Annex

This Annex summarises the major chapter-by-chapter changes made to the *Guidance Paper on Transaction Monitoring, Screening and Suspicious Transaction Reporting* as compared to the version issued in 2018[1].

Chapter 2 – Transaction Monitoring

Paragraphs	Major changes
2.7 to 2.10	Guidance and examples provided regarding system design and optimisation including customer segmentation, parameters and thresholds calibration and testing. These changes take into account industry developments, including the use of technology or statistical tools and methods to optimise system capability.
2.11	Guidance to underline the importance of validation of the integrity, accuracy and quality of data in the development of effective transaction monitoring systems.
2.14	Clarification of expectations for the transaction monitoring system to support integration of information and data from external sources as necessary to enhance targeting and mitigation of ML/TF risks.
2.16 to 2.20, 2.22	Additional guidance to clarify processes supporting the review of alerts, including access to sufficient databases, solutions or tools; establishment of alert triaging, backlog handling and independent assurance programmes to address timeliness, quality and consistency of alert clearance.

Chapter 3 – Screening

Paragraphs	Major changes
3.6 to 3.8	Further guidance on system setting and tuning to underline the importance of striking the right balance between system effectiveness and efficiency.
3.9, 3.12, 3.13	In response to comments/suggestions in industry consultation, clarification of processes and principles supporting the handling and management of alerts, with an example of the processes for handling names that use non-Latin script.
3.14, 3.15	Guidance regarding ongoing review and senior management oversight of screening systems and processes, to support greater effectiveness and efficiency.

[1] https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180510e2a1.pdf

Chapter 4 – Suspicious Transaction Reporting

Paragraphs	Major changes
4.4	Codification of the reporting or selection, on a best effort basis, of categories of underlying crime in STRs to support better threat understanding and risk targeting.
4.5	Additional information JFIU has requested to be covered in STRs where available, including intelligence received from law enforcement agencies (LEAs) or other parties (e.g. FMLIT) with reference number(s); goods purchased or merchant information; and transaction remarks or payment references.
4.8, 4.9, 4.15	Based on the more advanced analytics capabilities deployed in some AIs, expectations regarding the reporting of networks of suspicious accounts and entities involved in different layers of alleged fraud and money laundering, where identified and known, including the provision of a network diagram, as an attachment to the STR, to help visualise the connections, to facilitate the JFIU and LEA analysis and investigation.
4.3, 4.13, 4.14	Guidance on reporting data points relating to cyber-enabled fraud where available.