ANNEX B

Factsheet on Revised Technical Reference 76

The revised TR 76 introduces additional guidelines on how e-retailers and e-marketplaces can secure different areas of e-commerce transactions i.e. during, pre- and post-purchase activities, in customer support and merchant verification.

	Key Recommendations
Pre-purchase	• E-retailers and e-marketplaces should put in place adequate and reasonable monitoring and screening policies and procedures to safeguard the authenticity of customers' reviews.
Purchase	• For transactions which the customer is unable to verify the condition of the goods and/or services prior to payment, e-retailers and e-marketplaces should have in place commonly accepted modes of electronic payment or post-purchase payment protection mechanisms that allow the customer to avoid losses in the event of a dispute or non-fulfilment of orders. Examples include: ○ Providing secured escrow payment option(s); ○ Providing guarantees for customers on products sold; and ○ Releasing payment to the merchant after the customer's confirmation of satisfactory receipt of the products and/or services or after the lapse of a stipulated period to lodge a dispute.
Post-purchase	• In the absence of measures to verify the authorised recipient, parties involved should reschedule/reconsider the transaction until verification is possible.
Customer support	• Where the e-marketplace permits transactions to take place outside of the platform, the e-marketplace should guide the customer on how he/she may seek recourse in the event of a dispute.
Merchant verification	• E-marketplaces should determine the information to be collected from the merchants and the verification steps to be

	taken based on their own risk assessments. Where feasible, e-marketplaces should verify their merchant's information against Government records or review such information against the identification document(s) provided. Where merchant verification is outsourced to a third-party service provider, the e-marketplace should put in place arrangements to facilitate, where possible, the timely retrieval of records. • E-marketplaces should use reasonable efforts to conduct due diligence on merchants, especially those selling in the course of business, to the extent practicable, appropriate, reasonably necessary and relevant, to verify their identity and reject registrations or listings where the e-marketplace has reason to believe that there are security or fraud risks. • E-marketplaces should retain merchant identifiers and transaction records where relevant and available for at least two years from the transaction. Transaction records include payment information of transactions completed on platforms, merchant's login/logout date and time, reference number of transactions completed on platform. • E-marketplaces should consider introducing pre-emptive safeguards against fraudulent merchants on their platforms, such as activating early warning mechanisms when a non-verified device is used to access the account. • For merchants deemed to be of fraud risk, e-marketplaces should consider blacklisting the merchant, restricting the merchant's activities on the platform or raising the customer's awareness of the risks involved. • E-marketplaces that are officially informed of the authorities' investigation of a suspected fraudulent account or merchant should, even when not legally obliged to, where appropriate, necessary and practicable, consider retaining its profile, transaction and payment information and/or make available to law enforcement the processes to request preservation of such information.