Technical Reference TR 76:2020

Guidelines for electronic commerce transactions

AMENDMENT NO. 1

March 2022

1. Page 6, Foreword

Replace “sellers” in paragraph 3 item (a) with “merchants”.

2. Page 8, Clause 0 Introduction

a) *Replace* “internet access” in paragraph 1 with “digital adoption”.

b) *Add* “This is also a concerted effort to enhance professionalism among the e-marketplaces/merchants/e-retailers.” at the end of paragraph 1.

c) *Replace* “By implementing this Technical Reference, organisations will:” in the last paragraph with “By implementing this Technical Reference, e-marketplaces, e-retailers and merchants will:”.

3. Page 9, 2.4 Merchant

Replace “retailer” with “person”.

4. Page 11, 3.2.4 Information related to the transaction

Replace “Disclose policies and procedures safeguarding customer reviews.” with “Put in place adequate and reasonable monitoring and screening policies and procedures to safeguard the authenticity of customers’ reviews, where reviews are available.”

5. Page 15, 4.3.2 Modes of payment

Replace the clause with the following text:

E-retailers and e-marketplaces should consider the following when choosing a payment solution:

- The need to provide the customer with a range of commonly accepted modes of electronic payment;
- Availability of a payment method/ brand including in-platform payment modes where payments are protected;
- Processing fees;
- Settlement time;
- Ease of use for the customer (customer can select a payment option in an efficient and convenient manner such that there will be minimal website re-directs);

- Ease of communication between the organisation and the payment provider; and

- Transaction safety of users in the payment journey including the level of fraud protection.

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 provide commonly accepted modes of electronic payment, or have in place 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

- Implementing escrow or equivalent mechanisms where the payment is released 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.

6. Page 17, 4.3.5 Order confirmation

Replace the last paragraph with the following text:

Where applicable, e-retailers and e-marketplaces should provide a way to contact the e-retailer or merchant in the event that the customer requests changes (e.g. amend content of the order, change delivery address).

7. Page 20, 5.3.6 Proof of delivery

Replace the clause with the following text:

Whenever applicable and depending on the constraints of each platform, e-retailers and e-marketplaces should make suitable arrangements with logistics service providers to confirm that an order has been delivered or that a certain delivery method has been approved. This form of acknowledgement could be in various forms, depending on the delivery method.

For self-collection relating to transactions occurring on platform, acknowledgement proving the collection of goods is generally not required if the authorised recipient presents a valid unique identification code or relevant transaction information at the collection point. However, in the absence of measures to verify the authorised recipient, parties involved should reschedule/ reconsider the transaction until verification is possible.

8. Page 22, 6.4 Complaints handling

a) *Replace* the text in paragraph 3 with the following:

E-retailers and e-marketplaces should consider the following processes when handling complaints related to transactions that they facilitate:

b) *Replace* item (a) with the following:

(a) Ensure that the complaints handling process is adequately communicated to the customer, including information on where to file the complaint, how to file the complaint, the reasonable timeline for handling complaints, possible remedies and how to enquire on the status of the complaint.

c) *Replace* item (e) with the following:

(e) Track the complaint and monitor if all proposed actions are implemented effectively in a timely manner.

9. Page 22, 6.5 Dispute resolution

Replace the clause with the following text:

E-retailers and e-marketplaces should refer to 6.4 on complaints handling and establish clear dispute resolution policies and processes to facilitate dispute resolution related to e-commerce transactions completed on their platforms, but such policies and processes should not oust the jurisdiction of applicable courts and tribunals.

E-retailers and e-marketplaces may develop their dispute resolution mechanism in-house or outsource the process to a competent third-party service provider. E-retailers and e-marketplaces may refer to ISO 10003, “Quality management – Customer satisfaction – Guidelines for dispute resolution external to organizations”, and/or the Consumers Association of Singapore’s “Standard Dispute Management Framework for E-Marketplaces”, for guidance on dispute resolution.

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.

10. Page 23, Clause 7.2.1 Identifying merchants

Replace the clause with the following text:

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, based on risk assessment of merchants, implement reasonable measures to collect as many of the following identifiers of a merchant as reasonably practicable, relevant and available:

- Merchant’s legal name
- Merchant’s official identifying information (e.g. company registration number or NRIC);
- Contact details of the merchant for directing feedback, asking questions, filing a claim (e.g. registered postal address, email address, phone number);
- Details of merchant’s bank account or credit card information if payment is made in-platform; and

- Where the merchant is selling a service that is regulated as a profession in Singapore (e.g. electrical or plumbing services):
    - details of the professional title granted;
    - jurisdiction where the title has been granted;
    - professional body or similar institution with which the organisation is registered;
    - reference to the professional rules applicable to the organisation;
    - means to access the service; and
    - professional liability insurance or guarantee that the organisation is required to hold.

11. Page 23, 7.2.2 Monitoring systems

Replace the last paragraph with the following:

To facilitate investigation, remediation, and tracing of suspicious transactions when required, e-marketplaces should, as part of their operations, keep records of the identifiers of the merchant (see 7.2.1). They should also keep records of the following transactional data, where relevant and available, having regard to the purpose for which personal data was collected and for other legal or business purposes:

- Payment information of transaction completed on platform (e.g. bank account number, credit card or bank processing information).
- Merchant's login/ logout date and time.
- Reference number of transactions completed on platform (e.g. merchant's order identification number).

The records of the identifiers and transactional data should be kept for at least 2 years from the transaction, subject to legal restrictions in different jurisdictions, to support investigations by law enforcement agencies.

E-marketplaces should consider the following pre-emptive safeguards against fraudulent merchants on their platforms, subject to technical constraints and legal restrictions in different jurisdictions. Examples may include:

- Binding a unique identification (e.g. mobile device IMEI or device fingerprinting) to each merchant such that the same identification cannot be used for another account;
- Activating early warning mechanisms when a non-verified device is used to access the account; and
- Procuring an external fraud management service.

E-marketplaces should, if the merchant is deemed to be of fraud risk, consider blacklisting the merchant, restricting the merchant's activities on the platform or raising the customer's awareness of the risks involved. Examples may include:

- Using adequate means to disallow the high-risk merchant to operate under a different account or set up a new account;

- Denying data deletion by the high-risk merchant;

- Reporting identified fraudulent merchants to the authorities for investigation; and

- Informing the customer of the potential risks when engaging in higher risk transactions, so that the customer can make a more informed choice.

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 the account's or merchant's profile, transaction and payment information and/or make available to law enforcement the processes to request preservation as these records may be crucial for law enforcement agency's investigations.

12. Page 25, Bibliography

Insert the following for the Standards/Publications list:

15) Standard dispute management framework for e-marketplaces, Consumers Association of Singapore

Replace the following for the Regulations/ Acts list:

Regulations/Acts

16) Consumer Protection (Fair Trading) Act

17) Personal Data Protection Act

18) Small Claims Tribunals Act

NOTE – The list of regulations and acts is not exhaustive. Users of the standard will need to check with the relevant regulatory bodies on the latest regulatory and statutory requirements.