

Postal E-commerce and Trade Facilitation Guidelines

Acronyms and Abbreviations

AML	Anti-Money Laundering
B2C	Business-to-Consumer
CDD	Customer Due Diligence
CIRT	Cyber Incident Response Team
CRASA	Communications Regulators' Association of Southern Africa
CRM	Customer Relationship Management
EDI	Electronic Data Interchange
EMV	Europay, Mastercard and Visa
EU	European Union
GDPR	General Data Protection Regulation
HIPSSA	Harmonization of ICT Policies in Sub-Sahara Africa
ICT	Information and Communications Technology
KYC	Known Your Customer
MSME	Micro, Small and Medium-sized Enterprises
OECD	Organisation for Economic Co-operation and Development
PCIDSS	Payment Card Industry Data Security Standards
PKI	Public Key Infrastructure
QoS	Quality of Service
SADC	Southern African Development Community
UPU	Universal Postal Union

Contents

1. Introduction 3
   1.1 Background 3
   1.2 Objectives of the Guidelines 3
   1.3 Applicability 4
2. Context 4
   2.1 International Context 4
   2.1 SADC Protocol on Transport Communications and Meteorology 5
3. Understanding the E-commerce Transaction 5
   3.1 E-commerce Definition 5
   3.2 Guiding Principles 6
      3.2.1 Holistic Approach 6
      3.2.2 E-commerce Value-Chain Elements 6
      3.2.3 The Three (03) Flows Concept 7
4. Recommended Approaches to Postal E-commerce and Trade Facilitation Regulation 7
   4.1 Facilitating, Securing and Expediting the Flow of Online Data and Information 7
      4.1.2 Data Protection and Privacy 10
      4.1.3 Advertising and Misleading Information 13
      4.1.4 Cybersecurity 15
      4.1.5 Validity of Electronic Transactions 16
   4.2 Facilitating, Securing and Expediting the Financial Aspects of the 16
   E-commerce Transaction 16
      4.2.1 Online/electronic Payments and Security 16
      4.2.2 Taxation 22
   4.3 Facilitating, Securing and Expediting the Physical Delivery of Goods 23
      4.3.1 Choice of Delivery Channels and Service Providers 23
      4.3.2 Delivery Terms and Conditions 23
      4.3.3 Liability and Compensation 24
      4.3.4 Quality of Service - Late or non-delivery of products or delivery of defective products 26
      4.3.5 Returns 27
   4.4 General Legal and Regulatory Issues 28
      4.4.1 Identity Management 28
      4.4.2 Jurisdiction and Choice of Law 28
      4.4.3 Formation and Validity of Contracts 29
   4.5 Trade Facilitation 29
5. References 30

1. INTRODUCTION

1.1 Background

The SADC E-commerce Strategy is intended to transcend national borders and enable businesses and consumers to get the most out of their national markets through improving access to an increasingly large range of products and services. The Strategy is based on four key pillars as follows;

A. an enabled E-commerce environment,
B. E-commerce capacity development in each member state,
C. strengthening E-commerce sub-regional and national infrastructure, and
D. an institutionalised framework to maintain, evolve and govern the strategy.

In contribution to this regional approach and also in line with the Communications Regulators' Association of Southern Africa's (CRASA) mandate, of harmonising policy and regulations in the ICT and Postal spheres within SADC, the Association has developed these Regional Regulatory Guidelines that specifically aim to enhance the role of the Postal Sector in facilitating Regional Trade, especially involving Micro Small and Medium Enterprises (MSMEs) and E-commerce. The development of these guidelines is premised on the understanding that in order for E-commerce and intra-regional trade to flourish in the SADC Region, there is need for a regulatory environment that not only facilitates the participation of the Postal Sector and other value-chain stakeholders, but also creates confidence and promotes increased uptake by consumers.

1.2 Objectives of the Guidelines

The guidelines are offered as a reference source to guide CRASA Members in providing appropriate and proportionate regulatory oversight to stimulate intra-regional E-commerce and trade through the regional postal and courier services network. In so doing the specific objectives of the Guidelines include:

a) To promote a common Regional understanding of the regulatory considerations that are relevant to the Postal E-commerce and cross-border trade facilitation environment;
b) To identify the key regulatory processes and stakeholders that have a direct or indirect impact on the ability of the Postal sector to participate in intra-regional trade and E-commerce,
c) To provide guidance to CRASA Members on harmonised regional approaches to dealing with the specific regulatory issues in the E-commerce and trade facilitation environment including;
    i. Disclosure of information provided by e-merchants,
    ii. Unfair commercial practices,

iii. Unfair contract terms,

iv. Online payment security,

v. Data protection and privacy,

vi. Dispute resolution and redress and

vii. Cross-border online transactions and the associated exchange of data

d) To enhance Market Development and Access to E-commerce.

1.3 Applicability

These Guidelines are intended to apply primarily to the following identified stakeholders:

a) Policymakers;

b) Postal, ICT, Trade and Financial Sector Regulators;

c) Postal and Courier Service Providers;

d) Wider Postal Sector stakeholders;

e) Consumers; and

f) Customs and State Security Authorities; including Police, Anti-Money Laundering and Drug Enforcement agencies.

2. CONTEXT

2.1 International Context

E-commerce covers a wide range of transactions effected via mobile telephones and other devices such as personal computers and tablets, and purchases are often made by using applications and platforms. Purchases over the Internet usually involve businesses and consumers from different jurisdictions, which may have different regulations with respect to the key features of E-commerce. In the international context, a considerable body of work has been carried out by the Organisation for Economic Co-operation and Development (OECD) particularly in the provision of guidance to its Member Countries in the area of E-commerce Consumer Protection. Such guidance has for instance called upon Governments to establish National Policies for Consumer Protection that encourage good practices applicable also to e-commerce in areas including information disclosure, contract terms, secure payment mechanisms, consumer privacy and data security and dispute resolution and redress.

The guidance provided by the OECD, which has been drawn upon as a key reference for the development of this document, has also extended to listing the important aspects of consumer

protection that should be covered by education programmes, and includes E-commerce.

2.1 SADC Protocol on Transport Communications and Meteorology

From the perspective of the SADC Protocol on Transport Communications and Meteorology, the provision of an environment which is supportive of intra-regional e-commerce and trade can be seen in several articles including the following:

Article 3.4 – logistical Systems
Calls upon Member States to:

1) develop simplified and harmonised documentation which supports the movement of goods along the logistical chain,
2) harmonise domestic legislation including provisions dealing with statutory liability of service providers.

Article 10.1 – Telecommunications
Calls upon Member States to develop networks that ensure the provision of adequate, high quality and efficient services that are responsive to the needs of commerce.

Article 11.1 – Postal Services
Provide efficient, market-related and universally accessible Postal Services that support the economic needs of the Region and encourage cooperation between the relevant authorities to improve the reliability, speed and security of postal exchanges within the SADC Region and beyond.

3. UNDERSTANDING THE E-COMMERCE TRANSACTION

The purpose of this section is to ensure that all parties involved in the regulatory process associated with E-commerce have a common understanding of the subject in terms of the following:

3.1 E-commerce Definition

E-commerce involves all commercial activities carried out on electronic networks, including promotion, online sale of products and services, customer care, etc and is not limited to the Internet. Any commercial transaction completed totally or partially by electronic means is considered electronic commerce.[1]

- ✓ Includes inter-company relations as well as relations between companies and administrations and exchanges between companies and consumers.
- ✓ Includes not only purchases and sales carried out through a website but also purchases via an interactive telephone system (Audiotel type) and between companies, through direct and automated computer-to-computer relations such as Electronic Data Interchange (EDI).
- ✓ Does not require that payment be made online. The use of online payment systems may be necessary for Business to Consumer (B2C) and sales to end users. However, some companies expanding existing direct sales business using e- commerce continue to use more conventional methods of payment on delivery such as check or cash on delivery.
- ✓ There are four stages involved in e-commerce transactions: (1) searching; (2) negotiating/ ordering; (3) payment; and (4) delivery. Using E-commerce does not mean completing all the stages online. If one of these stages is carried out online, the transaction can be considered to be E-commerce.
- ✓ Additional reference to digitalisation is also relevant in the E-commerce definition including the

[1] Definition adapted from SADC Ecommerce Strategy 2012.

sharing of business and customer information, maintaining business relationships, and conducting business transactions by digital means over telecommunications networks. [2]

3.2 Guiding Principles

3.2.1 Holistic Approach

It should be emphasised from the outset that while the Postal Sector is seen as potentially active participant in the E-commerce and trade facilitation value-chain in SADC, thecreation of an enabling regulatory environment for E-commerce and trade cannot isolate this specific sub-sector. The measures recommended in these guidelines take a holistic view of the E-commerce and trade facilitation value-chain and in so doing, promote a regulatory environment that supports the involvement of value-chain players of all types; including postal and courier service providers.

3.2.2 E-commerce Value-Chain Elements

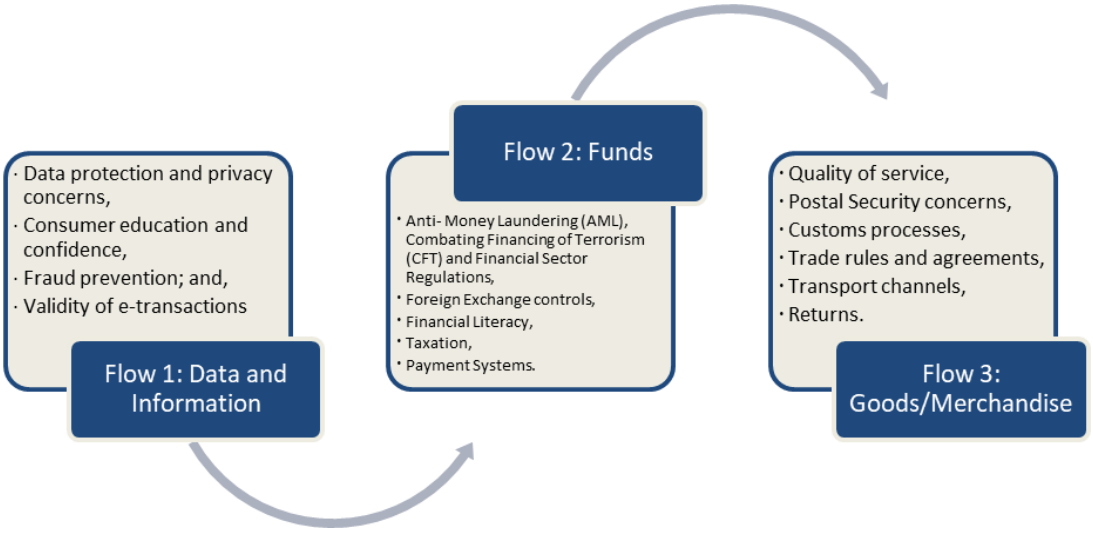
Regulatory intervention in the Postal E-commerce and Trade facilitation environment must be guided by the understanding that Postal and Courier service providers are potentially active participants in the provision of several value-chain elements, some of which may be within the ambit of multiple regulatory authorities and also open to competition from other value-chain players as follows:

a) Provision of Web-hosting services and online shopping platforms,
b) Provision of Payment channels,
c) Provision of Logistics, Delivery and fulfilment Services
d) Provision of Customer Relation Management (CRM),
e) Provision of Promotional Channels and Marketing,
f) Data exchange and data protection.

3.2.3 The Three (03) Flows Concept For

The concept essentially proposes that E-commerce and cross-border trade transactions consist of three key flows, for which regulatory intervention may be required in order to facilitate, expedite and secure them as follows;

[2] International Journal of Electronic Communications, Volume 26, Issue 3, 2022.



4. RECOMMENDED APPROACHES TO POSTAL E-COMMERCE AND TRADE FACILITATION REGULATION

4.1 Facilitating, Securing and Expediting the Flow of Online Data and Information

4.1.1 Electronic Identification and Authentication Tools

SADC Member States are called upon to create a conducive environment for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, digital signatures and electronic delivery services both domestically and across the SADC as well.

The main objective of such an approach shall be the removal or mitigation of existing barriers to the cross-border use of electronic identification and authentication in E-commerce transactions. The aim is not to intervene with regard to any electronic identity management systems and related infrastructures already being established in SADC Member States, but to rather ensure that for access to cross-border online services, secure electronic identification and authentication is possible**.** In the case of digital signatures for instance, they enhance the security of online transactions and help build the trust of buyers. They do this by validating the authenticity of a buyer and providing evidence to validate any transaction, digital message, or document. This is particularly relevant and advantageous in the E-commerce environment where the transactions happen between anonymous identities. [3]

In order for this to happen, SADC Members shall apply the following guidance:

[3] This process takes place in three stages:

- The first stage is called the Key Generation Algorithm, where a private key is generated using an advanced mathematical algorithm.
- In the next stage, after generating a private key, the document that is to be signed is also generated.
- This stage includes the Signing Algorithm. Although, the document cannot be signed until the signer's private key is verified.
- The verification happens in the third and the final stage, which utilizes Verification Algorithm. In this stage, the system verifies the authenticity of the private key and the message.
- In this process, the system generally generates two keys – a private and a public key.
- This means that for every private key, a public key is created.
- Now, the process of authentication is done to determine whether the private and public keys match or not. Once both the keys match, the signer can sign the document.

A. Members shall support the ongoing work of the SADC Expert Group on PKI and CIRT to ensure that all Member States have a National CIRT and PKI in place by December 2019. This work includes championing National PKI establishment, management, collaboration and to develop roadmaps with tangible activities leading to the establishment of a SADC Regional PKI.

B. Member States shall be at liberty to use or to introduce systems for electronic identification for accessing online services and to decide whether or not to involve the private sector in the provision of those systems. The principle of mutual recognition of such systems among SADC Member states shall however apply;

C. Furthermore, the principle of mutual recognition above (B) shall only relate to authentication for an online service. The access to those online services and their final delivery shall be subject to the right to receive such services under the conditions set out in national legislation,

D. Member States shall encourage the private sector to voluntarily use the electronic identification systems for identification purposes when needed for online services or electronic transactions,

E. Since the security of electronic identification systems is key to trustworthy cross- border mutual recognition, Member States shall cooperate with regard to the security and interoperability of the electronic identification systems at Regional level,

F. Such cooperation by Member States should facilitate the technical interoperability of the electronic identification systems with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices among Member States shall therefore be pursued in this regard,

G. In order to contribute to their general cross-border use, it should be possible to use the electronic identification systems as evidence in legal proceedings in all Member States,

H. Notification of security breaches and security risk assessments among Member States is essential. Members shall therefore endeavour to provide adequate information to concerned parties in the event of a breach of security or loss of integrity,

I. Members shall uphold the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form. Members shall in the same vein ensure that the national law unambiguously defines the legal effect of electronic signatures,

J. Members shall also consider the following additional principles in relation to the use of electronic signatures:

a) Where a law requires a document to be signed, an electronic form of the document shall satisfy the requirement if an electronic signature is used. An electronic signature shall be authentic if;

i. the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and not any other person;

ii. the means of creating the electronic signature was at the time of signing, under the control of the signatory and not any other person and was done without duress and undue influence;

iii. any alteration made to the electronic signature after signing is detectable.

b) A person who relies on a digital signature shall bear the legal consequences of failure to;
   a. take reasonable steps to verify the authenticity of the digital signature; or
   b. take reasonable steps where a digital signature is supported by a certificate, to;
      i. verify the validity of the certificate; or
      ii. observe any limitation with respect to the certificate

c) Unless otherwise prescribed by law, a person may decide the use of a digital signature, digital signature certificate or any other mode of authentication, of his choice,

d) Where a law requires a signature, statement or document to be notarized, acknowledged, verified or made under oath, that requirement shall be satisfied if the electronic signature of the person authorised to perform those acts is affixed to an electronic record,

e) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or in another physical form, that requirement shall be satisfied if an electronic copy of the document is certified to be a true copy by using an electronic signature of the certifying person.

4.1.2 Data Protection and Privacy

While SADC Member States are already equipped with and strongly encouraged to use the comprehensive SADC Model Law on Data Protection (2011 Harmonization of ICT Policies in Sub-Sahara Africa [HIPSSA] Project), Members may also apply the following general principles to complement the Legislative approach especially in the context of E-commerce:

A. Promoting Ownership of Personal Data

In simple terms, SADC Members must take the necessary legislative and regulatory measures to empower consumers to be the all-encompassing owners of their personal data. Specifically, consumers should be given the right to review, adjust, erase, and restrict the use and processing of their data. These requests must be facilitated online by E-commerce and other online service providers and provided to the individual within a reasonable time.

B. Promoting 'opt in' as opposed to 'opt out' consent

Whereas the current practice is skewed towards web visitors opting-out of data collection, SADC

Members are encouraged to promote a requirement for consumers to manually opt-in. This means that websites should no longer be able to pre-populate consent forms. This is meant to ensure that consumers become more conscious of what they are agreeing to. Within this consent, service providers should be required to clearly and simply communicate which parties are collecting the data (i.e., third parties), for what purpose, safeguards in place, and the length of time that the data shall be stored.

C. Ensuring Data Storage Requirements are met

To better protect consumers from having their data mishandled, various measures may be put in place as follows;

i. **Sensitive Data:** Data such as race, health, sexual orientation, religion, and political beliefs must be protected with additional safeguards,

ii. **Data Protection Officer:** All organisations that collect data on a large scale or deal with sensitive data, shall be compelled to appoint a data protection officer that has knowledge of the applicable data protection legislation in the Member State and SADC Region,

iii. **Data Breaches:** Regulated entities shall be required to inform affected customers within a specified timeframe of a serious data breach. [4]

iv. **Record Maintenance**: Regulated entities shall be obliged to keep records of all processing activity.

D. Punishing Non-compliance

Member States shall ensure that there are significant penalties for non-compliance with Data Protection Legislation and associated regulatory measures.

E. General Regulatory Terminology, Procedures and Processes

In addition to the above, Member States may also consider adopting the following general regulatory terminologies, procedures and processes in terms of Data Protection:

Data Controller	A person who, acting either alone or in common with other persons, determines the purpose for which, and the manner in which, any personal data is processed, or is to be

[4] As a matter of principle, it is recommended that all SADC Member states put in place a data protection regulatory framework that compels the Data Controller to report data breaches to the relevant supervisory authority within a specified timeframe (e.g. 72 hours). If it is not possible to make a full report within the said timeframe, the supervisory authority should be notified and full details should follow without undue delay, together with a justifiable reason for the late reporting.
While the reporting requirement should apply in all cases, individual jurisdictions may exclude the reporting of breaches that are not likely to present any risk to the rights or freedoms of the concerned data subject/(s).
If, however, there is a high risk to the rights and freedoms of data subjects, the individuals concerned must also be notified of the breach, without undue delay. There are generally three exceptions that may be exercised at the discretion of the supervisory authority in this regard:

i. when the data which has been breached has been made unintelligible by the use of methods such as encryption,
ii. when the data controller has acted to alleviate the high risk,
iii. and where sending individual communications would involve disproportionate effort and a different form of communication is more appropriate (Such communication could include a message on the website of the business or organisation, or a press release)

	processed and thus, controls and is responsible for the keeping and using of personal data, and the term includes a person who collects, processes or stores personal data. A data controller shall ensure that personal data is; a) processed fairly and legally; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are collected and processed; d) accurate and, where necessary, kept up to date; e) every reasonable step shall be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is erased or rectified; and f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.
Personal Data	Personal data; may be processed only if: a) the data subject has unambiguously given his consent; b) the processing is necessary for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) the processing is necessary for compliance with a legal obligation to which a data controller is subject; d) the processing is necessary in order to protect the vital interests of a data subject; e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a data controller or in a third party to whom the data is disclosed; or f) the processing is necessary for the purposes of the legitimate interests pursued by a data controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.
Consent	For purposes of this section, ***"consent"*** means any freely given specific and informed indication by a data subject, of his wishes, by agreement, to his personal data being collected, processed or stored.
Data Subject	A data subject; shall be entitled to obtain from a data controller, without constraint or unreasonable delay and at no expense: a) confirmation as to whether or not the data relating to the data subject is being processed and the purpose for such processing; b) communication to the data subject of the data undergoing processing and of their source;

c) communication for the purposes of the processing and the recipients to whom the data is disclosed;

d) to object at any time on legitimate grounds relating to his situation to the processing of data relating to him and where there is a justifiable objection, the processing instigated by the data controller may no longer involve;

e) to obtain from a data controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of these Guidelines, in particular because of the incomplete or inaccurate nature of the data.

F. Reference to the European Union (EU) General Data Protection Regulation (GDPR)

SADC Member States are also encouraged to take note of global trends in the Data Protection environment including the EU's GDPR. The overarching purpose of the GDPR is to ensure that the following questions are answered in the affirmative:

a. Are consumers comfortable in sharing their personal information with Platforms?
b. Is the information, so shared, safe?
c. Is the information only used for the given purpose?
d. Are remedies available to consumers against any data breach?

In this regard, the main elements of the GDPR are:

a. Enriched rights to the data subject (natural persons);
b. Strict obligations on the persons processing the personal data (data controllers & data processors);
c. Lawfulness of the purpose of personal data processing;
d. Stringent monitoring and enforcement through independent authorities; and
e. Administrative penalties.

G. Cross-Border Applicability of GDPR–Territorial Scope:

Due to its territorial scope, the GDPR, is applicable even outside the EU. In this context, even e-Commerce Platforms outside EU need to comply with the GDPR. The GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
b. the monitoring of their behaviour as far as their behaviour takes place within the EU.

4.1.3 Advertising and Misleading Information

While some SADC may currently have different enforcement systems to combat misleading

advertising in the E-commerce environment, ranging from civil law systems to public systems (including criminal sanctions) or a mixture of both, these guidelines recommend that deliberate actions be initiated to harmonise the said enforcement systems under the SADC umbrella. Such harmonisation will enable regional cooperation in the implementation of enforcement actions and create a legal basis for consumer protection coordination among the relevant national authorities at SADC level.

In this regard, SADC Member States may put in place policy and regulatory interventions that seek to ensure online advertisers are obliged:

I. To treat consumers fairly;
II. Not mislead through acts / omissions;
III. Stop aggressive commercial practices;
IV. Stop misleading advertising;
V. Create a framework for comparative advertising.

In addition to the above, Member states may adopt the following general principles and practices for inclusion in the appropriate regulatory instruments:

A. A person dealing with online communication shall not advertise in a misleading manner,
B. In determining whether online advertising is misleading, account shall be taken of all its features, and in particular, of any information it contains concerning;
    a) the characteristics of goods or services, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, geographical or commercial origin, the results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services;
    b) the price or the manner in which the price is calculated, and the conditions on which the goods are supplied, or the services provided; and
    c) the nature, attributes and rights of the advertiser, such as its identity, assets, qualifications, ownership of industrial, commercial or intellectual property rights or its awards and distinctions.
C. Comparative advertising shall, as far as the comparison is concerned, be permitted if the advertising;
    a) is not misleading;
    b) compares goods or services meeting the same needs or intended for the same purpose;
    c) objectively compares one or more material, relevant, verifiable and representative features of those goods and services, which may include price;

d) does not discredit or denigrate the trademarks, trade names, other distinguishing marks, goods, services, activities or circumstances of a competitor;

e) for products with designation of origin, relates in each case to products with the same designation;

f) does not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;

g) does not present goods or services as imitations or replicas of goods or services bearing a protected trademark or trade name; and

h) does not create confusion among traders, between the advertiser and a competitor or between the advertiser's trademarks, trade names, other distinguishing marks, goods or services and those of a competitor.

4.1.4 Cybersecurity

The ease of use and convenience of E-commerce also introduces significant security risks. This is primarily because sensitive information and personal data is routinely shared between merchants, payment providers and shoppers. In order to mitigate these risks, SADC Member States may introduce policy and regulatory interventions whose high-level objectives shall include ensuring:

A. **Integrity** – The ability to ensure that information being displayed on a web site or transmitted or received over the internet has not been altered in any way by an unauthorized party;

B. **Nonrepudiation** – The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions;

C. **Authenticity** – The ability to identify the identity of a person or entity with whom you are dealing on the internet;

D. **Confidentiality** – The ability to ensure that messages and data are available only to those who are authorised to view them;

E. **Privacy** – The ability to control the use of information about oneself;

F. **Availability** – The ability to ensure that an e-commerce site continues to function as intended;

The measures introduced shall also consider the need to combat the following specific security threats in line with the SADC Cybersecurity Action Plan 2018 (as may be amended from time to time):

Malicious Code		
1	Viruses:	Have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses
2	Worms:	Designed to spread from computer to computer
3	Trojan horse:	Appears to be benign, but then does something other than expected

4	Bots:	Can be covertly installed on computer; responds to external commands sent by the attacker
Unwanted Programs: Installed without the user's informed consent		
1	Browser parasites:	Can monitor and change settings of a user's browser
2	Adware:	Calls for unwanted pop-up ads
3	Spyware:	Can be used to obtain information, such as a user's keystrokes, e-mail, IMs, etc.
Phishing and Identity Theft		
1	Any deceptive, online attempt by a third party to obtain confidential information for financial gain	Most popular type: e-mail scam letter
Hacking and Cybervandalism		
1	Hacker:	Individual who intends to gain unauthorized access to computer systems
2	Cracker:	Hacker with criminal intent (two terms often used interchangeably)
3	Cybervandalism:	Intentionally disrupting, defacing or destroying a Web site
Credit Card Fraud		
1	Theft of Card Information	Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
Spoofing (Pharming) and Spam (Junk) Web Sites		
1	Spoofing (Pharming)	- Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else - Threatens integrity of site; authenticity
2	Spam (Junk) Web sites	Use domain names similar to legitimate one, redirect traffic to spammer redirection domains
DoS and DDoS Attacks		
1	Denial of service (DoS) attack	Hackers flood Web site with useless traffic to inundate and overwhelm network
2	Distributed denial of service (DDoS) attack	Hackers use numerous computers to attack target network from numerous launch points
Other Security Threats		
1	Sniffing:	Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
2	Insider jobs:	Single largest financial threat
3	Poorly designed server and client software:	Increase in complexity of software programs has contributed to increase is vulnerabilities that hackers can exploit
4	Cookies	Cookies are pieces of data sent by websites that remain stored on a user's computer to help with user-identification and future web browsing. E-commerce websites are particularly pre-disposed to the use of cookies. Cookies inherently pose several security and privacy risks that must be mitigated through appropriate legislation and effective enforcement thereof.

4.1.5 Validity of Electronic Transactions

In order to achieve the objectives of this section, Member states shall refer to the SADC Model Law on Electronic Transactions 2013 which was an output of the Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA) Project.

4.2 Facilitating, Securing and Expediting the Financial Aspects of the E-commerce Transaction

4.2.1 Online/electronic Payments and Security

Online merchants and consumers alike expect online buying and selling to be easy, efficient, and safe. E-commerce transactions trigger complex automated processes that involve downstream players: banks and payment processors to name just two. In addition, there have been unprecedented technological advances in smartphones and e-wallets, shifting purchase patterns, and demand for cross-border, multi-currency electronic payments all associated with the growth of E-commerce.

A. Challenges

Fraud:

Online transactions are "card-not-present" transactions. As E-commerce expands, opportunities for fraudulent misuse of payment networks and data theft grow right alongside. in addition to being costly, this can damage business reputations and reduce consumer confidence in online payment systems.

In order to mitigate this, SADC Member States shall, through the proportionate use of appropriate regulatory interventions, promote the following:

a) Use of customer service practices that are based on know-your-customer (KYC) principles and merchant accessibility,
b) Use of new technologies such as EMV and fingerprint recognition,
c) Use of advanced EMV technology to validate the genuineness of payment cards is and facilitate the authorization of transactions.[5]

Card data security:

In the E-commerce and associated online payment environment, customer and card data security should be given the highest priority. Preventing online payment security issues is therefore a must for anyone doing business online. In order to underscore this position, SADC Member States shall

[5] Europay, Mastercard and Visa -- is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. When a payment is made in-store, the card is inserted into a compatible card reader, the EMV chip is read, and data is exchanged in a highly secure manner, using encryption. PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.

promote the adoption and use of Payment Card Industry Data Security Standards (PCI DSS)[4]. Under the PCIDSS, Certification is required for every merchant or business accepting credit or debit cards, online or off. The standards require merchants and processors to meet 12 criteria across six security arenas:

a. Build and maintain a secure network and systems

b. Protect cardholder data

c. Maintain a vulnerability management program

d. Implement strong access control measures

e. Regularly monitor and test networks

f. Maintain an information security policy

Cross-border transactions:

SADC Member States shall, through the appropriate regulatory and policy measures, promote the development and deployment of new payment technologies and software platforms that are increasingly having a positive impact on supplementing traditional banking infrastructures in supporting cross-border E-commerce and trade. These include the following:

a. Emerging transnational systems that decrease reliance on correspondent networks;
b. Government-led initiatives and mandates to regulate payments and fees;
c. Payment systems designed to manage credit risk, liquidity, and costs more effectively;
d. Multinationals seeking to achieve economies of scale, with a side-benefit of consolidating credit risk;
e. Outsourcing that seeks to increase processing efficiency and drive down costs.

Multi-currency and payment methods:

Global E-commerce means accepting a variety of payment methods and currencies. Electronic payments such as e-wallets, mobile payments, and credit/debit cards help online merchants compete in international markets by allowing their customers to pay in their native currencies. For merchants, multi-currency, cross-border transactions can require new bank accounts, new business entities, and new regulatory hurdles in each national market. In support of a conducive cross-border E-commerce environment, SADC Member States shall promote the deployment of payment solutions that enable the easy collection of payments in one currency and credit the merchant account in its home currency.

Money Laundering and Terrorism Financing:

Money laundering refers to the process of trying to hide or disguise the source of illegal money by converting it to funds that appear legitimate. Money laundering is most likely to be successful when criminals avoid leaving a paper trail of transactions linking the money back to the crime. The prevention of terrorist financing generally involves the placement of strict obligations on payment providers such as those outlined in the Patriot Act of the United States of America. In this regard, Payment providers are obliged to retrieve and maintain lists of sanctioned entities, screen A digital wallet/electronic device or online service that allows an individual to make electronic transactions payment parties, block attempted payments to listed entities and countries and report attempted infringement to regulators.

Criminal Exploitation of E-commerce Channels:

Due to the limited capabilities of Member States in terms of detecting, investigating and prosecuting E-commerce-related offences in instances such as drug trafficking, counterfeited and pirated goods, and illegal financial flows such as money laundering, SADC Member States encouraged to establish and cultivate mechanisms for international, inter-agency cooperation to combat various E-commerce-related crimes. It is only through such cooperation mutual legal assistance can be rendered across jurisdictional lines to allow for investigations or prosecutions when websites are hosted outside a national territory. [6]

B. Regulatory Approach

In a general regulatory sense online/electronic payments associated with E-commerce may be considered from the supply side (e-payment service providers) and the demand side (E-commerce consumers).

Supply-side Considerations:

SADC Member States shall, through the proportionate use of appropriate policy and regulatory measures, ensure that the following challenges (associated with electronic payments) are mitigated:

i. Ensuring payment safety and reliability;

ii. Interoperability of bank and nonbank financial service providers;

iii. Divergence between know your customer (KYC) and anti-money laundering (AML) processes;

iv. Difficulty of licensing requirements and procedures for new types of financial services;

v. Outdated technology;

[6] http://www.wcoomd.org/zh-cn/topics/facilitation/activities-and-programmes/ecommerce.aspx

vi. Underdeveloped and inefficient distribution channels;

vii. Risk mitigation for infrastructure failures;

viii. Inadequate infrastructure – whether related to information communication technology or in terms of power supply.

ix. Isolated payment networks and their inherent risks of delays, limited transparency and high costs that the customer often has to bear;

x. Local currency liquidity and associated foreign exchange risks.

Demand-side Considerations:

On the demand side, SADC Member States shall take measures to address the predominance of cash-on-delivery which currently remains popular due to lack of trust, apparent safety, financial illiteracy, sociocultural factors favouring face-to face interactions, slow or no internet connections and inadequate product design.

SADC Member States are further encouraged to enhance existing E-commerce consumer education efforts with the focus on the following aspects:

Consumer Education considerations:

Member states are encouraged to enhance consumer education efforts targeting contractual procedures for E-commerce transactions in particular. Consumers need to be aware of their rights and obligations and how to exercise these in terms of modifying, correcting, or eliminating information on E-commerce platforms. Consumers should also be aware of the terms of use of specific E-commerce platforms/websites which should include clear explanations about how personal data will be used, stored and disposed of.

Additionally, consumers should be made aware of the importance of purchase notifications/confirmations that must be received within a stipulated time by business users in line with applicable legislation. These notifications can be delivered electronically or by any other means indicated that should be indicated in the legal contracts.

Furthermore, Member States may incorporate in their respective consumer education frameworks, the following non-exhaustive consumer checklist or other similar mechanisms to enhance this aspect of the E-commerce regulatory regime:

a) Is there a visible link to the data protection policy for customers?
b) Is it in line with the rules of the laws?
c) Is there a small box that the user must tick to confirm that they have read the data protection policy before sending their information?

d) Is there a small box that the user must tick to confirm a purchase where providing personal information was necessary?[7]

C. Regulatory Principles

In order to address the challenges affecting the supply and demand side of the E-commerce payments ecosystem described above, SADC Member States shall adopt the following general regulatory goals for the associated financial services:

i. Preserving confidence in the system,

ii. Ensuring its integrity and stability,

iii. Protecting users – whether consumers, business or investors –

iv. Promoting efficiency through competition.

Additionally, Member States shall put in place appropriate policies and regulations to ensure minimal risk of loss, prevent systemic meltdowns, address illicit or fraudulent activities, liver compensation to users in the event of a problem, and encourage enough choice to

support various types of economic activity.

Clarity:

i. E-payment regulatory frameworks should provide clear definitions of the roles and responsibilities of the various parties involved in the payment system, including which laws and regulations apply to each of these, and how any relevant supervisory authority may conduct appropriate oversight.;

ii. Overall financial regulatory frameworks should also look to implement e-payment- related rules in a coherent manner;

iii. In some instances, particularly around e-payment service innovations, different regulatory authorities may require specific information or impose specific processes, but may not be collaborating with each other, leading to further fragmentation.

Balanced oversight and supervision:

i. Oversight and supervision of payment systems are crucial for maintaining their integrity and stability;

ii. One of the main objectives of oversight and supervision is the reduction of systemic risk, which could result from legal, liquidity, credit, operational, settlement and/or reputational

[7] https://single-market-economy.ec.europa.eu/sectors/tourism/business-portal/understanding-legislation/legal-regulations-e-commerce_en

risk in the payment system;

iii. To the greatest extent possible, oversight should proceed on a collaborative basis with industry to ensure policy and regulations reflect actual operating conditions and the overall business environment;

iv. Oversight should also take into account the possibility that unnecessarily broad regulations could have unintended consequences that may inhibit investment and innovation in e-payment systems.

Technology-neutrality:

i. As far as possible, regulatory frameworks should be neutral with regard to the payment technology, and should focus on the functions of the service being offered;

ii. The ability of frameworks to stay up to date with technological developments to ensure balanced outcomes is also important.

Encouraging innovation:

i. In the face of technological change, it has become increasingly common practice to enable innovation by creating regulatory safe zones;

ii. These "regulatory sandboxes" are controlled environments in which certain requirements are temporarily suspended, or additional support measures are provided to allow experimentation with new products, most likely with a limited number of consumers;

iii. The approach enables technology firms and financial institutions to collaborate in a less regulated, closed marketplace, with the end result being more effective technology that benefits both business and consumers;

iv. It also enables regulators to better understand the benefits and impacts of a potential technology or payment method being applied more widely.

Access:

i. The regulatory framework should be flexible enough to accommodate innovative payment services and to allow increased access by new participants, such as non- bank PSPs, and other niche service suppliers;

ii. Policymakers may also want to think about the degree to which licensing requirements for the provision of e-payment services are transparent, objective and accessible – including by suppliers not based within the territory.

Risk-based:

i. Policies and regulations dealing with issues such as KYC, anti-money laundering/combating the financing of terrorism (AML/CFT), preventing fraud and cybercrime, currency and reserve

requirements, and data protection should all be applied in a way that is commensurate with associated risk – regardless of who is supplying that service;

- In the case of AML/CFT and based on the assessed risk, Member States may for instance consider the following measures in this regard:

    a. Measures to be considered shall include issuance of Postal KYC/AML/CFT guidelines focussed on the E-commerce business.

    b. Such guidelines may include procedures that enable Postal entities to know and better understand their E-commerce customers and their financial dealings better, which in turn help them manage their risks prudently.

    c. The guidelines may also include the obligation for Postal entities to conduct Customer Due Diligence (CDD) for E-commerce transactions above prescribed monetary thresholds in order to obtain satisfactory evidence and properly establish the identity and legal existence of the customers and business entities involved in such transactions.

    d. Unwillingness of the customer to provide the information requested and to cooperate with the customer due diligence process may itself be considered a factor of suspicion.

i. An active and engaged approach from regulators around e-payment innovations can lead to regulatory frameworks that are sound and that also drive financial inclusion.

ii. Increasingly complex regulation and compliance procedures can result in e-payment or other financial service suppliers "de-risking" – which has a clear knock-on impact on the poorest parts of the population;

iv. Further, from a cross-border perspective, efforts could be made to standardise risk- based models;

- A group of countries could, for example, align on the risk threshold below which simplified due diligence KYC measures would apply.

4.2.2 Taxation

Taxation of E-commerce is a normal part of the accepted pattern of how our countries operate. It is therefore incumbent upon tax administrations to exploit the technology available to improve taxpayer services and lower their cost of administration. E-commerce transactions typically introduce the following difficulties when it comes to taxation:

a. Determination of economic activity (to avoid double taxation),

b. Identification of the existence of permanent establishment,

c. Tracing commencing and end point of a transaction,

d. Lack of documentation to know the nature of contract.

In addressing these difficulties, SADC Member states shall adopt a non-discriminatory posture towards the taxation of E-commerce by applying existing rules and concepts such as upholding the fair sharing of the tax base internationally. This objective shall in part be pursued through intensified dialogue with business and trading partners. In so doing, SADC Member States shall prioritise the identification of practical and reasonable ways of applying internationally accepted taxation norms to e-commerce; and, where necessary, of clarifying or developing those norms. Specific attention shall in this regard be given to:

1. Direct Taxation: Concepts such as 'permanent establishment': - the rule which determines the right of a state to tax the profits of an enterprise of another state and how this applies to the E-commerce environment;
2. The evolution of Indirect taxation laws to keep pace with the changing business dynamics of E-commerce since the activities involve high volume and low-value merchandise,
3. Furthermore, for indirect taxes (such as value-added tax) confirming how international transactions should be treated and clarifying how to collect such taxes on products delivered online. It should in this regard be noted that international online deliveries actually present the greatest challenge, especially when the supplier has no presence at all in the jurisdiction of the customer. While self-assessment by individuals may not be effective in securing this sort of tax, looking to the supplier to collect the tax, (as is the norm for VAT-type taxes), will also have its challenges since the supplier is in another state.
4. Looking towards technology-based systems where the tax calculation and remittal is undertaken by a trusted third party as part of the online transaction.
   While the details of such systems are still being developed, Member States may also consider implementing simplified registration systems for non-resident suppliers.

4.3 Facilitating, Securing and Expediting the Physical Delivery of Goods

4.3.1 Choice of Delivery Channels and Service Providers

The postal operator, be it the public postal operator or the courier service provider need to get into partnership with the online seller to fulfil the delivery of goods bought online.

SADC Member States shall therefore provide a regulatory environment which facilitates Postal and Courier Service providers to offer the following:

A. The collection, transportation, delivery and return of goods bought online;

B. To package their services in such a way that they will entice or meet the expectations of the online seller or supplier as well as of the customers buying goods online;

C. Delivery options which shall meet the online buyer's needs and preferences;

D. Customer- choice in terms of express delivery, non-express delivery, same day delivery and even immediate delivery in case of local deliveries (Universal Postal Union, 2015);

E. Sophisticated options for receiving goods which shall cater for the changing lifestyles of the current generation;

F. Flexible delivery options which shall include scheduled delivery, outside regular times delivery, weekends delivery, and notice of delivery by e-mail and or by short message services;

G. Track and trace of goods as a basic service which shall record the precise information about the status of the order, from the booking to return (Universal Postal Union, 2015);

H. In this regard, operators shall be obliged to ensure that the tracking systems are user- friendly to both the supplier and the buyer and that the tracking information is clear, accurate, in real-time and capable of locating misrouted and delayed orders.

4.3.2 Delivery Terms and Conditions

The terms and conditions of service delivery is an important aspect in every business as it specify the conditions under which the service provider shall render its services and spells out the kind of service the customer should expect from the postal operator. The terms and conditions of service delivery are vital to the postal service provider providing delivery of goods to the e-commerce market. Hence, there should be clear terms and conditions of delivery which shall guide the postal operators in delivery of goods bought online.

The following terms and conditions of delivery shall be followed by postal operators offering services to the E-commerce industry:

A. In delivering goods bought online, the postal operator shall be compliant to the requirements of the laws of the country they are operating in;

B. The postal operator shall publicize its service commitments on the online store website for customer consumption and any changes in service commitments shall be promptly publicized on the online store and the buyers be alerted of such changes;

C. The postal operator shall provide guidelines to the online seller regarding how they should package their goods to protect them from being damaged on transit;

D. The postal operator shall specify its rights and obligations to inspect e-commerce goods upon collection for delivery in their contract with the online seller and the buyer;

E. The postal operator shall refuse to collect and convey e-commerce goods where it finds that the information provided by the seller or the buyer is false;

F. The postal operator shall perform its examination obligation while collecting e- commerce goods and shall not collect and or convey any prohibited item under the provisions of the country they are operating in or by any recognized international organization;

G. The online buyer may treat the goods as lost if they have not been delivered a stipulated timeframe from the expiry of the agreed time for delivery. The determination of the said timeframe may be expressed as a percentage of the agreed delivery time that is to be determined by the National Regulatory Authority if not provided for in the service providers' approved terms and conditions. The loss of items under this provision shall allow the buyer to seek the remedies outlined in the relevant sections of these guidelines;

H. The operator shall be compelled to provide full disclosure of Cost, Insurance and Freight information with regards to all applicable E-commerce transactions.

4.3.3 Liability and Compensation

General Considerations and Rules:

In order for the E-commerce market to be sustainable there is a critical need to provide clarity around the liability exposure of the e-seller (Web-shop or e-merchant) and the carrier (postal or courier service provider). The allocation of risk and liability must be commensurate with the level of responsibility assumed by either party and allow for fair compensation in case of poor performance of the carriage contract. This is especially desirable in cases where the bargaining position is lacking for the e-seller.

In establishing this fair balance between the e-seller and the carrier, SADC Member States shall set forth and apply the following rules:

a) The e-seller's obligations under the sales contract and/or the agreed terms and conditions of sale shall be taken into consideration when determining liability;

b) Based on the specific features of the merchandise/parcel/shipment and also taking into account existing conventions and general conditions, the following principles shall be applied:

   i. The determination of liability shall not be mode-specific, as postal and courier service providers operate different means of transportation and often even stipulate the freedom to select the means of transportation;

   ii. There shall be no per-kilo limit to liability, as especially for consumer goods the weight cannot be considered as a relevant parameter to determine the value of the

goods,

iii. The actual value of the goods is often totally unknown to the postal or courier service provider. Compensation may therefore impose an unknown exposure to liability on the service provider,

iv. It has to be taken into account that if the e-seller is required to take up insurance in order to be able to get compensation in full, this creates additional transaction costs and eventually also raises the price for the consumer.

c) Default rules on delay, in case a contractual stipulation is missing in the sales contract/terms and conditions,

d) Explicit rules on the liability in case of delivery on the driveway or with third parties not designated for delivery. (In order to avoid moral hazards, it seems possible to impose the liability for this on the postal or courier service provider).

e) Compensation should be based upon the consumer's price, as this includes possible commissions paid to other websites,

f) A limit to liability both in case of loss or damage as in cases of delay. This is to enable the e-seller to easily predict the liability exposure and, if desirable, take out additional insurance.

Carrier Liability:

In determining carrier (postal or courier service provider) liability carrier shall be deemed to be in charge of the goods from the time they have accepted the goods from the e-seller until the time they have delivered the goods to the buyer. Therefore, the carrier shall be liable for any loss, or damage or delay in delivery, if that loss, damage or delay took place while the goods were under their charge, unless the postal operator proves that they took all measures required to prevent such occurrence and its consequences. In this regard, SADC Member States shall set forth within the appropriate regulatory instruments, the following measures:

A. The carrier shall be liable and shall compensate the buyer for the total or partial loss of the goods and for damage which is due to its own negligence and occurring between the time when they take over the goods and the time of delivery as well as for any delay in delivery.

B. However, the carrier shall not be liable for the delay of delivery, loss or damage of goods caused by the wrongful act or negligence by the seller and or the buyer or due to circumstances which the postal operator could not avoid and the consequences of which they could not prevent.

C. If the postal carrier is liable to compensate the online buyer for the total or partial loss of goods, such compensation shall be calculated by reference to the value of the goods at the

place and time at which they were accepted for conveyance.

D. In case of damage, the carrier shall be liable for the amount by which the goods have diminished in value, calculated by reference to the value of the goods at the place and time at which they were accepted for conveyance.

E. Transportation or conveyance charges, customs duties and other charges incurred in respect of the conveyance of goods shall be refunded in full in case of total loss and in proportion to the loss sustained in case of partial loss, but no further damage shall be payable.

4.3.4 Quality of Service - Late or non-delivery of products or delivery of defective products

Quality of Service (QoS) is an important aspect of any business. In the context of E-commerce, the carrier has a crucial obligation to deliver goods to the buyer in accordance to the agreed terms and conditions. SADC Member States shall therefore ensure that the regulatory framework obliges Postal and courier operators to:

a) Deliver goods in good condition;

b) at an agreed place;

c) and to deliver them within the agreed time frame or period.

Delayed Delivery:

A delay in delivery shall be deemed to have occurred when goods have not been delivered within the agreed time or within a reasonable time. Where applicable, the delay in delivery shall constitute a failure to perform contractual obligations on the side of the carrier, except for reasonable or justifiable deviations which shall not be resulting from its own negligence. Over and above this stipulation carriers shall remain bound to the current Quality of Service Standards applicable in SADC Member States in line with the SADC QoS Guidelines of 2016-2017.

4.3.5 Returns

In order to protect E-commerce consumers, the regulatory framework should also give customers the right to return the goods bought in case they are dissatisfied with the condition of those goods.

The postal operator shall therefore make arrangements with the online supplier such that in case the buyer is dissatisfied with the goods bought, they can return them back to the supplier. The postal operator shall accommodate for the return of goods in their pricing. The above notwithstanding, the operators shall clearly define the circumstances under which goods can be returned and disclose beforehand, who bears the cost of such returns.

Furthermore, for return of goods to happen, the supplier and the buyer must have agreed on the

return of the goods and have a written agreement. For the postal operator to accept return of goods, the buyer shall produce an agreement for return of order from the supplier to the postal operator. According to the Universal Postal Union, there are two models for merchandise return process. These models are:

a) Simple Return or Non-Simultaneous Exchange: Under this model, the seller authorizes the buyer to ship the goods to be returned and the buyer posts the returning goods in any facility for posting.
b) Simultaneous Exchange: Under this model the seller sends the buyer a new product and request the postal operator to make delivery after receiving the product being returned by the buyer. The postal operator then sends the returned goods back to the seller.

The postal operator shall allow the exchange of goods to happen either at their own office or at the buyer's premises. The postal operator shall receive a checklist of the content to be returned from the online supplier which shall use to ensure that the right items are being returned. The postal operator shall accordingly label the goods being returned across border with the Return Label developed by the UPU to avoid the risk of the goods being mistakenly taxed as a new import (Universal Postal Union, 2015).

Also, in relation to Returns, Service providers shall be compelled to clearly spell out the Refund and Payment Reversal Conditions in the context of E-commerce transaction.

4.4 General Legal and Regulatory Issues

4.4.1 Identity Management

In order ensure the provision of reliable proof of digital identity in the E-commerce environment, SADC Member States shall, through the proportionate use of appropriate legal and regulatory instruments, establish a framework for the effective verification of the identity of remote parties by determining:

a) who is seeking access to an online database of sensitive information, who is trying to do an online transfer of funds from an account,
b) who signed an electronic contract,
c) who remotely authorised a shipment of a product?

Recommended Approach:

SADC Member States shall, take the necessary steps to further increase trust in Identity Management systems in order to extend its use. This objective shall be pursued through the review and/or introduction of legal/regulatory instruments specifically addressing Identity Management in

the following ways:

1. Clarification of parties' obligations,
2. Allocation of liability, e.g., through Presumptions; Exemptions and limitations of liability,
3. Establishing an enabling environment for identity management,
4. Clarifying the legal status of Identity management,
5. Preparation of adequate legal tools to facilitate mutual recognition,
6. Identification of legal obstacles in cross border identity management systems.

4.4.2 Jurisdiction and Choice of Law

E-commerce exists in a borderless environment. It is this characteristic that creates the concern of Jurisdiction including the following specific questions:

1. Where to take action?
2. What test and laws to be followed?
3. What happens when an individual resides outside the jurisdictional area?
4. Laws of which country applies on a particular E-commerce transaction?
5. Courts/Authorities of which country are to be approached for enforcement of rights? While the exercise of jurisdiction across national borders is governed by treaties between the countries, the promotion of intra-regional ecommence will require the harmonisation and concerted implementation of applicable legal/regulatory provisions dealing with the following aspects of cross-border transactions:

1. Enforcement of Rights of the Parties
2. Dispute Settlement
3. Intellectual Property Rights
4. Consumer Protection
5. Data Protection
6. Taxation

4.4.3 Formation and Validity of Contracts

SADC Member States shall have a common approach to determining the legal enforceability of contracts in the E-commerce environment. SADC Member States shall seek a common approach to addressing the following questions through the appropriate legal/regulatory provisions:

1. When an offer is said to have been made,
2. When an acceptance has been communicated back to the offeror,
3. whether the website advertisement is an ‘invitation to treat" or an offer,
4. When a contract is actually formed,
5. Establishment of time and place of contract,
6. Electronic Signatures,
7. Evidential weight of electronic signatures.

In so doing, Member States shall set forth within the appropriate legal instruments, the legal provisions in Appendix 1 of these Guidelines

4.5 Trade Facilitation

Within the context of these guidelines, SADC Member States shall take the necessary policy and regulatory measures to ensure that the Postal Sector remains an integral element of regional trade value-chains. In so doing, Member States shall ensure that the unique characteristics of the regional postal network are fully utilised to promote and facilitate cross- border trade by MSMEs.

In this regard, the postal sector shall be positioned to complement and support the implementation of the SADC Industrialisation Strategy by facilitating affordable and efficient market access for goods and services that are produced in the region by not only providing appropriate postal and courier services but also providing information and assistance to traders.

Implementation of Guidelines

It is recommended that CRASA Members implement the applicable provisions of these guidelines, or revisions thereof, within two years of approval by the CRASA AGM.

6. References

- Assessing regulatory and procedural measures in trade: An Evaluation Methodology **– United Nations (2013)**
- White Paper on Addressing E-Payment Challenges in Global E-Commerce - **World Economic Forum (2018)**
- Stuck between consumer protection and carrier's limited liability: The recourse GAP in the Case of E-commerce – **Dr. Wouter Verheyen (2015)**
- Legal Issues in E-commerce – Nishith Desai Associates (**Aashit Shah and Parveen Nagree)**
- Legal Issues in E-commerce – **S. U. Khan Associates Corporate & Legal Consultants (Islamabad –Pakistan)**
- Worldwide trade integration through the postal network: UPU activities **– UPU (2014)**

APPENDIX 1. GENERAL LEGAL PROVISIONS FOR E-COMMERCE PROMOTION

- **Time of contract formation:**
  - Where parties conclude a contract by means of electronic communications, such contract is formed at the time when and the place where the acceptance of the offer becomes effective.
  - An offer in the form of an electronic communication becomes effective at the time it is received by the offeree.
  - The acceptance of an offer by means of an electronic communication becomes effective at the time that it is received by the offeror.

- **Contract Validity:**
  - Where electronic communications are used in the formation of a contract, that contract shall not be denied legal effect, validity or enforceability on the sole ground that an electronic communication was used to make an offer or to accept an offer for that purpose.
  - A proposal to conclude a contract made through one or more electronic communications, which is not addressed to one or more specific parties but is generally accessible to parties making use of information systems (including proposals that make use of interactive applications for the placement of orders through such information systems) is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

- **Variation by agreement:**
  - The provisions above shall apply, unless the parties involved in generating, sending, receiving, storing or otherwise processing electronic communications, have agreed otherwise.

- **Time of dispatch of electronic communications:**
  - The dispatch of an electronic communication occurs when it enters an information system outside the control of the originator or of the person who sent the electronic communication on behalf of the originator,
  - Where the originator and the addressee are in the same information system, the dispatch of an electronic communication occurs when it is capable of being retrieved by the addressee.

- **Time of receipt of electronic communications:**
  - If the addressee has designated an information system for the purpose of receiving electronic communications, the time of receipt of an electronic communication is determined as follows: a. at the time when the electronic communication enters the designated information system; or b. when the electronic communication is sent to an information system of the addressee that is not the designated information system, at the time when the electronic communication is capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.
  - An electronic communication is deemed to be capable of being

retrieved by the addressee for the purposes of subsection 12(2) and paragraph b of subsection 13(1) when it reaches the addressee's electronic address,

- If the addressee has not designated an information system, receipt occurs when the

electronic communication is retrieved by the addressee or should reasonably have been retrieved by the addressee.

- **Place of dispatch and receipt of electronic communications:**
  - An electronic communication is deemed to have been dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business,
  - For the purposes of subsection (a) above: a. if the originator or the addressee has more than one place of business, the place of business is: i. that which has the closest relationship to the underlying transaction having regard to the circumstances known or contemplated by the parties at any time before or at the conclusion of the contract; or ii. where there is no underlying transaction, the principal place of business. b. If the originator or the addressee does not have a place of business, reference is to be made to that person's habitual residence.
  - This section shall apply notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be dispatched or deemed to be received under this section.

- **Automated message systems**:
  - A contract formed by the interaction of an automated message system and a person, or by the interaction of automated message systems, shall not be denied legal effect, validity or enforceability on the sole ground that no natural person reviewed each of the individual actions carried out by the systems or the resulting contract,
  - Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the electronic communication in which the input error was made if: a. the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication and wishes to cancel the contract or cancel the input error,
  - The person, or the party on whose behalf that person was acting, takes reasonable steps, including steps that conform to the other party's instructions, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services, or to cancel the input error; c. the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, or the input error, if any, from the other party; d. if a person has paid for any goods or services prior to exercising a right referred to in subsection 1, such person is entitled to a full refund of such payment, and the refund shall be made within 30 days of the date of cancellation,

- Nothing in this section affects the application of any rule of law that may govern the consequences of any errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in subsection 2.

- **Attribution of electronic communications:**
    - An electronic communication is that of the originator if it was sent by:
    - the originator personally;
    - a person who had authority [is duly authorised] to act on behalf of the originator in respect of that electronic communication;
    - an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

- **Admissibility and Evidentiary Weight of Electronic Communications:**
    - Where the law requires information to be presented in its original form, that requirement is met by an electronic communication if: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as an electronic communication or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed in the form of an electronic communication to the person to whom it is to be presented,
    - Sub-section 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form,
    - For the purposes of paragraph (a) of subsection 1: (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and (b) the level of reliability shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances,
    - In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic communication in evidence: a. on the sole ground that it is in the form of an electronic communication; or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form,
    - Information in the form of an electronic communication shall be given due evidential weight,
    - In assessing the evidential weight of an electronic communication, regard shall be had to: a. the reliability of the manner in which the electronic communication was generated, stored or communicated; b. the reliability of the manner in which the integrity of the electronic communication was maintained; c. the manner in which its originator was identified; and d. any other relevant factor,
    - An electronic communication made by or on behalf of a person in the ordinary course of business, or a copy or printout of, or an extract from such electronic communication certified to be correct, is admissible in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, as evidence of the facts contained in such record, copy, printout or extract against any person, provided: a. the affidavit is made by the person who was in control of the system at the time when the electronic communication was created; b. the affidavit contains sufficient information on the following: i. the reliability of the manner in

which the electronic communication was generated, stored or communicated; ii. the reliability of the manner in which the integrity of the electronic communication was maintained; iii. the manner in which the originator of the electronic communication was identified; and iv. the reliability of the information system.

- **Retention of records:**
    - Where the law requires that certain documents, records or information be retained, that requirement is met by electronic record retention, providing that the following conditions are satisfied: a. the electronic record contained therein is an electronic communication;

b. the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and c. such electronic record is retained in a form that enables the identification of the origin and destination of an electronic record or electronic communication and the date and time when it was first generated, sent or received, and the date and time it was first retained.

    - An obligation to retain documents, records or information in accordance with subsection 1 does not extend to any information of which the sole purpose is to enable the message to be sent or received.
    - A person may satisfy the requirement referred to in subsection 1 by using the services of any other person, provided that the conditions set forth in paragraphs a, b and c of subsection 1 are met.

- **Production of document or information:**
    - Where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of an electronic communication, an electronic form of that document or information, and if: a. considering all the relevant circumstances at the time that the electronic communication was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and b. at the time the electronic communication was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.
    - For the purposes of subsection 1, the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for a. the addition of any endorsement; or b. any immaterial change, which arises in the normal course of communication, storage or display.

- **Notarisation, acknowledgement and certification:**
    - Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the secure electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or electronic communication.
    - Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a printout certified to be a true reproduction of the document or information.
    - Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by

the use of a secure electronic signature.

- **Other requirements:**
    - A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single electronic communication that is capable of being reproduced by that addressee.
    - An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, shall be interpreted so as to include or permit such form, format or action in relation to an electronic communication unless otherwise provided for in this Act.
    - Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such a document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the secure electronic signature of the person by whom it is required to be sealed.
    - Where any law requires or permits a person to send a document or information by post or similar service, that requirement is met if an electronic form of that document or information is sent to the electronic address provided by the addressee.

- **Consumer Protection - Obligations of the supplier:**
    - A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following information available to consumers: a. its full contact details, including its place of business, e-mail addresses and telefax number(s); b. a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction; c. the full price of the goods or services, including transport costs, taxes and any other fees or costs; d. information regarding the payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned; e. any terms of agreement and the manner and period within which consumers can access and maintain a full record of the transaction.
    - The supplier shall provide the consumer with an opportunity: – a. to review the entire electronic transaction; b. to correct any mistakes; and c. to withdraw from the transaction, before finally placing any order.
    - If a supplier fails to comply with the provisions of sub-sections 1 or 2, the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.
    - If a transaction is cancelled in terms of subsection 3: – a. the consumer shall return the performance of the supplier or, where applicable, cease using the services performed; and b. the supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

- **Consumer Protection – Performance:**
    - The supplier shall execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed

otherwise.

- Where a supplier has failed to execute the order within 30 days or within the agreed period, the consumer may cancel the agreement with seven days' written notice.
- If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

- **Consumer Protection - Cooling-off:**
    - A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply: a. of goods within seven days after the date of the receipt of the goods; or b. of services within seven days after the date of the conclusion of the agreement.
    - The only charge that may be levied on the consumer is the direct cost of returning the goods.
    - If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection 1, the consumer is entitled to a full refund of such payment, which shall be made within 30 days of the date of cancellation.
    - This section shall not be construed as prejudicing the rights of a consumer provided for in any other law.
    - This section shall not apply to electronic transactions: a. for financial services, including but not limited to investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities; b. by way of an auction; c. for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer; d. for services which began with the consumer's consent before the end of the seven-day period referred to in this section; e. where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier; f. where the goods: i. are made to the consumer's specifications; ii. are clearly personalised;

iii. by reason of their nature cannot be returned; or iv. are likely to deteriorate or expire rapidly; g. where audio or video recordings or computer software were downloaded or unsealed by the consumer; h. for the sale of newspapers, periodicals, magazines and books; i. for the provision of gaming and lottery services; j. for online gambling; k. for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period; and l. such other exception/s as may be prescribed.

- **Applicability of foreign law:**
    - The protection provided to consumers in this chapter applies irrespective of the legal system applicable to the agreement in question.

- **Non-exclusion:**
    - Any provision in an agreement which excludes any rights provided for in this chapter is null and void.

- **Mere conduit:**
    - A service provider shall not be subject to any civil liability in respect of third-party material in the form of electronic communications to which he merely provides access to information system services for the transmitting, routing or storage of electronic communications via an information system under its control, as long as the service provider: a. does not initiate the transmission; b. does not select the addressee; c. performs the functions in an automatic, technical manner without selection of the data; and d. does not modify the data contained in the

transmission.

- The acts of transmitting, routing and providing access referred to in subsection 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place:

- for the sole purpose of carrying out the transmission in the information system; b. in

a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and c. for a period no longer than is reasonably necessary for the transmission.

- **Caching:**
  - A service provider shall not be subject to any civil liability in respect of third-party material in the form of electronic communications for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider: a. does not modify the data; b. complies with conditions on access to the data; c. complies with rules regarding the updating of the data, specified in a manner widely recognized and used by industry; d. does not interfere with the lawful use of rights management information, widely recognized and used by industry, to obtain information on the use of the data; and e. removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 35.

- **Hosting:**
  - A service provider shall not be subject to civil liability in respect of third-party material in the form of electronic communications where the service provider provides a service at the request of the recipient of the service that consists of the storage of data provided by a recipient of the service, as long as the service provider: a. does not have actual knowledge that the electronic communication or an activity relating to the electronic communication is infringing the rights of a third party; or
  - b. is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic communication is apparent; and c. upon receipt of a take-down notification from the aggrieved party referred to in section 30, acts expeditiously to remove or to disable access to the data.
  - (2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its service, including on its websites in locations accessible to the public, the contact details of the agent.
- Subsection 1 does not apply when the recipient of the service is acting under the authority or the control of the service provider.

- **Information location tools:**
  - A service provider shall not be subject to civil liability in respect of third-party material in the form of electronic communications if the service provider refers or links users to a web page containing an infringing electronic communication or an infringing activity, by using information location tools, including a directory, index, reference, pointer or hyperlink, where the service provider: a. does not have actual knowledge that the electronic communication or an activity relating to the electronic communication is infringing the rights of that

person; b. is not aware of facts or circumstances which evidences the infringing activity or the infringing nature of the electronic communication;

c. does not receive a financial benefit directly attributable to the infringing activity; and d. removes or disables access to the reference link of the electronic communication or activity within a reasonable time after being informed that the electronic communication or the activity relating to such electronic communication infringes the rights of a person.

- **Take-down notification:**
    - For the purposes of this chapter, a notification of unlawful activity shall be in the form of an electronic communication, and it shall be addressed to the service provider or its designated agent.
    - The notification shall include a. the full names and address of the complainant; b. the signature of the complainant; c. identification of the right that has allegedly been infringed;

d. identification of the material or activity that is claimed to be the subject of unlawful activity; e. the remedial action required to be taken by the service provider in respect of the complaint; f. telephonic and electronic contact details, if any, of the complainant; g. a statement that the complainant is acting in good faith; h. a statement by the complainant that the information in the take-down notification is to his or her knowledge true or correct.

- Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.
- A service provider is not liable for wrongful take-down in a bona fide response to a notification of unlawful activity which complies with subsection 2.

- **No general obligation to monitor:**
    - When providing the services contemplated in this chapter there is no general obligation on a service provider to:

- monitors the data which it transmits or stores; or
- actively seek facts or circumstances indicating an unlawful activity.
    - The regulator may, subject to the provisions of any other law, prescribe procedures for service providers to:
- informs the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and
- to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.