East African Communications Organisation

Communications for all in East Africa

EACO GUIDELINES ON CONSUMER EXPERIENCE AND PROTECTION IN DIGITAL FINANCIAL SERVICES

Prepared by EACO

July 2017

Table of Contents

1. Introduction

Digital Financial Services (DFS) refers to the use of an electronic device or system to access financial services such as storing funds, making and receiving payments, applying for credit or for insurance. Due to the inaccessibility and high costs of formal banking for low income and rural communities and the increase in access to mobile phones, DFS has become a viable way for the unbanked to access formal financial services.

The legal and regulatory frameworks that govern DFS play a critical role in creating an enabling environment for low income and unbanked populations to become financially included. One important aspect within regulation is how the rights and interests of consumers are protected and promoted. It is therefore important that regulations are developed to among others protect consumers from fraud, safeguard personal data and consumer funds, ensure transparency in the operation of the systems and make available recourse mechanisms as and when required.

An effective consumer protection framework within DFS can increase consumer confidence thereby increasing adoption and active use of the services. While the interests of consumers are important it is also imperative that the legal and regulatory framework remains fair and balanced for all stakeholders.

Accordingly, Mobile financial services can be delivered using any of the following communication modes:

- Interactive Voice Response (IVR)
- Short Messaging Service (SMS)
- Wireless Access Protocol (WAP)
- Stand-alone Mobile Application Clients (Mobile Apps)
- Unstructured Supplementary Service Data (USSD)
- Using SIM tool Kit (STK)
- Internet

Editor note: From DFS ITU_T document on Consumer protection

2. Scope

This guideline covers the following:

- Issues in Digital financial services

- Dispute resolution
- Fraud prevention issues
- Data protection and privacy
- Quality of Service parameters

3. References

[ITU-T E.800] Recommendation ITU-T E.800 (2008): *Definitions of terms related to quality of service*

4. Abbreviations and Acronyms

EACO : East African Communication Organisation

NRA : National Regulatory Authorities

ITU : International Telecommunication Union

5. Definition of Terms

6. Guideline

For a MNO, mobile money services began as value added services, additional to the core mobile voice and data business and partly a customer retention strategy. MNOs leverage their existing physical telecommunication networks, agent networks, existing contractual relationships with customers, and distribution interface with the customer through the mobile phone, and deliver the service. In EAC region, most of MNOs had launched mobile money transfer and payment services.

However, MNOs are not the only providers of mobile financial services; banks and other providers also offer services, according to [Digital Financial Services: Regulating for Financial Inclusion]. Numerous providers that are neither MNOs nor banks can offer account, transfer and payment services over the mobile network as well.

The network services required are usually unstructured supplementary service data (USSD), as discussed in section 3.4.1. A variety of models are used to negotiate access to these channels, and it is a key area where competition problems arise, as discussed in section 3.4.2.

Some banks have even chosen to enter the mobile services market by establishing a mobile virtual network operator (MVNO) in order to distribute their banking services, as Equity Bank has done in launching Equitel My Money in Kenya.

6.1. Issues of Digital Financial Services

Mobile financial services: Mobile money transfer and payments services

1) **Issues faced by Consumers:**

a) **Subscribers: (normal customers)**

Challenges faced by subscribers:

i. Delayed transactions: time it takes to receive a response on the status of a transaction to notify if it has failed or successfully.
ii. Notification on the cost of a transaction.
iii. Send the money to the wrong number ;
iv. SIM card lifecycle : access to fund on expired or disabled SIM card
v. Fraud : Impersonation
vi. Data privacy – use of customer data for other purposes other than the subscribed service
    a. In rural areas, agents may face a problem in accessing mobile financial services because they do not have reliable power supply.
vii. International mobile money transfer and roaming

b) **Agents:** (they are working on behalf of the Telecom Operators in making deposit, withdraw the money, registration of customers to mobile money, transfer money on behalf of subscribers.

Challenges faced by agents:

a. In rural areas, agents may face a problem in accessing mobile financial services because they do not have reliable power supply.
b. Insecurity
c. Fake money /currency
d. Account reconciliation: the amount registered by the system is not equal to the cash received by the Agent.

c) Financial Institutions (Super Agents): Electronic-money management;

d) Corporate customers: Government institutions, SMEs.

- Payment to wrong account / business number
- Delayed transactions:
- Fraud
- Integration with MNOs platforms (that provides Mobile financial services)

2) Issues faced by Telecom Operators:

a. Transaction Reversal request
b. Competition malpractices (in both telecom and financial industry)
c. Cyber attacks
d. Unequal global uptake
e. Unclear regulatory framework
f. Digital illiteracy of customers
g. Accessibility of network, service and devices
h. Interoperability

3) Issues faced by Regulators:

a. Cyber attacks
b. Unclear regulatory mandate between telecoms, financial and competition regulators
c. MFS is an new technology which need more studies

6.2. Dispute Resolution

Providers of DFS should ensure that that access to redress is accessible, affordable, independent, fair, accountable, timely and efficient. In doing this service providers shall:

6.2.1. Ensure that a complaints policy and procedure is put in place

6.2.2. That the Policy is effectively communicated to consumers using multiple channels and in common local languages

6.2.3. Make available multiple recourse channels for consumers to file their complaints

6.2.4. Inform their clients on the available alternative dispute resolutions mechanisms or external recourse whenever they are not satisfied with resolution mechanisms provided by the service provider

6.2.5. Ensure that the time frames of how long consumers should expect to wait for a response are reasonable and clearly communicated to consumers.

6.2.6. Consumers have access to a designated toll free phone line for dispute resolution

6.2.7. Employees are trained and provided with scripts/procedures for the most common complaints received.

6.3. Provision of Information and Transparency

Providers of DFS should ensure that clear, adequate, accurate and complete information on the services is provided to all users. In doing this, providers of DFS shall ensure that:

6.3.1. Full disclosure of terms and conditions of contract is made prior to the customer initiating use of the services.

6.3.2. Full disclosure of all fees and charges related to the service are made prior to a transaction.

6.3.3. Standardized key fact documents on the service are made available to consumers in a language that they can understand.

6.3.4. Adequate time is given to consumers before any changes to fees or terms and conditions come in effect.

6.3.5. Advertisements are devoid of any ambiguity and that they use a simple and plain language

6.3.6. When an account becomes dormant, all the funds are transferred to a specified account and the transaction is effectively communicated to the consumers.

6.4. Fraud Prevention issues

6.5. Data protection and Privacy

DFS providers shall ensure that the highest levels of data protection and privacy are maintained in the way customer data is collected, stored, shared and exploited. In doing this, service providers shall ensure that:

6.5.1. Data related to DFS is encrypted both when in transportation and when stored

6.5.2. They implement levels of authorization and/or separation of roles to ensure that employees, agents, or business partners are not able to access the entirety of a

consumer's data without justification

6.5.3. Customers are clearly and effectively informed of what data will be collected and how it will be used, prior to its collection and use, and are given the option to consent or not

6.5.4. They collect personal information that is only necessary for the purpose

6.5.5. A data collection and handling policy is put in place indicating the different types of data to be collected and under which circumstances it may be shared

6.6. QoS Parameters

6.6.1. USSD Parameters

7.1.1. USSD service non-accessibility [%]

The USSD service non-accessibility is the probability that the end-user cannot access the Unstructured Supplementary Service Data (USSD) when requested while it is offered by display of the network indicator on the UE.

• Target: 2% - 1% - 0.5%

7.1.2 USSD completion failure ratio [%]

• Target: 1% - 0.5% - 0.1%, Or even 0%

7.1.3 USSD end-to-end delivery time [s] - Target values:

– 60 sec for 90%, 120 sec for 100%

– 30 sec for 95%, 90 sec for 100%

– 10 sec for 98%, 30 sec for 100%

7.1.4. USSD receive confirmation failure ratio [%]

• Target: 1% - 0.5% - 0.1%

7.2. Short Message Services

7.2.1 SMS service non-accessibility [%]

The SMS service non-accessibility is the probability that the end-user cannot access the Short Message Service (SMS) when requested while it is offered by display of the network indicator on the UE.

• Target: 2% - 1% - 0.5%

7.2.2. SMS end-to-end delivery time [s]

The SMS end-to-end delivery time is the time period between sending a short message to the network and receiving the very same short message at another UE.

• Target values:

– 60 sec for 90%, 120 sec for 100%

– 30 sec for 95%, 90 sec for 100%

– 10 sec for 98%, 30 sec for 100%

7.2.3. SMS receive confirmation failure ratio [%]

The SMS receive confirmation failure ratio is the probability that the receive confirmation for a sent attempt is not received by the originating UE although requested.

• Target: 1% - 0.5% - 0.1%

7.3. HTTPS

7.3.1. HTTPS Service non accessibility [%]

The HTTPS service non-accessibility ratio is the probability that a subscriber cannot establish a PDP context and access the service successfully.

The packet data protocol (PDP) context is a data structure present in several parts of the mobile network which contains the subscriber's session information when the subscriber has an active session.

• Target: 2% - 1% - 0.5% ?

.

7.3.2. HTTPS set-up time [s]

The HTTPS set-up time is the time period needed to access the service successfully, from starting the connection to the point of time when the content is sent or received.

• Target values:

– 30 sec for 90%, 60 sec for 100%

– 15 sec for 95%, 30 sec for 100%

– 8 sec for 98%, 20 sec for 100%

7.3.3. HTTPS session failure ratio [%]

The HTTPS IP-service access ratio is the probability that a subscriber would not be able to establish a TCP/IP connection to the server of a service successfully.

• Target: 2% - 1% - 0.5%

7.3.4. HTTPS session time [s]

The HTTP session time is the time period needed to successfully complete a packet switching data session.

• Target values:

– 30 sec for 90%, 60 sec for 100%

7.3.5. HTTPS data transfer cut-off ratio [%]

The HTTP data transfer cut-off ratio is the proportion of incomplete data transfers and data transfers that were started successfully.

• Target: 2% - 1% - 0.5%

7.3.6 Integrity of complaint resolution [%]

Ratio of the number of complete and professional resolutions of the contributory causes of a complaint, to the total number of user complaints accepted.

• Target: 2% - 1% - 0.5% ?