



## PRESS RELEASE

MR No.: 030/22  
Saturday, 14 May 2022

### **INTRODUCTION OF E-COMMERCE MARKETPLACE TRANSACTION SAFETY RATINGS AND REVISED TECHNICAL REFERENCE 76 ON E-COMMERCE TRANSACTIONS**

To secure e-commerce marketplaces from scams, the Inter-Ministry Committee on Scams (IMCS) will launch the following two initiatives today:

- (a) **E-commerce Marketplace Transaction Safety Ratings (“TSR”)** to provide consumers with information on anti-scam measures that major e-commerce marketplaces have in place; and
- (b) **Revised Technical Reference 76 on Guidelines for Electronic Commerce Transactions (“TR 76”)** to provide e-retailers and online intermediaries such as e-commerce marketplaces, with additional guidelines to better secure e-commerce transactions from scams.

#### **E-Commerce Marketplace TSR**

2. The TSR informs consumers on the transaction safety of different e-commerce marketplaces, based on the range of anti-scam measures they have in place. It covers major e-commerce marketplaces that facilitate online transactions from multiple sellers to multiple buyers, with a significant local reach or a significant number of e-commerce scams reported. The TSR microsite can be found at the following link: <https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>.

3. Major e-commerce marketplaces have been assigned an overall safety rating. The rating indicates the extent to which they have implemented anti-scam measures that ensure (a) user authenticity, (b) transaction safety and (c) availability of loss remediation channels for consumers, as well as (d) the effectiveness of their anti-scam measures. The ratings range from one to four ticks, with four ticks being the highest and best rating. E-commerce marketplaces with all the critical anti-scam measures in place will be awarded the full four-ticks. These ratings will be reviewed annually. Further details are in Annex A.

4. The TSR was developed in partnership with the following major e-commerce marketplaces, which have been rated as follows:

**Table 1: E-Commerce Marketplace TSR**

<b>Rating</b>	<b>E-Commerce Marketplace</b>
✓ ✓ ✓ ✓	Amazon, Lazada, Qoo10
✓ ✓ ✓ ✎	Shopee
✓ ✓ ✎ ✎	Carousell
✓ ✎ ✎ ✎	Facebook Marketplace

5. Consumers can also refer to the TSR microsite for advisories on safety features to look out for, and specific features provided by each e-commerce marketplace. The TSR microsite aims to raise consumer awareness on features that keep e-commerce transactions safe and encourage the use of safety features and good practices when transacting online.

### **Revised TR 76**

6. TR 76, the national standard for e-commerce transactions, has been revised to include additional anti-scam guidelines for e-retailers and e-commerce marketplaces, to offer better protection for consumers transacting online.<sup>1</sup> The revised TR76 is developed by a multi-stakeholder Working Group appointed by the Singapore Standards Council, overseen by Enterprise Singapore.<sup>2</sup>

7. The additional anti-scam guidelines will set out best practices for e-retailers and e-commerce marketplaces. These best practices secure different areas of transactions, covering pre-, during- and post-purchase activities, customer support and merchant verification. The intent is to better enable merchant authenticity, improve transaction security and aid enforcement against e-commerce scams. The additional guidelines in TR76 are part of the safety features rated in the TSR. Generally, e-commerce marketplaces that adopt TR76 guidelines would score better on the TSR. Further details are in Annex B.

### **Feedback from the E-commerce Industry**

8. E-commerce industry stakeholders have been instrumental to the development of the TSR and the revised TR 76. Feedback from the e-commerce industry on the TSR and the revised TR 76 has been very positive so far.

9. Mr Desmond Tan, Chairman of the Inter-Ministry Committee of Scams and Minister of State, Ministry of Home Affairs & Ministry of Sustainability and the Environment, said: “Adoption of anti-scam measures in the revised TR 76 guidelines by e-commerce retailers and e-commerce marketplaces will better secure e-commerce transactions and protect our consumers from e-commerce scams. The E-

---

<sup>1</sup> First published in 2020, TR 76 equips e-commerce businesses with industry best practices on key activities relating to online transactions.

<sup>2</sup> The Working Group consisted representatives from the following organisations who contributed in their individual capacity: Amazon Asia-Pacific Holdings Pte Ltd, Carousell Pte Ltd, Consumers Association of Singapore, Facebook Singapore Pte Ltd, JP Morgan Chase Bank, Lazada Singapore Pte Ltd, Lee & Lee, Mastercard Asia/Pacific Pte Ltd, Ministry of Home Affairs, Pick Network Pte Ltd, RSM Risk Advisory Pte Ltd, Shopee Singapore Pte Ltd, Singapore Institute of Retail Studies, Singapore Retailers Association, Smart Media4u Technology Pte Ltd and Temasek Polytechnic.

commerce Marketplace Transaction Safety Ratings build on these guidelines, by raising consumer awareness on the anti-scam measures on major e-commerce marketplaces in Singapore. MHA would like to thank our partners from the e-commerce industry for working with us on these initiatives to combat e-commerce scams.”

10. Ms Choy Sauw Kook, Director-General (Quality & Excellence), Enterprise Singapore, said: “We are encouraged by the strong support and commitment of the Working Group members, including MHA, Singapore Retailers Association, the Consumers Association of Singapore and e-commerce industry stakeholders, who have come together with Singapore Standards Council to develop new anti-scam guidelines under the revised TR 76. The guidelines cover the end-to-end process of e-commerce transactions, and we hope they will help e-retailers and e-marketplaces improve their transaction traceability and transaction security for consumers. We look forward to working with our partners to promote wider adoption of this standard in the industry.”

11. The TR 76 is available for viewing at the following link: <https://www.singaporestandardseshop.sg/Covid19/Desktop>. A PDF copy may also be purchased at the Singapore Standards eShop. New and existing e-retailers as well as e-marketplaces can refer to the guidelines in the TR 76 to secure themselves against scams.

**MINISTRY OF HOME AFFAIRS  
SINGAPORE STANDARDS COUNCIL**

**14 MAY 2022**

## **ANNEX A**

### **Factsheet on the E-Commerce Marketplace Transaction Safety Ratings**

1. The TSR will comprise an overall rating and general consumer advisory that will be refreshed annually, as well as marketplace-specific consumer advisories that will be updated every six months.
  - (a) **Overall rating**. E-commerce marketplaces will be assigned an overall rating, based on the extent to which they have in place the following critical anti-scam measures. E-commerce marketplaces with all the critical anti-scam measures in place will be awarded the full four-ticks.
    - i. **User Authenticity**. E-commerce marketplaces will be evaluated on whether they put in place measures to verify sellers' identity and continuously monitor for inauthentic seller behaviour.
    - ii. **Transaction Safety**. E-commerce marketplaces will be evaluated on the availability of secure payment solutions within the e-commerce marketplace for transactions, and whether they maintain transaction records and user data.
    - iii. **Loss Remediation Experience for Consumers**. E-commerce marketplaces will be evaluated on the availability of dispute reporting and resolution mechanisms.
    - iv. **Effectiveness of Anti-scam Efforts**. E-commerce marketplaces will be evaluated on the overall efficacy in safeguarding users from e-commerce scams, using the number of scam reports as a proxy.
  - (b) **Consumer advisory**. General advisories on how consumers may protect themselves when transacting online, as well as the features which keep e-commerce transactions safe, will be published on the TSR microsite.
  - (c) **Marketplace-specific advisories**. These advisories will be tailored to reflect the safety features that are deployed by individual e-commerce marketplaces.
2. An infographic summarising the TSR is shown below.

# E-commerce Marketplace Transaction Safety Ratings



The E-commerce Marketplace TSR show the extent to which platforms have anti-scam measures in place to combat e-commerce scams, taking into account the number of scam reports made on the platforms.



## Overall Platform Rating

Platform	Rating
Amazon, Lazada, Qoo10	✓ ✓ ✓ *
Shopee	✓ ✓ ✓
Carousell	✓ ✓
Facebook Marketplace	✓

\* Platforms with all the critical anti-scam measures in place will be awarded four ticks.

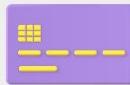
### Overview of Criteria Considered in Platform Rating

- ✓ Improving seller authenticity
- ✓ Improving transaction safety
- ✓ Enhancing loss remediation experience for consumers
- ✓ Effectiveness of anti-scam efforts

## What Should You Do When Transacting Online?



Transact with sellers whose identities are verified by the marketplaces.



Utilise in-platform secure payment solutions, where available.



Check the reviews of the seller before making direct payment.



Report all unfulfilled transactions, disputes, suspicious listings and errant sellers promptly, via the marketplaces.



Protect yourself by keeping transactions within the platform.



**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
<b>Pre-purchase</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Purchase</b>	<ul style="list-style-type: none"> <li>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: <ul style="list-style-type: none"> <li>Providing secured escrow payment option(s);</li> <li>Providing guarantees for customers on products sold; and</li> <li>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.</li> </ul> </li> </ul>
<b>Post-purchase</b>	<ul style="list-style-type: none"> <li>In the absence of measures to verify the authorised recipient, parties involved should reschedule/reconsider the transaction until verification is possible.</li> </ul>
<b>Customer support</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Merchant verification</b>	<ul style="list-style-type: none"> <li>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.</li> </ul>

	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>
--	---