

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(05/2019)

DSTR-DFSCP

**Digital Financial Services – Commonly identified
consumer protection themes for digital financial
services**

Summary

This Technical Report is a synthesis of existing research, legal provisions, guidelines, and other related resources related to consumer protection for digital financial services. This Technical Report identifies four common themes that policy makers or regulators may want to consider when developing laws, regulations, or guidelines related to DFS.

This list is not exhaustive, but rather indicative of the types of issues that can be considered. In addition, consumer protection for digital financial service is a new area for regulations, and in many cases there is continued discussion and debate about which aspects can be best addressed by industry-led actions, versus requiring regulations. Finally, the feasibility of implementation and enforcement have not been taken into account when developing this list; these of course are critical elements when developing actual DFS guidelines.

The four themes are:

- 1 Provision of information and transparency
- 2 Fraud prevention
- 3 Dispute resolution
- 4 Data privacy and protection

For each theme, a set of key issues have been identified, and these are discussed in the following Report.

Keywords

Consumer protection, digital financial services.

Change Log

This document contains the ITU-T Technical Report on "*Digital Financial Services – Commonly identified Consumer Protection themes for Digital Financial Services*", which was agreed at the ITU-T Study Group 3 meeting held in Geneva, 23 April – 2 May 2019.

Table of Contents

	Page
1 Scope.....	3
2 References.....	3
3 Definitions	3
3.1 Terms defined elsewhere	3
3.2 Terms defined in this Technical Report	3
4 Abbreviations.....	3
5 Introduction.....	3
6 Methodology.....	4
7 Key themes in consumer protection for digital financial services.....	4
7.1 Provision of information and transparency	5
7.2 Dispute resolution.....	6
7.3 Fraud prevention.....	7
7.4 Data protection and privacy.....	8
Bibliography.....	10

Technical Report ITU-T DSTR-DFSCP

Digital financial services – Commonly identified consumer protection themes for digital financial services

1 Scope

See Summary.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations

AFI	Alliance for Financial Inclusion
BB	Bangladesh Bank
BTRC	Telecommunication Regulatory Commission
CBN	Central Bank of Nigeria
CCI	Competition Commission of India
CEP	Consumer, Experience and Protection Working Group
CGAP	Consultative Group to Assist the Poor
DFS	Digital Financial Services
FGDFS	Focus Group Digital Financial Services
GSMA	Groupe Speciale Mobile Association
ITU	International Telecommunication Union
MNO	Mobile Network Operator
MMO	Mobile Money Operator
NCC	Nigerian Communications Commission
PPIs	Prepaid payment instruments
RBI	Reserve Bank of India
TRAI	Telecom Regulatory Authority of India

5 Introduction

Digital Financial Services (DFS) in this Technical Report 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 (Potnis, 2014). Increasing access to formal financial services and thus reducing financial exclusion is seen as an important development goal as it has been argued to stimulate economic growth, thereby increasing welfare and reducing poverty (Kundu, 2015).

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. Consumer trust is the foundation for achieving sustainable uptake and active usage of DFS. This includes protecting consumers from fraud, safeguarding personal data and consumer funds, ensuring transparency and ensuring recourse mechanisms are available.

Financial consumer protection has gained increased attention since the global financial crisis, which increased pressure for providers to be transparent in their business conduct, disclose key information about their products and services, and treat consumers fairly and ethically (Tiwok, 2013).

An effective consumer protection framework within DFS can increase consumer confidence thereby increasing adoption and active use of the services. This is even more important for unbanked users who may not have prior experience with formal banking services (World Bank, 2014). While the interests of consumers (and especially low income consumers to increase financial inclusion) are important it is also imperative that the legal and regulatory framework remains fair and balanced for all stakeholders (World Bank, 2015).

6 Methodology

The study involved a desk review of key issues for consumer protection in digital financial services. This included reviewing the key publications and research conducted by leading international organizations and experts within DFS on the consumer risks and consumer protection approaches.

The methodology did not, however, attempt to analyze the feasibility of implementation or enforcement of the identified issues. It also did not aim to identify which consumer protection issues are best addressed through industry action, and which are best addressed through regulation. Therefore, a more detailed analysis is necessary before regulators take action on any of the points listed below.

7 Key themes in consumer protection for digital financial services

The publications, reports and focus notes from leading DFS organizations and research groups such as AFI, CGAP, GSMA and the World Bank were reviewed to determine the key themes for consumer protection. These organizations were chosen as they are at the forefront of driving financial inclusion in low income countries.

Good consumer protection practices protect the interests of consumers, creating trust in using digital financial services, while preserving the commercial incentive to provide these services at scale. Developing a regulatory framework requires regulators to analyze the roles of players in the value chain (banks, MNOs, non-banks, agents, e-money issuers, etc.) and consumer risks. DFS in many emerging economies are driven by innovations in mobile technologies, so the mobile network operators that provide the telecommunication infrastructure are critical players in the ecosystem.

Consumers can experience a number of potential risks when conducting DFS transactions. Fraud is an example of the various forms these risks can take. For example, DFS provider employees may gain access to consumer accounts and use the private information for dishonest purposes, or fraudsters may use social engineering scams to obtain money or information from unsuspecting customers.

Consumers can also experience fraud from agents, who could charge them unauthorized fees, or access private customer information including their PINs.

The DFS provider is the entity which is actually providing the service to the consumer and is ultimately responsible for ensuring transparent, fair, and safe services and protecting the consumer's funds and personal information. For instance, clear terms and conditions in the DFS service contract explaining the consumer rights and obligations, clear explanation of fees charged to consumers, the availability of timely complaint mechanisms and dispute resolution process reduces risk while enhancing consumer trust in using DFS. The liability of consumers, agents and DFS providers in case of errors is also an important part of transparency.

Four core themes were identified as central to consumer protection in order to mitigate the risks for consumers.

- 1 Provision of information and transparency
- 2 Dispute resolution
- 3 Fraud prevention
- 4 Data privacy and protection

Each of these areas of focus are now considered in more detail.

7.1 Provision of information and transparency

Providing consumers with information and transparency in all digital financial services and products is crucial to develop trust and uptake. Absence of information is likely to result in consumer lack of knowledge and awareness on key product features, terms and conditions, which heightens the risk to consumers. To counter this, 'clear, adequate, accurate and complete information' should be provided to all users (AFI, 2014, p. 6).

It is vital that providers are transparent about their services and products so that consumers have the opportunity to make informed choices and avoid risks such as agent misconduct, overcharging or misleading advertisements and scams (McKee, Kaffenberger, & Zimmerman, 2015; World Bank, 2014). Collaborative research undertaken by MicroSave, CGAP and BFA in four countries (Uganda, the Philippines, Bangladesh and Colombia) found that unclear pricing was seen as a high risk by consumers (Malady, 2015).

In addition to providers, delivering transparent and accurate information it is essential that consumers are able to understand the information provided to them in order to increase their capabilities and empower consumers to make informed choices.

The key issues in information and ensuring transparency are detailed below:

Table 1 – Information and transparency

Key issues	Examples
1. Transparency of fees	Full disclosure of all fees and charges is provided prior to a transaction. Ideally fees are disclosed in multiple formats (in brochure, verbally, on website etc).
2. Key facts or summary document	Standardized key fact documents can enable providers to give consumers the key information related to the service or product concisely and in local language.

Table 1 – Information and transparency

Key issues	Examples
3. Terms and conditions are transparent	Full disclosure of terms and conditions of contract is made prior to the customer initiating use of the services. Unclear terms or complicated sentences are avoided so that they are as easy to understand as possible. T&Cs are available in common local languages. Simplified contracts and standard form contracts also enable simplified disclosure of terms and conditions to customers.
4. Cooling off period	Cooling off period is available to consumers so that if they change their mind on a product/service within x weeks and terminate a contract without facing penalties.
5. Notice period for changes to terms and conditions, fees	There is an adequate time given to consumers by the providers before any changes to fees or terms and conditions come in effect.
8. Misleading advertisements and sales promotions are prohibited	Advertisements, which are misleading, are prohibited. Ideally advertisements should use plain and simple language
9. Policy on dormant accounts	Clear policies over when an account is considered dormant and what happens to the funds are effectively communicated to the consumers.

7.2 Dispute resolution

As the DFS ecosystem continues to expand with more services and products available to consumers, it becomes increasingly essential to have effective recourse mechanisms in place. Principle 9 of the G20 High Level Principles on Financial Consumer Protection states that access to redress should be 'accessible, affordable, independent, fair, accountable, timely and efficient.' (World Bank, 2014, p. 27). Effective dispute resolution is even more important for DFS users who were previously unbanked and are new to formal financial services as it can help consumers in overcoming challenges related to adoption and trust (Mazer & Garg, 2015; Chapman & Mazer, 2013). Evidence of this was found in a study of M-Pesa in Kenya where the ability to receive effective dispute resolution led to increased trust and loyalty, which had a positive effect on increasing customer uptake of the services (Collins and Zollman 2011 cited in Chapman & Mazer, 2013).

Effective dispute resolutions are not only important in improving trust and adoption for consumers, but the wealth of information that can be collected and analysed offers an opportunity to improve products and services. For example, in Pakistan, Tameer Microfinance Bank used data collected from complaints to identify the consumers who have a higher default risk and subsequently were able to target these consumers with more assistance (Chapman & Mazer, 2013).

Table 2 – Dispute resolution

Key issues	Examples
1. Complaints policy and procedures in place	DFS providers have a complaints policy and procedure in place
2. Complaints policy is transparent and communicated to consumers	Policy is effectively communicated using multiple channels (such as in branch, online, leaflets, verbally by agents etc.), and the policy is made available in common local languages.
3. Multiple recourse channels available to the consumer	Access to a variety of channels to make complaints such as toll-free numbers, local agents, social media, and branches etc.

Table 2 – Dispute resolution

Key issues	Examples
4. Alternative dispute resolutions or external recourse	Consumers who are not satisfied with how their complaint was handled by their provider are able to access alternative or external channels to seek redress. Information on how to use alternative methods is readily available.
5. Time frame provided for dispute resolution	Time frames of how long consumers should expect to wait for a response are reasonable and clearly communicated to consumers.
6. Dedicated, toll-free recourse helpline available	Consumers have access to a designated phone line for dispute resolution and it is toll free.
7. Coordination between the financial and telecom regulators in dispute resolution	Close coordination and collaboration between the financial and telecom regulators (including sharing data and analysis on DFS complaints) ensures effective resolution. This information can also inform their DFS-related licensing, supervision/oversight, and enforcement roles.
8. Oversight of the recourse system by the financial regulator or supervisor	Financial regulator or supervisor has the remit to monitor complaints and listen to and resolve disputes. This can include providers sharing complaints data with the regulator and/or onsite checks for compliance.
9. Employees and agents are trained in handling disputes	Employees are trained and provided with scripts/procedures for the most common complaints received. Moreover, the categorization of complaints makes handling disputes more efficient.

7.3 Fraud prevention

Fraud is a key issue for consumer protection as not only can it result in loss of funds or the misuse of personal data, but the fear of fraud can prevent users from adopting DFS in the first place or prevent OTC users from adopting wallets and more advanced services. There are a number of ways that fraud can be categorized. GSM Association has identified three common types of fraud by the perpetrator¹:

- 1) **Transactional** – Fraud that may be committed by a user posing as a genuine consumer
 - a) vishing/smishing – Use of phone calls or SMS to gather personal information such as account details, PINs or passwords or other identification details.
 - b) advance fee scams – Where customers are tricked into sending funds under fake circumstances or promises (e.g., lottery scams).
 - c) reversal requests – Where a person may ask a user to refund them an incorrect transaction that was deposited in their account.
- 2) **Channel** – Fraud that may be carried out by the agent
 - a) **split transaction** – Agents split a transaction to earn more commission.
 - b) **false transactions** – Agents transfer consumer funds to their own account.
 - c) **registration fraud** – Creating false accounts for the purpose of obtaining extra registration commissions.
 - d) **overcharging** – Agents charging unauthorized or incorrect fees.

¹ Source: Managing the risk of fraud in mobile money, GSMA.

- 3) **Internal** – Fraud that may be committed by an internal employee
- a) **internal fraud** – Employees colluding for unfair personal gain.
 - b) **identity theft** – Employees accessing and exploiting customer information without authorization.

Examples of when fraud has occurred include lottery scams in Bangladesh where users were told they must send a fee in order to gain access to their winnings. In Uganda cases of reversal requests were reported where SMS requests were sent to users informing them that funds had been incorrectly deposited in their account and that they should return them (McKee, Kaffenberger, & Zimmerman, 2015). While the occurrence of fraudulent activity is relatively low, the perception of the threat of fraud is high. The key issues for fraud prevention are described below:

Table 3 – Fraud prevention issues

Key issues	Examples
1. DFS providers are licensed and supervised under a regulatory framework	DFS can only be provided by licensed entities (banks and non-banks) and are regulated by the financial regulator. The DFS provider is required to adhere to the licensing requirements at all time.
2. Regular network testing, real-time monitoring and ongoing checks for security systems and processes	To prevent and detect fraud there should be ongoing checks to ensure that information systems and applications are working correctly.
3. Due diligence to be conducted on staff and agents	Due diligence is carried out on all staff (employees, contractors, agent etc.) prior to hiring.
4. Providers are responsible for their agents	Providers are responsible for the conduct of their agents, ensuring providers effectively manage and train their agents.
5. Agent monitoring	To ensure that agents comply with regulations and guidelines their activities are monitored by providers. This may be done through onsite checks or mystery shopping. Clear sanctions are in place for agents who are found to be not complying.
6. Agent training	Providers ensure agents are trained to a high standard to reduce the chance of errors occurring and to be able to offer knowledgeable support to consumers. Ideally, training should be compulsory and ongoing.
7. Transactions occur in real time	When the network is down, consumers sometimes leave money with agents to carry out the transaction later. This can leave customers open to agent fraud, if the agent instead keeps the money. Real time transactions would cut down on this type of fraud, though in many geographical areas real time transactions are still challenging in practice.
8. Consumers are encouraged to report fraudulent activity	Consumers are aware of and understand the process to report suspected incidences of fraud to their provider or to financial and telecom regulators.
9. Consumer awareness campaigns on the common types of fraud	Consumers are informed of the common types of frauds prevalent in the market through various channels (such as SMS alerts, radio announcements, signage at agent location, etc.).

7.4 Data protection and privacy

Data protection and privacy measures are concerned with the way that data is collected, stored, shared and exploited. This is important for consumers because the misuse of data may result in identity theft, damage to a user's credit profile, unsolicited offers, nuisance calls and the influx of fraudulent or

unsolicited messages among other risks and harms. This area of consumer protection in DFS is in very early stages, with little law and regulation in existence.

Many new users of DFS are creating a 'digital footprint' for the first time. This refers to the accumulation of data that takes place when a consumer uses their digital device (McKee, Kaffenberger, & Zimmerman, 2015).

In a recent study carried out by Makulilo (2015) on data privacy for DFS in Africa, it was noted that there are many opportunities for data abuse and leakage due to extended value chains and many players involved in a transaction. In addition, there may be incentives for data commoditization for things such as targeted advertising. Makulilo claims that in Uganda the government has misused data on claims of national security and then passed it on to business entities to promote their services through unsolicited messages.

Early considerations in data privacy include:

Table 4 – Data protection and privacy

Key issue	Examples
1. Encryption of data	Where feasible, data related to DFS is encrypted both when in transportation and when stored. The systems in place, which encrypt data, are regularly tested and problems addressed.
2. Access restriction to consumer data	As a measure to prevent the misuse of data, providers 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.
3. Informed consent	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.
4. Minimization of data collection and limitation of retention	Providers limit the amount of personal data they collect from consumers to only what is necessary for the purpose. Providers limit the retention of data and destroy data after it is used for its intended purpose.
5. Protection of personal data	Providers ensure that personal data is maintained securely, and there are authentication systems in place. There are repercussions in place when personal data is misused.
6. Clear policy on data collection and sharing	Providers should have a data collection and handling policy that states what types of data will be collected and under which circumstances it may be shared.

Bibliography

- [1] AFI (2013), Mobile Financial Services, *Technology Risks*.
- [2] AFI (2014), Mobile Financial Services, *Consumer Protection in Mobile Financial Services*.
- [3] Chapman, M., & Mazer, R. (2013), *Making Recourse Work for Base-of-the-Pyramid Financial Consumers*. CGAP.
- [4] Collins, D., & Zollman, J. (2011), *Financial Capability and the Poor: Are we missing the mark? Kenya: FSD Insights*.
- [5] Consumers International (2011), *Safe, fair and competitive markets in financial services, recommendations for the G20 on the enhancement of consumer protection in financial services*.
- [6] Dermish, A. (2015), *Country Diagnostic: Nigeria. Better Than Cash Alliance*.
- [7] Di Castri, S., Grossman, J., & Sihin, R. (2015), *Proportional risk-based AML/CFT regimes for mobile money*. GSMA.
- [8] Grossman, J. (2016), *Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected*. London: GSMA.
- [9] GSMA (2014), Country Overview: Bangladesh. London: GSMA. GSMA. (2015), *Code of Conduct for Mobile Money Providers*.
- [10] GSMA (2015), *Digital Inclusion and the Role of Mobile in Nigeria*. London: GSMA.
- [11] GSMA (2015), *Digital Inclusion and the Role of Mobile in Nigeria*. London: GSMA.
- [12] GSMA (nd) (2016), *Mobile Money Regulatory Guide*. Retrieved February 1.
- [13] Kundu, D. (2015), *Addressing the demand side factors of financial inclusion. Journal of commerce and management thought*, 6(3), 397-417.
- [14] Makulilo, A. (2015), *Privacy in Mobile Money: Central Banks in Africa and their Regulatory Limits*. International Journal of Law and Information Technology, 0, 1-20.
- [15] Malady, L. (2015), *Consumer Protection Issues for Digital Financial Services in Emerging Markets*. Centre for International Finance and Regulation (CIFR), UNCDF, Working Paper.
- [16] Mazer, R., & Garg, N. (2015), *Recourse in Digital Financial Services: Opportunities for Innovation*. CGAP.
- [17] Mazer, R., & Rowan, P. (2016), *Competition in Mobile Financial Services*. CGAP.
- [18] McKee, K., Kaffenberger, M., & Zimmerman, J. (2015), *Doing Digital Finance Right*. CGAP.
- [19] Murithi, J. (2015), *Competition in the Kenyan Digital Finance Market: Mobile Money (Part 1 of 3)*. Retrieved February 23, 2016, from Helix Institute of Digital Finance.
- [20] Parvez, J., Islam, A., & Woodard, J. (2015), *Mobile Financial Services in Bangladesh*. USAID.
- [21] Potnis, D. (2014), *Examining mobile banking in developing nations from a pro-poor 'context, culture and community' perspective. Proceedings of the American Society for information science and technology*, 1-4.
- [22] Sitbon, E. (2015), *Addressing competition bottlenecks in digital financial services*. Journal of Payments.
- [23] Strategy & Systems, 9(3), 351-365.

- [24] Tiwok, s. (2013), *Developing a framework for financial consumer protection in Vanuatu*. The Flether School, Tufts University.
- [25] Tumusiime-Mutebile, E. (2015), *The development in mobile banking in Uganda*. Remarks by Mr Emmanuel Tumusiime-Mutebile, Governor of the Bank of Uganda, at the meeting with Parliamentary Committee on Information and Communication Technology. Kampala: Bank for International Settlements. Retrieved from <http://www.bis.org/review/r150310d.htm>
- [26] World Bank (2012), *Good Practices for Financial Consumer Protection*.
- [27] World Bank (2014), *Global Survey on Consumer Protection and Financial Literacy: Oversight Frameworks and Practoces in 114 Economies*. Washington DC.
- [28] World Bank (2015), *Payment Aspects of Financial Inclusion*. Committee on Payments and Market Infrastructures, World Bank Group.
- [29] World Bank, DfID, OECD. (2009), *The case for financial literacy in developing countries*.
-