist AIs in the submission of STRs. This document has incorporated feedback provided by the JFIU on "Quality of STR" (Feedback No. 191) set out in the STR Quality Analysis Issue 03/17 and an alert message on "Inclusion of digital footprints in Suspicious Transaction Reporting" published by the JFIU on 21 June 2021.

12 For example, Internet Protocol (IP) addresses, timestamps, geographical locations and device IDs

Structure the Content Systematically

4.5 STRs should contain sufficient information to assist the JFIU in understanding the background for analysis and investigation. While the information required for each STR will vary, it is important to ensure sufficient information is provided in all cases and inputted into the mandatory fields, e.g. account number and balance. The following topics should be covered, where available:

(i) Triggering factors

- Commission / types / association of offence (e.g. fraud, corruption, sanctioned, TF)
- Receipt of search warrant / court order and the reference number(s), where relevant
- Intelligence received from LEAs or other parties (e.g. FMLIT) with reference number(s), where available (e.g. FMLIT alert references)
- Material from publicly available information (e.g. adverse news, SFC alerts)
- Evidence of suspicious transaction patterns (e.g. substantial cash deposits, temporary repository of funds, suspected unlicensed money service operator)

(ii) Background of subject(s) and summary of the business relationship

For individuals:

- Full name
- Date of birth or age
- Nationality
- Identity document type and number
- Address and telephone number
- Occupation or employment
- Income or other relevant information relating to source of wealth and/or funds
- Any other relevant information that relates to net worth

For corporates:

- Full name and business nature
- Date and place of incorporation
- Registration or incorporation number
- Registered office address and business address
- Details of connected parties (e.g. beneficial owners, directors, shareholders)
- Summary of known financial situation of the entity

Summary of the business relationship:

- Bank account numbers (and other related accounts where applicable)
- Anticipated level and nature of the activity to be undertaken through the relationship (e.g. what the typical transactions are likely to be)
- Origin / destination of the funds[13]
- Purpose and intended nature of the account as provided by the customer
- Banking history

(iii) Transactions

- Specification of reviewing period
- Date and type of fund flow
- Previous transaction pattern (e.g. dormant)
- Total amount of deposit and withdrawal
- Counterparty information
- Goods purchased or merchant information (if available)
- Transaction remarks or payment references
- Suspicious indicators and patterns (not simply frequent / large-amount transactions)[14]

(iv) CDD and open source

- Result of CDD enquiry and internal investigation[15] in relation to the adverse news from open source or other suspicious activities
- Provision of hyperlinks of the relevant open source information

(v) Conclusion and way forward

- Summary of the narrative
- Follow-up action to be taken (e.g. further review, account closure[16])

4.6 Providing the basic background information of the subject and related bank accounts is only the first step. A summary should also be provided explaining the knowledge or suspicion and the grounds and analysis for it, i.e. which suspicious activity indicators or red flags are present.

---

13 This refers to the funds involved in the transaction or other activity giving rise to the relevant knowledge or suspicion.

14 When reporting suspicious activities on the basis that they deviate from normal customer/business practices, a simple description of "large transaction incommensurate with customer profile" is insufficient; the AI should elaborate on the suspicion supported by facts, transactions, findings, etc.

15 The background and process of the CDD enquiry and internal investigation generally need not be included unless the information is useful in demonstrating the suspicion.

16 It is important to make the JFIU aware of any intention to discontinue an account or relationship. Where such a course of action is contemplated, AIs should include this in the STR.

4.7 Suspicion should be supported by information on relevant conduct or activities. Reporting purely on certain high-risk businesses, without the requisite knowledge or suspicion and supporting details of any unusual activities, should be avoided.

Focus on the Main Subject and be Concise

4.8 STRs should be precise and concise with sufficient information to establish suspicion and facilitate follow-up enquiries. Too much or irrelevant information will divert focus from the main subject, making timely understanding and assessment of the STR difficult. Entities involved in different layers of alleged fraud and ML, where known, should be included to give a full picture of the fund flows. Where entities are only remotely associated with the subject matter of an STR, AIs should assess their relevance and consider whether they should instead be covered in separate STRs.

4.9 Where a network of relationships or accounts has been identified, AIs should report the network in the same STR, as far as is reasonably practicable. To help the JFIU and LEAs conduct analysis and investigation more efficiently, AIs should include sufficient information to illustrate the connections among accounts, such as common attributes [17] and transaction counterparties.

4.10 Where enquiries have been made with the customer to clarify or gather information, the results (i.e. brief details of those enquiries) can also be relevant. However, when making such enquiries with the customer, AIs should also be mindful about the risk of tipping off.

4.11 The source of funds of the transactions, the source of wealth of the subject persons and connected accounts or relationships are often key information supporting suspicion and should be included in the STR.

4.12 If the subject of an STR has been or is connected to the subject of a previous STR, this will be important information for the JFIU and AIs should, as far as is reasonably practicable be included by quoting the previous STR reference number(s). Background information on the subject and related bank accounts should still be provided even if this has been provided previously. Similarly, if an AI is aware that the subject of the STR has been the subject of a previous and/or on-going investigation by any LEA, it should quote the

[17] For example, IP addresses and device IDs

relevant case reference and the details of officer-in-charge (if available) in the STR.

Include Digital Footprints related to Online Banking Activities

4.13 With the growth of remote customer on-boarding and online banking, AIs are encouraged to record and include digital footprint information in editable format and other information, such as date, time, account activities, etc., associated with the identified digital footprints, where:

- the digital footprints are relevant (i.e. if the suspicious transactions are conducted via online banking or the internet, or otherwise relates to a cyber-enabled financial crime); and
- the relevant data or information is available in an AI's internal systems.

4.14 The retrieval and collation of digital footprints information should not delay the filing of STRs. Where additional time is required for this process (e.g. complex transactions involving various parties), AIs should consider providing digital footprint information later through a supplementary STR.

Appropriate Use of File Attachments

4.15 Narratives should be entered in the 'suspected crime' and/or 'suspicious indicators' columns in the STR proforma. This information is sometimes included as file attachments in the STRs, which makes prompt assessment by the JFIU more difficult. Attachments [18] should only be used to supplement the information provided in the narratives. For instance, where a network of suspicious relationships is reported, AIs could attach a diagram to help visualise the connections among the accounts.

Avoid Providing Non-Editable Transaction Records

4.16 AI should provide transaction records in editable format, where possible, to facilitate the JFIU's further processing and analysis. Transaction records generated from reporting AIs' internal systems should be comprehensible with adequate explanation of abbreviations used.

---

[18] Where attachments are used, they should be named in a way that reflects the nature of the document in order to assist the JFIU's investigation.