



Keeping clients first  
in microfinance

# **Potential risks to clients when using Digital Financial Services**

*An analysis report to inform the Evolution  
of the Client Protection Standards*

**Lead Author:  
Sonia Arenaza, Director, Channels and Technology**

**September 2014  
Collaboration between the Smart Campaign and  
Accion Channels and Technology**

## Potential Risks to Clients in using Digital Financial Services: From Risk Awareness to Recommendations

Potential Risks to Clients in using DFS: From risk awareness to recommendations .....	2
1. Introduction .....	2
2. Purpose of this Report .....	2
3. Methodology: risks to consumers mapping exercise .....	3
4. Key takeaways .....	4
5. Key players in the Digital Financial Services Ecosystem .....	5
6. Critical potential risks to clients .....	5
7. Risks and the Smart Campaign CPPs.....	7
8. Early Evidence .....	9
9. Risk Mitigation for DFS Ecosystem .....	14
10. Annex A – Complete Risk Matrix for DFS.....	20
a. Client Protection .....	20
b. Quality of Service .....	27
11. Annex B.....	30
a. Type of risk.....	30
b. Terminology .....	30
12. Annex C – The Client Protection Principles and Standards .....	31
13. Annex D – About the Authors .....	32
a. Smart Campaign.....	32
a. Accion Channels and Technology .....	32
14. References .....	33

## Potential Risks to Clients in using DFS: From risk awareness to recommendations

### 1. Introduction

The Client Protection Standards were created to operationalize where the microfinance industry sets the bar in terms of the minimum behaviors clients should expect from institutions with which they conduct business. Building off of the seven Client Protection Principles (CPPs), the Client Protection Standards specify what 'doing no harm' must entail in practice. The current 30 standards represent the output of several years of industry collaboration and input managed by the Smart Campaign (See Annex C for the complete list of the standards). For the standards released in January 2013 as part of the Client Protection Certification program, the Campaign worked with a Task Force of over 30 experts representing various stakeholders to develop and vet the recommendations. The standards are truly a public good for and by the industry.

Standards which reflect social norms and expectations of an evolving industry must be dynamic. In order to incorporate an ever-growing sector and its diversity of products, services and related client-protection risks, the Smart Campaign has begun to work to evolve and improve its standards. One of the key directions of industry evolution is towards the use of Digital Financial Services (DFS). Therefore in partnership with the Accion Channels and Technology team, and under the management of an Evolution of Standards working group, the Smart Campaign began a work stream to understand the potential emerging risks to clients when using Digital Financial Services and how best to mitigate those risks.

Given the Smart Campaign's momentum of working directly with microfinance and financial service providers since 2009, the work stream initially sought to understand the intersection of two primary areas:

- How are microfinance providers using digital financial services? For which we have published a first research note: *Digital Financial Services and Microfinance: State of Play*<sup>1</sup>
- What are the potential emerging risks to clients using digital financial services? How do these risks align with the seven Client Protection Principles? What is the current evidence and frequency of those risks? What are the possible recommendations? This latter point is the main purpose of this report.

**It is from the intersection of these two key inquiries that the first set of recommendations for the Evolution of the Client Protection standards will emerge.** These recommendations will then be discussed, debated and tested in the field for viability before becoming a permanent part of the standards and part of the Client Protection Certification Program.

It is anticipated that most immediate application of these recommendations will be to microfinance institutions as part of the Certification program, however the Campaign firmly believes that the Client Protection Principles and standards are relevant and applicable to the wider ecosystem encompassed by all DFS.

### 2. Purpose of this Report

In the context of the Evolution of Standards of the Smart Campaign and its Digital Financial Services work stream –which analyzes the potential risks that the use of these services poses to clients– this paper aims to deep dive into a thorough analysis of potential risks to clients in using DFS by involving all the variety of typical actors of the ecosystem in the analysis, exploring evidence of those risks in implementations, and recommending actions to mitigate those risks and minimize harm to clients and offer a comprehensive client protection risk matrix.

This desk research is intended to fill a knowledge gap in the mapping of risks to clients by answering the following questions:

<sup>1</sup> See research at [https://centerforfinancialinclusionblog.files.wordpress.com/2014/08/20140821\\_eos\\_dfs\\_mfis.pdf](https://centerforfinancialinclusionblog.files.wordpress.com/2014/08/20140821_eos_dfs_mfis.pdf)

- What are the emerging risks to clients using digital financial services?
- How do these risks align with the seven Client Protection Principles?
- What are the potential consequences of those risks?
- What is the potential impact to clients?
- What is the current evidence on those risks and their consequences?
- What are the possible recommendations to overcome/mitigate those risks?
- When identifying risks, how to draw the line between Client Protection and Service Quality?

Understanding the risks and harms clients face in using DFS will help the Smart Campaign narrow the scope for its initial set of recommendations by understanding what is salient and being used in the field. Indeed, this research will help the Smart Campaign be in a better position to improve the existing Client Protection Standards to pinpoint safeguards to minimize and mitigate against risks to clients when different providers roll out DFS. This research on *Risk to Clients in using DFS* along with the first note on *Digital Financial Services and Microfinance: State of Play* will lead to key recommendations for service providers implementing DFS who strive to meet the Smart Campaign's principles of Client Protection.

### 3. Methodology: risks to consumers mapping exercise

As part of this analysis, we have performed a risk stocktaking that considers what goes wrong or could go wrong for clients when using DFS and what are the possible harms to the client, and applying the lens of the CPPs. The attributes of the potential risks in the Client Matrix are presented visually in Figure 1:

**Figure 1 - Attributes of Potential Risks to Clients Matrix**



The risk matrix includes the following information:

- *Who is affected:* while clients are mainly affected and are our focus, this exercise has also identified risks in which agents and providers can also be affected;
- *Potential Risk:* provides a title for the risk e.g., agent's misconduct, data privacy, data protection and security;
- *Description of the risk:* provides detailed information regarding the risk;
- *Smart Campaign Principle:* we have mapped the risks to one or more of the CPPs since a hypothesis was to test whether the seven CPPs are an appropriate conceptual umbrella;
- *Potential impact of risk on client:* indicates our assessment –based on evidence and our experience working in the field– of the impact of a specific risk on clients. It can be high, medium, or low;
- *Evidence:* we have gathered information of examples, statistics, and scenarios in which risks happen in DFS deployments. Despite this, we consider that more evidence is needed in the vast use of DFS for the BoP. Where no direct evidence has been found, we provide cases that could be extrapolated from the provision of DFS services to the commercial sector;
- *Recommendations:* we have recommended actions to mitigate risks and safeguards to reduce/eliminate the impact of risks based on an analysis of the risk along with its evidence and impact on clients;
- *Type of risk:* classifies the risk as pertaining to a standard risk category such as operational, reputational, technology, financial, systemic, regulatory, and institutional. See Annex B: Type of Risk;
- *Client protection/Service quality:* In exploring risks we have considered all the variety of typical actors of the ecosystem and have found that some risks are closely related to Client Protection while others are related to Service Quality, which is not as relevant for the Smart Campaign. We have preserved all those risks in the risk matrix.

#### 4. Key takeaways

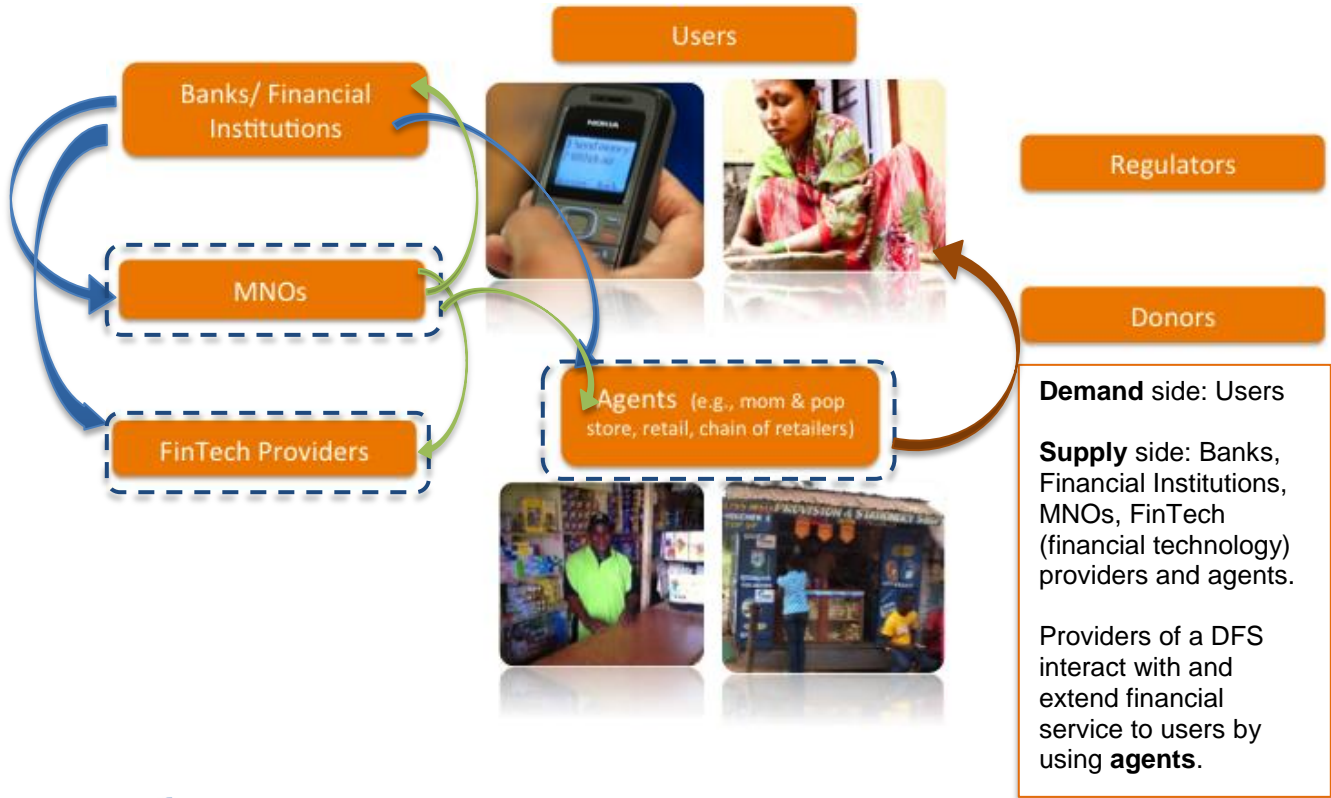
In drawing key takeaways from this risk mapping exercise, we recognize the following:

- The Smart Campaign **CPPs** are robust **umbrellas** that cover the risks identified in the matrix
- There is a need for **more evidence** of harm to clients in using DFS for the BoP. The nascent field of DFS requires more data to be collected globally that considers the different players in the ecosystem that provide and receive the services as well as regulators and experts;
- The most common **consequences** of the risks are: loss of trust and significant drop along the client's journey –from awareness to registration, then from registration to first use, and from first use to regular use; clients lose trust in the system and therefore reduce use of the service; client loses funds and might not use the service anymore which in general leads to low adoption and usage drops;
- There is no clarity on who is **responsible** for protecting the client –is it the bank, financial institution, MNO, third party provider? As there are many actors along the value chain, there are blurry lines with regards to responsibility (e.g., on effectively communicating the client in such a manner that clients understand the service, their rights and obligations, on adequately performing clients' requests such as cash in/cash out, and on solving clients' questions, doubts and complaints);
- The involvement of many players along the value chain makes DFS **complex**; in addition to that the regulatory framework varies from country to country. It is yet to be determined how much self-regulation can protect clients, when the regulator should intervene to ensure risks to clients are mitigated, or who is responsible for compliance when services are provided by different providers;
- While mobile money and branchless banking are services provided by different actors, **agents play a key role in client protection**. Agents are sometimes the sole form of interaction with clients. There is need for a better design of the incentives, training, and monitoring of agents to ensure clients are well served and there is no harm against them.

### 5. Key players in the Digital Financial Services Ecosystem

The provision of digital finance involves the participation of different players such as banks/financial institutions, mobile network operators (MNOs), financial technology providers, regulators, agents, chains of retailers, clients, and donors. As such, the interaction of these actors and the conditions of the regulatory environment and market archetype in which they participate pose complexities both to them and to the clients they serve.

Figure 2 - DFS Ecosystem



**Banks/FI** get into partnerships or use the services of MNOs, FinTech companies and Agents



**MNOs** get into partnerships or use the services of Bank/FI, FinTech companies and Agents

Worth noting is that providers of the service can either perform the function of managing the agent network internally or subcontract the services of one or more Agent Network Manager (ANM).

### 6. Critical potential risks to clients

We have identified a list of 36 key potential risks clients face in using DFS corresponding to the Smart Campaign’s Client Protection Principles and classified them based on **evidence** (how frequently the risk is seen; availability of examples, statistics, and scenarios in which risks happen in DFS deployments) and potential **impact** of risk on clients (high, medium or low risk that might harm clients and/or hinder adequate provision of services to them).

In light of the depth and breadth of these risks, we have narrowed half of the risks in 10 prioritized potential risks (*Table 1* also shows a detailed description of those risks).

These risks have also been categorized into standard types of risks such as operational, reputational (poor client adoption, trust, and perception), technology, financial, systemic, regulatory, and institutional risks. See *Annex A – Complete Risk Matrix for DFS* for the complete list of risks.

With regards to the evidence for risks: Preliminary results from a forthcoming study conducted by CGAP and carried out by MicroSave and Bankable Frontier Associates –performed in 2014 in Uganda, Bangladesh, Philippines, and Colombia– ‘*Consumer Protection and Emerging Risks in Digital Financial Services*’ shows that customers are mainly worried about high/unclear service charges, poor customer service support, agent liquidity, service downtime, agent unavailability, and wrong transactions followed by PIN related risks, agent overcharges, fake messages and untrustworthy agents. These risks pertain to the following Client Protection Principles: appropriate business conduct, data privacy and protection, customer recourse, and transparency.

**Table 1 – Lists of Key DFS Potential Risks Explained**

Key Potential Risks		
<b>A</b>	<b>Clients do not make informed decisions due to inadequate information from providers</b>	1 Clients are not adequately communicated with nor trained on: (i) Service understanding (e.g., how the service works, how to use it, how to register, how to opt-out), (ii) Trust in the service (e.g., reinforce client confidence in the service, security of data), (iii) Client service (e.g., where to complain/call if the service does not work, if the transaction did not go through, if the agent does not provide adequate service, etc.)
<b>B</b>	<b>Inadequate or lack of client care channel/recourse mechanism (e.g., client support, client helpdesk, dispute resolution, and complaint mechanisms)</b>	2 Provider offers inadequate support, dispute resolution, and complaint mechanisms to clients. Thus, when issues occur: (i) clients do not know who to approach, (ii) these centers are not accessible, (iii) call centers/complaint line do not adequately deal with client queries and complaints, (iv) client's concerns are not addressed in a timely and fair manner.
<b>C</b>	<b>Data protection and security</b>	3 Client identity is stolen and may be used to open an account or perform transactions, which could lead to identity theft.
<b>D</b>	<b>Data privacy</b>	4 Clients are not informed/misinformed on how their data and history is being used or shared. Hence: (i) client information could be inappropriately sold or tracked without client consent, (ii) client could start receiving abused/unauthorized advertising online and cross marketing.
<b>E</b>	<b>Clients are defrauded and/or lose their funds</b>	5 When (i) Service presents faulty security that allows information to be stolen and misused, (ii) Clients share their PINs with another person, (iii) A non-client uses a friend or family member's account (more than one user of the service) to perform unauthorized transactions instead of the registered client
		6 When the mobile money/branchless banking service has system downtime or some processes are manual, transactions performed by clients can be delayed, lost, or clients can even be victims of stolen payments.

Key Potential Risks		
	7	When an employee of the service provider commits fraud by manipulating data and transactions performed by clients
<b>F Clients cannot access their funds or float</b>	8	Agents often have either cash or float when client is asking for other so they can't get their money (float and liquidity management issues)
	9	Clients cannot redeem funds/perform transactions due agent's to lack of liquidity.
<b>G Insufficient transparency and disclosure of information</b>	10	Information on roles and responsibilities of the agent, product and service fees, prices, terms, conditions, mechanism to address client's complaints, and timeliness of updates/changes are not properly disclosed to client.
<b>H Unauthorized fees, abusive prices charged to clients</b>	11	Agents charge unauthorized fees or agent does not clearly disclose fees/prices to the client;
	12	Clients are charged abusive prices due to market structure i.e., in non-competitive markets with a dominant player or a monopoly, the provider could abuse its position and charge abusive prices)
<b>I Agent's inability leads to lack of service</b>	13	Clients cannot access the service because agent does not know how to perform the transaction.
<b>J Agent's misconduct against clients</b>	14	Clients are treated unfairly due to inadequate incentive structure rewards to agent
	15	Agents persuade clients to avail of particular transactions and services not because those are in their best interest but because they provide higher fee/commissions for agents;
	16	Female clients fear harassment from agents or are not served by agent
	17	Agent's discriminate against clients due to security concerns (e.g., agent working in high-risk neighborhoods can be target of thefts and robbery. This situation is aggravated when agents do not have any insurance provided by a bank, MNO, or provider; or are not self-insured;
	18	Agent performs/accepts transactions with counterfeit cash by himself or colluding with a third-person. Also, agent provides this money to clients

### 7. Risks and the Smart Campaign CPPs

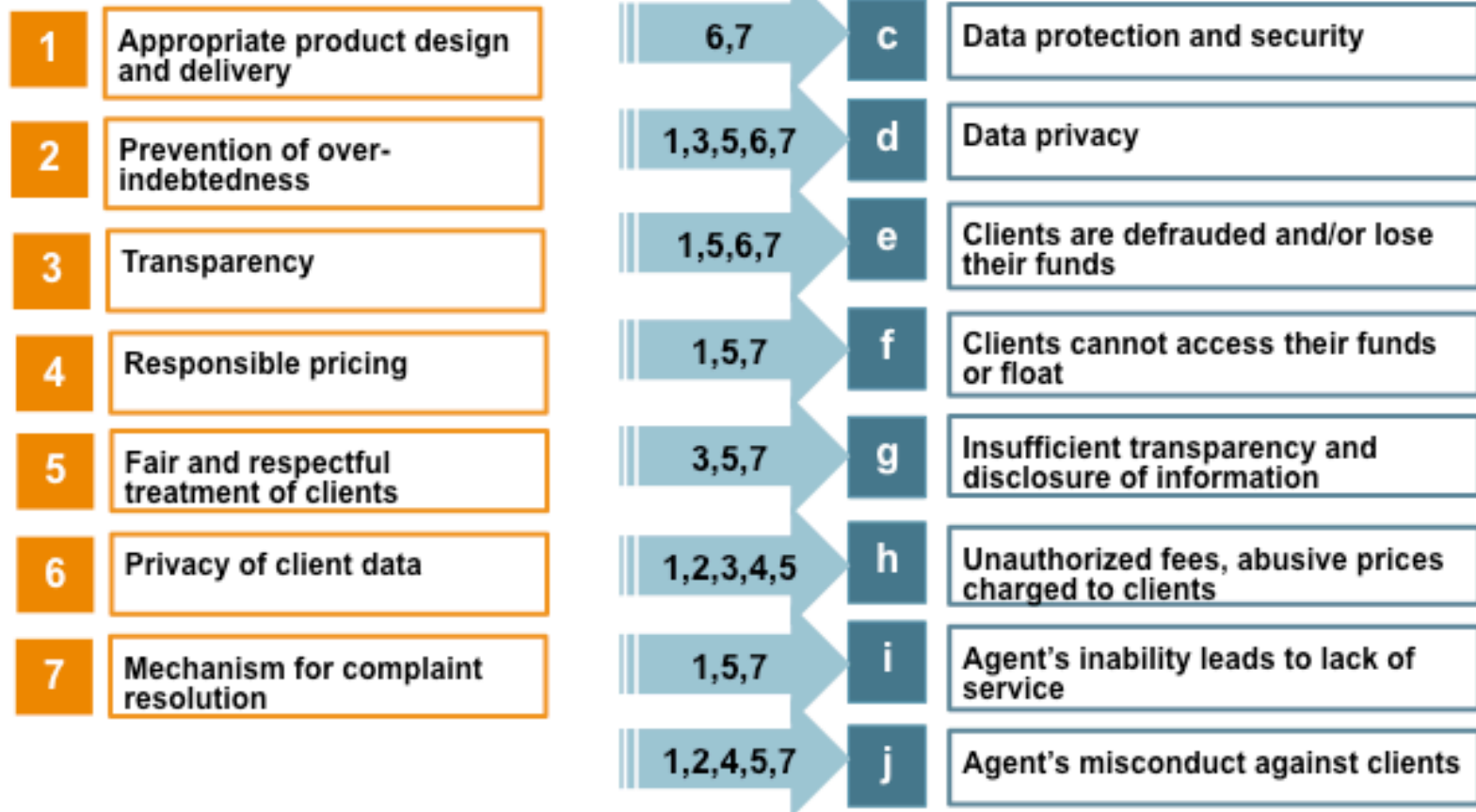
During the analysis, we mapped out the Smart Campaign seven principles next to major potential risks to clients and have determined that the principles robustly cover those risks, for example:

The risk "Clients do not make informed decisions due to inadequate information by providers" is mapped to the Principles: 1. Appropriate product design and delivery, 3. Transparency, and 7. Mechanism for complaint resolution. Therefore we encourage the CPPs to continue to be used as a framework within which responsible digital financial services are enumerated and discussed.



Figure 3- Mapping Key DFS Potential Risks to 7 CPPs

During the analysis, we mapped out the Smart Campaign seven principles next to major potential risks to clients and have determined that the principles robustly cover those risks, for example:



## 8. Early Evidence

While much more evidence is needed in order to properly rank the impact of each risk and prioritize mitigation effect, there are some clear examples of these risks occurring in the field, both in developing and developed markets, particularly among aforementioned top critical risks to clients, shown below. Overall, we believe that more evidence will be helpful to understand if the digital delivery of financial services poses more or less risks to clients than when services are delivered by traditional means to the BoP.

Some evidence (sources provided below):

- In Tanzania, one in five registered users share their mobile money PIN with another person, one in seven carried out mobile money transactions with the help of an agent, and might have had to share their PINs with the agent.
- In the use of Agents, 25% have used a friend or family member's account
- In Pakistan, 19% of women and 10% of men who are not interested in opening an account agreed with the statement that it's not safe to give money to agents.
- In Papua New Guinea, 47% of women and 35% of men who want a mobile financial services account identified lack of understanding of how to use it as their chief reason for not opening an account
- The usual daily transactions per day in Africa are 21-30 (e.g., Kenya 46, Uganda 30, Tanzania 31)
- A study showed that 80% of mobile users desired privacy of their personal data
- There is prevalence of agents charging unauthorized fees.

**Table 2 - Early Evidence on DFS Potential Risks**

Risk	#	Description of risk	Evidence (examples and statistics)
A <b>Clients do not make informed decisions due to inadequate information from providers</b>	1	Clients are not adequately communicated with nor trained on: (i) Service understanding (e.g., how the service works, how to use it, how to register, how to opt-out), (ii) Trust in the service (e.g., reinforce client confidence in the service, security of data), (iii) Client service (e.g., where to complain/call if the service does not work, if the transaction did not go through, if the agent does not provide adequate service, etc.)	<ul style="list-style-type: none"> <li>• Implementations lack adequate client education, communication, and marketing. (Source: Accion's fieldwork experience)</li> <li>• In Papua New Guinea, 47% of women and 35% of men who want a mobile financial services account identified lack of understanding of how to use it as their chief reason for not opening an account. (Source: GSMA and Visa, 2013)</li> <li>• The usual daily transactions per day in Africa are 21-30 (e.g., Kenya 46, Uganda 30, Tanzania 31). (Source: Helix Institute, 2014)</li> </ul>
B <b>Inadequate or lack of client care channel/recourse mechanism (e.g., client support, client helpdesk, dispute resolution, and complaint mechanisms)</b>	2	Provider offers inadequate support, dispute resolution, and complaint mechanisms to clients. Thus, when issues occur: (i) clients do not know who to approach, (ii) these centers are not accessible, (iii) call centers/complaint line do not adequately deal with client queries and complaints, (iv) client's concerns are not addressed in a timely and fair manner.	<ul style="list-style-type: none"> <li>• The size and level of client care channels/recourse mechanisms vary from sophisticated centers that can expedite client concerns to no client care channels at all. (Source: Accion's fieldwork experience)</li> </ul>

Risk	#	Description of risk	Evidence (examples and statistics)
C <b>Data protection and security</b>	3	Client identity is stolen and may be used to open an account or perform transactions, which could lead to identity theft.	<ul style="list-style-type: none"> <li>Target revealed in 2013 that up to 70 million credit and debit card information of clients was stolen in a data breach. Information swept was names, addresses and phone numbers along with credit card transactions. Target refunded its affected clients. (Source: The Washington Post, 2014)</li> <li>More recently, Visa and MasterCard will face class-action lawsuits related to the development of their chip and PIN technology. (Source: Washington Post and Payment Week, 2014)</li> </ul>
D <b>Data privacy</b>	4	Clients are not informed/misinformed on how their data and history is being used or shared. Hence: (i) client information could be inappropriately sold or tracked without client consent, (ii) client could start receiving abused/unauthorized advertising online and cross marketing.	<ul style="list-style-type: none"> <li>A study showed that 80% of mobile users desired privacy of their personal data (Source: CGAP, 2014)</li> <li>As an example, in a case pitting privacy issues against a Google, European court says Google must respect 'right to be forgotten'. This could be the beginning of more sensitive rules on data privacy and protection (Source: Reuters, 2014)</li> </ul>
E <b>Clients are defrauded and/or lose their funds</b>	5	When (i) Service presents faulty security that allows information to be stolen and misused, (ii) Clients share their PINs with another person, (iii) A non-client uses a friend or family member's account (more than one user of the service) to perform unauthorized transactions instead of the registered client	<ul style="list-style-type: none"> <li>A common fraud risk is vishing, smishing scams tricking clients to use their PINs (Source: GSMA).</li> <li>In Tanzania, one in five registered users share their mobile money PIN with another person, one in seven carried out mobile money transactions with the help of an agent, and might have had to share their PINs with the agent. (Source: Intermedia, 2013).</li> <li>In the use of Agents, 25% have used a friend or family member's account. (Source: Intermedia, 2013).</li> </ul>
	6	When the mobile money/branchless banking service has system downtime or some processes are manual, transactions performed by clients can be delayed, lost, or clients can even be victims of stolen payments.	<ul style="list-style-type: none"> <li>Evidence shows this occurs in cases when there is a system downtime or manual reconciliation process for example provider does not perform reconciliation and agents do not report transactions simultaneously.</li> </ul>
	7	When an employee of the service provider commits fraud by manipulating data and transactions performed by clients	<ul style="list-style-type: none"> <li>In Pakistan, 19% of women and 10% of men who are not interested in opening an account agreed with the statement that it's not safe to give money to MFS</li> </ul>

Risk	#	Description of risk	Evidence (examples and statistics)
			<p>agents. (Source: GSMA and Visa, 2013)</p> <ul style="list-style-type: none"> <li>In one case attracting headlines in Kenya, a man stole more than US\$1,200 through fraudulent transactions on people's phones once he had been told their PINs (CGAP, Kiplagat 2010)</li> </ul>
F <b>Clients cannot access their funds or float</b>	8	Agents often have either cash or float when client is asking for other so they can't get their money (float and liquidity management issues)	<ul style="list-style-type: none"> <li>Especially in rural areas clients might be unable to withdraw the funds they receive electronically.</li> <li>When Zain's ZAP first established an agent network in Kenya, it set a very low bar to be an agent (US\$60 in float and no need to be a licensed business). As a result, it quickly acquired a large agent network, but most agents did not have adequate capital and were looking to make short-term profits rather than committing to a long-term business development strategy. (Source: CGAP, 2011)</li> </ul>
	9	Clients cannot redeem funds/perform transactions due agent's to lack of liquidity.	<ul style="list-style-type: none"> <li>Rapid growth and the non-exclusivity of agents is putting pressure on agents' liquidity, with five transactions a day being denied due to lack of float. Liquidity issues are being driven by non-exclusivity of agents (forcing agents to manage multiple liquidity pools) and agents' apathetic approach to float management (Source: Helix study in Tanzania, 2014).</li> </ul>
G <b>Insufficient transparency and disclosure of information</b>	10	Information on roles and responsibilities of the agent, product and service fees, prices, terms, conditions, mechanism to address client's complaints, and timeliness of updates/changes are not properly disclosed to client.	<ul style="list-style-type: none"> <li>Regulators typically require mobile money, branchless banking service providers to meet certain disclosure and transparency requirements (e.g., Ghana, Philippines, India, Pakistan) (GSMA, 2013)</li> </ul>
H <b>Unauthorized fees, abusive prices charged to clients</b>	11	Agents charge unauthorized fees or agent does not clearly disclose fees/prices to the client;	<ul style="list-style-type: none"> <li>There is prevalence of agents charging unauthorized fees. (Source: Research from MicroSave, InterMedia, CGAP)</li> </ul>
	12	Clients are charged abusive prices due to market structure i.e., in non-competitive markets with a dominant player or a monopoly, the provider could	<ul style="list-style-type: none"> <li>Financial institutions are free to set fees, charges and interest rates. However, La Superintendencia de Banca (SBS) in Peru has legal authority to actively identify and</li> </ul>

Risk	#	Description of risk	Evidence (examples and statistics)
		abuse its position and charge abusive prices)	curb/prohibit predatory or abusive practices and to impose sanctions on financial institutions. SBS, in the course of its supervisory process, evaluates the technical grounds on which the provider sets its prices and fees. Providers cannot unilaterally modify contracts and may change prices only after a 15-day notice so the customer is able to withdraw from the contract if he or she chooses. (Source: SBS and CGAP, 2010)
I <b>Agent's inability leads to lack of service</b>	13	Clients cannot access the service because agent does not know how to perform the transaction.	<ul style="list-style-type: none"> <li>In Papua New Guinea, 47% of women and 35% of men who want a mobile financial service account identified lack of understanding of how to use it as their chief reason for not opening an account. This gap suggests an opportunity to improve education across a provider's network, generally through investments in agent capacity-building. Well-trained agents are better equipped to reduce potential customers' anxiety and overcome women's risk aversion to try new tools. ' (Source: GSMA and Visa, 2013)</li> </ul>
J <b>Agent's misconduct against clients</b>	14	Clients are treated unfairly due to inadequate incentive structure rewards to agent	<ul style="list-style-type: none"> <li>Clients in some markets report the service is not provided to them without any reason from the agent.</li> <li>Also for example, Zain's ZAP in Tanzania pays agents only one-third of the US\$1 registration commission after customer verification. The remainder is paid when a customer makes five transactions in the six months after registering. (Source: CGAP, 2011)</li> <li>One provider in Colombia is experimenting with a tiered system in which the commission per transaction varies depending on how many transactions are done. If agents do very few transactions (five or fewer) they are paid US\$0.08 per transaction. If they are active (more than 25 transactions a day), they are paid almost double, or US\$0.15 per transaction. (Source: CGAP, 2011)</li> </ul>
	15	Agents persuade clients to avail of particular transactions and services not because those are in their best interest but because they provide higher	<ul style="list-style-type: none"> <li>A chit fund (Ponzi scheme) passed through the Pilkhi village in the Nalanda District of Bihar in 2012, convincing individuals to invest in a particular product</li> </ul>

Risk	#	Evidence (examples and statistics)
	Description of risk fee/commissions for agents;	that would earn the agent higher commission. The agent fled overnight with hard-earned savings of many families that had believed was a life insurance product. Now families, and in particular women, are afraid to invest in the government-run JEEViKa program for them to open accounts and receive their remittances via an agent. (Source: CGAP, 2013)
	<b>16</b> Female clients fear harassment from agents or are not served by agent	<ul style="list-style-type: none"> <li>Female clients in some markets report reluctance to provide their phone numbers to agents for fear of harassment.</li> </ul>
	<b>17</b> Agent's discriminate against clients due to security concerns (e.g., agent working in high-risk neighborhoods can be target of thefts and robbery. This situation is aggravated when agents do not have any insurance provided by a bank, MNO, or provider; or are not self-insured;	<ul style="list-style-type: none"> <li>Brazilian banks occasionally are willing to bear the cost of armored car services—usually when an agent is deemed to be playing an important role in reducing congestion at a nearby branch. Ninety-three percent of agents in Brazil say being an agent increases the risk of being robbed, and 25 percent have been robbed in the past three years. In fact, most Brazilian agents go to the bank to drop off extra cash even when the cash they are holding is far below the limit set by the bank. (Source: CGAP, 2011).</li> <li>There is no standard in the provision of insurance against thefts (e.g., banks in some cases provide insurance while other banks and or payment services do not). As a consequence agents leave the network due to robbery (e.g., one or two agents per month). (Source: Accion's fieldwork experience)</li> </ul>
	<b>18</b> Agent performs/accepts transactions with counterfeit cash by himself or colluding with a third-person. Also, agent provides this money to clients	<ul style="list-style-type: none"> <li>In Brazil, 27% of agents have experienced worker theft (avg. loss approx. \$6K USD) and 16% have experienced client fraud, usually counterfeit bills (avg. loss \$189 USD) (Source: CGAP, 2010)</li> </ul>

### 9. Risk Mitigation for DFS Ecosystem

A thorough analysis of the risks clients could potentially face in using DFS including evidence and potential impact on clients has allowed us to define appropriate, suggested actions to mitigate those risks. N.B. These suggestions are aimed at the entire DFS ecosystem and **are not the set of recommendations** for the Client Protection Standards and Certification 2.0. That latter set of recommendations will emerge as an output from this note as well as the first research paper on how microfinance providers are using DFS. The following graphs show the suggested actions for the ten most critical risks.

The general theme of recommendations revolves around:



- Focus on **client communications** and education on effective client understanding of and trust in the service
  - Clients should be able to clearly understand the service, the fees, benefits, their rights and obligations
  - This communication includes techniques that consider the literacy limitations of target BoP clients
  - Research/analyze clients' feedback before, during, and after designing and delivering a product. Also, analyze the data on an on-going basis
  - Clients are informed on roles and responsibilities of the agent, product fees/price/term/conditions, timeliness of updates/changes, and cancellation or disruption of the service
  - Inform clients that when performing a money transfer transaction: (i) in cases where receiver cannot cash out money after a period of time then funds should return to sender and sender should receive a notification; and (ii) if money is sent to the wrong number, a cash reversal needs to be provided by either the agent or the provider (i.e., via client care channel)
- Continuously reinforcing client communication, keeping an open channel of communication and performing periodic client surveys
- **Fees** from the use of services of digital channels (e.g., money transfers, cash-in, cash-out, loan disbursement, loan repayment, top-up) are **not excessive**
- Implementing adequate client **care channels/recourse mechanisms** for client's questions, complaints and support; and informing client regarding those resources
- Clearly define which provider is ultimately **responsible for providing services** and solving client issues
- Defining clear recruitment, selection, and monitoring processes for **agents**. Also, improving liquidity management support such as improving procedures, monitoring agents, cash management services, ATMs, and providing credit to agents
- Monitoring **agent performance** and defining processes for reinforcing training, warning of misconduct, and/or removing underperforming agents
  - Ensure agent does not charge unauthorized fees to clients
  - Ensure agent does not request pin codes, passwords and account numbers from clients which should be kept confidential to the client
  - Ensure agent does not persuade clients to avail of particular transactions and services not because those are in their best interest, but because they provide higher fee/commissions for the agent
  - Ensure agent does not discriminate against clients

- Establish minimum **security** requirements and put in place a written **data privacy and security policy** that governs the gathering, processing, use, distribution and storage of client information to maintain its confidentiality, safety and integrity

**Table 3 - Suggestions for Risk Mitigation for top DFS Potential Risks**

Risk	#	Description of risk	Recommendations ( options and considerations)
A <b>Clients do not make informed decisions due to inadequate information from providers</b>	1	Clients are not adequately communicated with nor trained on: (i) Service understanding (e.g., how the service works, how to use it, how to register, how to opt-out), (ii) Trust in the service (e.g., reinforce client confidence in the service, security of data), (iii) Client service (e.g., where to complain/call if the service does not work, if the transaction did not go through, if the agent does not provide adequate service, etc.)	<ul style="list-style-type: none"> <li>Focus communication &amp; education on client understanding of and trust in the service and how the provider will support if things go wrong.</li> <li>Research/analyze clients' feedback before, during, and after designing and delivering a product. Also, analyze the data on an on-going basis.</li> <li>Continuously reinforce client communication/education and keep an open channel of communication and perform periodic client surveys, particularly to gauge client service comprehension.</li> <li>Improve education across providers (e.g., agent capacity building as they have a continuous interaction with clients).</li> </ul>
B <b>Inadequate or lack of client care channel/recourse mechanism (e.g., client support, client helpdesk, dispute resolution, and complaint mechanisms)</b>	2	Provider offers inadequate support, dispute resolution, and complaint mechanisms to clients. Thus, when issues occur: (i) clients do not know who to approach, (ii) these centers are not accessible, (iii) call centers/complaint line do not adequately deal with client queries and complaints, (iv) client's concerns are not addressed in a timely and fair manner.	<ul style="list-style-type: none"> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> <li>Clearly define which provider is ultimately responsible for resolving clients issues and the time those issues should be resolved.</li> </ul>
C <b>Data protection and security</b>	3	Client identity is stolen and may be used to open an account or perform transactions, which could lead to identity theft.	<ul style="list-style-type: none"> <li>Incorporate data security and encryption requirements into all DFS solutions. However, this could limit the possibility of using SMS technology for monetary transactions and USSD for transactions with higher amounts.</li> <li>Establish minimum security requirements for the mobile money provider.</li> <li>There is need to clearly identify who is financially liable to refund funds to the client if those are stolen.</li> </ul>



Risk	#	Description of risk	Recommendations ( options and considerations)
D <b>Data privacy</b>	4	Clients are not informed/misinformed on how their data and history is being used or shared. Hence: (i) client information could be inappropriately sold or tracked without client consent, (ii) client could start receiving abused/unauthorized advertising online and cross marketing.	<ul style="list-style-type: none"> <li>• There is still a debate on allowing clients to share data voluntarily or to opt-out from data tracking as a default.</li> <li>• The Federal Trade Commission's report, <i>Protecting client Privacy in an Era of rapid change</i>, urged providers to adopt three practices: (i) privacy by design, (ii) simplified choice for businesses and clients, and (iii) more transparency.</li> </ul>
E <b>Clients are defrauded and/or lose their funds</b>	5	When (i) Service presents faulty security that allows information to be stolen and misused, (ii) Clients share their PINs with another person, (iii) A non-client uses a friend or family member's account (more than one user of the service) to perform unauthorized transactions instead of the registered client	<ul style="list-style-type: none"> <li>• Improve/repeat client awareness and education, users should understand the importance of a PIN and not disclose it to any other user.</li> <li>• If clients suspect the agent of fraud, they should be able to contact the call center or any client care channels or go to the nearest provider shop and report the case for investigation.</li> <li>• Perform account monitoring and other controls supported by technology to evaluate transactions for strange behavior in order to reduce attractiveness of the service for criminal activity (monitoring systems could detect unusual patterns).</li> <li>• Regulate for security minimums.</li> <li>• Evaluate to set transaction limit to avoid ability to clean out an account in a period of time. However, this needs a study because limits on transactions may hinder repeat use of the service.</li> </ul>
	6	When the mobile money/branchless banking service has system downtime or some processes are manual, transactions performed by clients can be delayed, lost, or clients can even be victims of stolen payments.	<ul style="list-style-type: none"> <li>• Define clear recruitment, selection, and monitoring process for agents.</li> <li>• Improve and automate reconciliation process.</li> <li>• Users should receive an electronic confirmation once their transactions are performed.</li> <li>• Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>• Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> </ul>

Risk	#	Description of risk	Recommendations ( options and considerations)
	7	When an employee of the service provider commits fraud by manipulating data and transactions performed by clients	<ul style="list-style-type: none"> <li>Providers of the service can use data to monitor attempts of fraud and data manipulation on the systems</li> </ul>
F <b>Clients cannot access their funds or float</b>	8	Agents often have either cash or float when client is asking for other so they can't get their money (float and liquidity management issues)	<ul style="list-style-type: none"> <li>Improve float and liquidity management support such as improving procedures and repeating training, monitoring of float and liquidity of agents, tactics for managing liquidity of agents, and providing credit to agents.</li> </ul>
	9	Clients cannot redeem funds/perform transactions due agent's to lack of liquidity.	<ul style="list-style-type: none"> <li>Define clear recruitment, selection, and monitoring process for agents.</li> <li>Improve liquidity management procedures at agents.</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> </ul>
G <b>Insufficient transparency and disclosure of information</b>	10	Information on roles and responsibilities of the agent, product and service fees, prices, terms, conditions, mechanism to address client's complaints, and timeliness of updates/changes are not properly disclosed to client.	<ul style="list-style-type: none"> <li>Establish minimum disclosure and transparency requirements and frequency to the solution (mobile money, branchless banking service) provider.</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> </ul>
H <b>Unauthorized fees, abusive prices charged to clients</b>	11	Agents charge unauthorized fees or agent does not clearly disclose fees/prices to the client;	<ul style="list-style-type: none"> <li>Establish disclosure of fees as a required activity of the agent.</li> <li>Define clear recruitment, selection, and monitoring process for agents.</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels) where they can inform on these agents.</li> </ul>




Risk	#	Description of risk	Recommendations ( options and considerations)
	12	Clients are charged abusive prices due to market structure i.e., in non-competitive markets with a dominant player or a monopoly, the provider could abuse its position and charge abusive prices)	<ul style="list-style-type: none"> <li>Regulators will need to monitor markets structure and benchmark prices in similar markets</li> </ul>
I <b>Agent's inability leads to lack of service</b>	13	Clients cannot access the service because agent does not know how to perform the transaction.	<ul style="list-style-type: none"> <li>Reinforce agent training and monitoring.</li> <li>Inform and train client regarding available recourse mechanisms (e.g., call centers, complaint line) where they can report poor agent service.</li> <li>If any of these issues is related to receiver not being able to cash out money, then after a period of time funds should return to sender and sender should receive a notification.</li> </ul>
J <b>Agent's misconduct against clients</b>	14	Clients are treated unfairly due to inadequate incentive structure rewards to agent	<ul style="list-style-type: none"> <li>Review and set incentivizing commission structure.</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> </ul>
	15	Agents persuade clients to avail of particular transactions and services not because those are in their best interest but because they provide higher fee/commissions for agents;	<ul style="list-style-type: none"> <li>Review and set incentivizing commission structure.</li> <li>Define clear recruitment, selection, and monitoring process for agents.</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call centers, complaint line) where they can inform about these agents.</li> </ul>
	16	Female clients fear harassment from agents or are not served by agent	<ul style="list-style-type: none"> <li>Define clear recruitment, selection, and monitoring and termination process for agents.</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>Inform and educate client regarding recourse</li> </ul>

Risk	#	Description of risk	Recommendations ( options and considerations)
			mechanisms (e.g., call center, complaint line, and resort channels)
	17	Agent's discriminate against clients due to security concerns (e.g., agent working in high-risk neighborhoods can be target of thefts and robbery. This situation is aggravated when agents do not have any insurance provided by a bank, MNO, or provider; or are not self-insured;	<ul style="list-style-type: none"> <li>Evaluate/define mechanisms to provide insurance to agents against thefts; either paid by them, co-paid, or financed by the provider. Or inform agents on options to better secure their shops.</li> <li>Monitor agents and analyze cases of unfair treatment and no attention due to issues not related to security</li> </ul>
	18	Agent performs/accepts transactions with counterfeit cash by himself or colluding with a third-person. Also, agent provides this money to clients	<ul style="list-style-type: none"> <li>Train agents on illicit transactions such as counterfeit, consequences, and reporting mechanisms</li> <li>Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> <li>Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> </ul>




## 10. Annex A – Complete Risk Matrix for DFS

### a. Client Protection




#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
1	Clients	<b>Clients do not make informed decisions due to inadequate information from providers</b>	Clients are not adequately communicated with nor trained on: (i) Service understanding (e.g., how the service works, how to use it, how to register, how to opt-out), (ii) Trust in the service (e.g., reinforce client confidence in the service, security of data, there is a lack of client awareness, empowerment), (iii) Client service (e.g., where to complain/call if the service does not work, if the transaction did not go through, if the agent does not provide adequate service, etc.)	1. Appropriate product design and delivery, 3. Transparency, 7. Mechanism for complaint resolution	↑	<ul style="list-style-type: none"> <li>- Focus communication &amp; education on client understanding of and trust in the service and how the provider will support if things go wrong.</li> <li>- Research/analyze clients' feedback before, during, and after designing and delivering a product. Also, analyze the data on an on-going basis.</li> <li>- Continuously reinforce client communication/education and keep an open channel of communication and perform periodic client surveys, particularly to gauge client service comprehension.</li> <li>- Improve education across providers (e.g., agent capacity building as they have a continuous interaction with clients).</li> </ul>	<ul style="list-style-type: none"> <li>- Implementations lack adequate client education, communication, and marketing.</li> <li>- 'In Papua New Guinea, 47% of women and 35% of men who want a MFS account identified lack of understanding of how to use it as their chief reason for not opening an account.' (Source: GSMA and Visa, 2013)</li> <li>- The usual daily Tx's per day in Africa are 21-30 (e.g., Kenya 46, Uganda 30, Tanzania 31). (Source: Helix Institute, 2014)</li> </ul>	Operational, Reputational
2	Clients	<b>Inadequate or lack of client care channel/recourse mechanisms</b>	Provider offers inadequate support, dispute resolution, and complaint mechanisms to clients. Thus, when issues occur: (i) clients do not know who to approach, (ii) these centers are not accessible, (iii) call centers/complaint lines do not adequately deal with client queries and complaints, (iv) client's concerns are not addressed in a timely and fair manner.	1. Appropriate product design and delivery, 7. Mechanism for complaint resolution	↑	<ul style="list-style-type: none"> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> <li>- Clearly define which provider is ultimately responsible for resolving clients issues and the time those issues should be resolved.</li> </ul>	The size and level of client care channels/recourse mechanisms vary from sophisticated centers that can expedite client concerns to no client care channels at all. (Source: Accion's fieldwork experience)	Operational, Reputational
3	Clients	<b>Data protection and security</b>	Client identity is stolen and may be used to open an account or perform transactions, which could lead to identity theft.	6. Privacy of client data, 7. Mechanism for complaint resolution	↑	<ul style="list-style-type: none"> <li>- Incorporate data security and encryption requirements into all DFS solutions. However, this could limit the possibility of using SMS technology for monetary transactions and USSD for Tx's with higher amounts.</li> <li>- Establish minimum security requirements for the mobile money provider.</li> <li>- There is need to clearly identify who is financially liable to refund funds to the client if those are stolen.</li> </ul>	<ul style="list-style-type: none"> <li>- Target revealed in 2013 that up to 70 million credit and debit card information of clients was stolen in a data breach. Information swept was names, addresses and phone numbers along with credit card transactions. Target refunded its affected clients. (Source: The Washington Post, 2014)</li> <li>- More recently, Visa and Mastercard will face class-action lawsuits related to the development of their chip and PIN technology. (Source:</li> </ul>	Reputational, Financial

#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
4	Clients	<b>Data privacy</b>	Clients are not informed/misinformed on how their data and history is being used or shared. Hence: (i) client information could be inappropriately sold or tracked without client consent, (ii) client could start receiving abused/unauthorized advertising online and cross-marketing.	1. Appropriate product design and delivery, 3. Transparency, 5. Fair and respectful treatment of clients, 6. Privacy of client data, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- There is still a debate on allowing clients to share data voluntarily or to opt-out from data tracking as a default.</li> <li>- The Federal Trade Commission's report, <i>Protecting client Privacy in an Era of rapid change</i>, urged providers to adopt three practices: (i) privacy by design, (ii) simplified choice for businesses and clients, and (iii) more transparency.</li> </ul>	<ul style="list-style-type: none"> <li>- A study showed that 80% of mobile users desired privacy of their personal data (Source: CGAP, 2014)</li> <li>- As an example, in a case pitting privacy issues against a Google, European court says Google must respect 'right to be forgotten'. This could be the beginning of more sensitive rules on data privacy and protection (Source: Reuters, 2014)</li> </ul>	Reputational
5	Clients	<b>Clients are defrauded and/or lose their funds</b>	When: (i) Service presents faulty security that allows information to be stolen and misused, (ii) Clients share their PINs with another person, (iii) A non-client uses a friend or family member's account (more than one user of the service) to perform unauthorized transactions instead of the registered client.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 6. Privacy of data, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Improve/repeat client awareness and education, users should understand the importance of a PIN and not disclose it to any other user.</li> <li>- If clients suspect the agent of fraud, they should be able to contact the call center or any client care channels or go to the nearest provider shop and report the case for investigation.</li> <li>- Perform account monitoring and other controls supported by technology to evaluate Tx's for strange behavior in order to reduce attractiveness of the service for criminal activity (monitoring systems could detect unusual patterns).</li> <li>- Regulate for security minimums.</li> <li>- Evaluate to set Tx's limit to avoid ability to clean out an account in a period of time. However, this needs a study because limits on transactions may hinder repeat use of the service.</li> </ul>	<ul style="list-style-type: none"> <li>- A common fraud risk is vishing, smishing scams tricking clients to use their PINs (Source: GSMA).</li> <li>- In Tanzania, one in five registered users share their mobile money PIN with another person, one in seven carried out mobile money transactions with the help of an agent, and might have had to share their PINs with the agent. (Source: Intermedia, 2013).</li> <li>- In the use of Agents, 25% have used a friend or family member's account. (Source: Intermedia, 2013).</li> </ul>	Operational, Reputational
6	Clients	<b>Clients are defrauded and/or lose their funds</b>	When the mobile money/branchless banking service has system downtime or some processes are manual, transactions performed by clients can be delayed, lost, or clients can even be victims of stolen payments.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 6. Privacy of data, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Define clear recruitment, selection, and monitoring process for agents.</li> <li>- Improve and automate reconciliation process.</li> <li>- Users should receive an electronic confirmation once their transactions are performed.</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> </ul>	<ul style="list-style-type: none"> <li>Evidence shows this occurs in cases when there is a system downtime or manual reconciliation process for example provider does not perform reconciliation and agents do not report transactions simultaneously.</li> </ul>	Operational, Reputational




#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
7	Clients	<b>Clients are defrauded and/or lose their funds</b>	When an employee of the service provider commits fraud by manipulating data and txs performed by clients	1. Appropriate product design and delivery, 6. Privacy of data, 7. Mechanism for complaint resolution	↑	Providers of the service can use data to monitor attempts of fraud and data manipulation on the systems	<p>-In Pakistan, 19% of women and 10% of men who are not interested in opening an account agreed with the statement that it's not safe to give money to MFS agents. (Source: GSMA and Visa, 2013)</p> <p>-In one case attracting headlines in Kenya, a man stole more than US\$1,200 through fraudulent transactions on people's phones once he had been told their PINs (CGAP, Kiplagat 2010)</p>	Operational, Reputational
8	Clients	<b>Clients cannot access their funds or float</b>	Agents often have either cash or float when client is asking for other so they can't get their money (float and liquidity management issues)	1. Appropriate product design and delivery, 7. Mechanism for complaint resolution	↑	- Improve float and liquidity management support such as improving procedures and repeating training, monitoring of float and liquidity of agents, tactics for managing liquidity of agents, and providing credit to agents.	<p>- Especially in rural areas clients might be unable to withdraw the funds they receive electronically.</p> <p>-When Zain's ZAP first established an agent network in Kenya, it set a very low bar to be an agent (US\$60 in float and no need to be a licensed business). As a result, it quickly acquired a large agent network, but most agents did not have adequate capital and were looking to make short-term profits rather than committing to a long-term business development strategy. (Source: CGAP, 2011)</p>	Operational, Reputational
9	Clients	<b>Clients cannot access their funds or float</b>	Clients cannot redeem funds/perform transactions due agent's to lack of liquidity.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution	↑	<p>- Define clear recruitment, selection, and monitoring process for agents.</p> <p>- Improve liquidity management procedures at agents.</p> <p>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</p> <p>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</p>	Rapid growth and the non-exclusivity of agents is putting pressure on agents' liquidity, with five transactions a day being denied due to lack of float. Liquidity issues are being driven by non-exclusivity of agents (forcing agents to manage multiple liquidity pools) and agents' apathetic approach to float management (Source: Helix study in Tanzania, 2014).	Operational, Reputational
10	Clients	<b>Insufficient transparency and disclosure of information</b>	Information on roles and responsibilities of the agent, product and service fees, prices, terms, conditions, mechanism to address client's complaints, and timeliness of updates/changes are not properly disclosed to client.	3. Transparency, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution	↑	<p>- Establish minimum disclosure and transparency requirements and frequency to the solution (mobile money, branchless banking service) provider.</p> <p>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</p>	Regulators typically require mobile money, branchless banking service providers to meet certain disclosure and transparency requirements (e.g., Ghana, Philippines, India, Pakistan) (GSMA, 2013)	Operational, Reputational

#	Who is affected ?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
11	Clients	<b>Unauthorized fees, abusive prices charged to clients</b>	Agents charge unauthorized fees or agent does not clearly disclose fees/prices to the client.	1. Appropriate product design and delivery, 2. Prevention of over-indebtedness, 3. Transparency, 4. Responsible pricing 5. Fair and respectful treatment of clients		<ul style="list-style-type: none"> <li>- Establish disclosure of fees as a required activity of the agent.</li> <li>- Define clear recruitment, selection, and monitoring process for agents.</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels) where they can inform on these agents.</li> </ul>	There is prevalence of agents charging unauthorized fees. (Source: Research from MicroSave, InterMedia, CGAP)	Operational, Reputational
12	Clients	<b>Unauthorized fees, abusive prices charged to clients</b>	Clients are charged abusive prices due to market structure i.e., in non-competitive markets with a dominant player or a monopoly, the provider could abuse its position and charge abusive prices)	4. Responsible pricing		Regulators will need to monitor markets structure and benchmark prices in similar markets	Financial institutions are free to set fees, charges and interest rates. However, La Superintendencia de Banca (SBS) in Peru has legal authority to actively identify and curb/prohibit predatory or abusive practices and to impose sanctions on financial institutions. SBS, in the course of its supervisory process, evaluates the technical grounds on which the provider sets its prices and fees. Providers cannot unilaterally modify contracts and may change prices only after a 15-day notice so the customer is able to withdraw from the contract if he or she chooses. (Source: SBS and CGAP, 2010)	Systemic
13	Clients	<b>Agent's inability leads to lack of service</b>	Clients cannot access the service because agent does not know how to perform the transaction.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Reinforce agent training and monitoring.</li> <li>- Inform and train client regarding available recourse mechanisms (e.g., call centers, complaint line) where they can report poor agent service.</li> <li>- If any of these issues is related to receiver not being able to cash out money, then after a period of time funds should return to sender and sender should receive a notification.</li> </ul>	- In Papua New Guinea, 47% of women and 35% of men who want a mobile financial service account identified lack of understanding of how to use it as their chief reason for not opening an account. This gap suggests an opportunity to improve education across a provider's network, generally through investments in agent capacity-building. Well-trained agents are better equipped to reduce potential customers' anxiety and overcome women's risk aversion to try new tools. ' (Source: GSMA and Visa, 2013)	Operational, Reputational







#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
14	Clients	Agent's misconduct	Clients are treated unfairly due to inadequate incentive structure rewards to agent.	5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Review and set incentivizing commission structure.</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> </ul>	<p>- Clients in some markets report the service is not provided to them without any reason from the agent.</p> <p>- Also for example, Zain's ZAP in Tanzania pays agents only one-third of the US\$1 registration commission after customer verification. The remainder is paid when a customer makes five transactions in the six months after registering. (Source: CGAP, 2011)</p> <p>- One provider in Colombia is experimenting with a tiered system in which the commission per transaction varies depending on how many transactions are done. If agents do very few transactions (five or fewer) they are paid US\$0.08 per transaction. If they are active (more than 25 transactions a day), they are paid almost double, or US\$0.15 per transaction. (Source: CGAP, 2011)</p>	Operational, Reputational
15	Clients	Agent's misconduct	Agents persuade clients to avail of particular transactions and services not because those are in their best interest but because they provide higher fee/commissions for agents.	1. Appropriate product design and delivery, 2. Prevention of over-indebtedness, 4. Responsible pricing, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Review and set incentivizing commission structure.</li> <li>- Define clear recruitment, selection, and monitoring process for agents.</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call centers, complaint line) where they can inform about these agents.</li> </ul>	A chit fund (Ponzi scheme) passed through the Pilkhi village in the Nalanda District of Bihar in 2012, convincing individuals to invest in a particular product that would earn the agent higher commission. The agent fled overnight with hard-earned savings of many families that had believed was a life insurance product. Now families, and in particular women, are afraid to invest in the government-run JEEViKa program for them to open accounts and receive their remittances via an agent. (Source: CGAP, 2013)	Operational, Reputational
16	Clients	Agent's misconduct	Female clients fear harassment from agents or are not served by agent	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Define clear recruitment, selection, and monitoring and termination process for agents.</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels)</li> </ul>	Female clients in some markets report reluctance to provide their phone numbers to agents for fear of harassment.	Operational, Reputational





#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
17	Clients	Agent's misconduct	Agent's discriminate against clients due to security concerns (e.g., agent working in high-risk neighborhoods can be target of thefts and robbery. This situation is aggravated when agents do not have any insurance provided by a bank, MNO, or provider; or are not self-insured.	5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution	→	<ul style="list-style-type: none"> <li>- Evaluate/define mechanism to provide insurance to agents against thefts either paid by them, co-paid, or financed by the provider. Or inform agents on options to better secure their shops.</li> <li>- Monitor agents and analyze cases of unfair treatment and no attention due to issues not related to security</li> </ul>	Brazilian banks occasionally are willing to bear the cost of armored car services—usually when an agent is deemed to be playing an important role in reducing congestion at a nearby branch. Ninety-three percent of agents in Brazil say being an agent increases the risk of being robbed, and 25 percent have been robbed in the past three years. In fact, most Brazilian agents go to the bank to drop off extra cash even when the cash	Operational, Reputational
18	Clients, Agents, Service Providers	Agent's misconduct	Agent performs/accepts transactions with counterfeit cash by himself or colluding with a third person. Also, agent provides this money to clients	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution	→	<ul style="list-style-type: none"> <li>- Train agents on illicit transactions such as counterfeit, consequences, and reporting mechanisms</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> <li>- Monitor agent performance and define process for reinforcing training, warning of misconduct, and/or removing underperforming agents.</li> </ul>	In Brazil, 27% of agents have experienced worker theft (avg. loss approx. \$6K USD) and 16% have experienced client fraud, usually counterfeit bills (avg. loss \$189 USD) (Source: CGAP, 2010)	Systemic, Operational, Financial
19	Clients	Solvency	Client cannot redeem funds against electronic value due to insolvency or illiquidity of the service provider or the bank where the funds are held.	1. Appropriate product design and delivery	→	<ul style="list-style-type: none"> <li>- Regulate the diversification of e-float fund by safeguarding client funds in one or more banks or financial institutions.</li> <li>- Impose restrictions on the use of these safeguards by the providers so that funds are available when clients want to redeem them.</li> <li>- Isolate mobile money client's funds from the provider's funds and protect them from provider's creditors.</li> </ul>	<ul style="list-style-type: none"> <li>- There has not been a case of insolvency or illiquidity as the regulator usually requires for MNO led mobile money deployments to keep an equivalent amount of the funds at a bank.</li> <li>- Evidence suggests that mobile money represents a low systemic risk. For example in 2010 the accumulated balance of all mPesa represented just 0.2% of banks deposits by value, though total transactions represented approx. 70% of all electronic transactions in the country.</li> <li>- Prudential regulation and rules are applied for</li> </ul>	Systemic, Institutional
20	Clients	Solvency	Client loses money he/she has stored in the system due to failure of trustee where the funds are held	1. Appropriate product design and delivery	→	<ul style="list-style-type: none"> <li>- Evaluate and determine deposit insurance for mobile money client's funds;</li> <li>- Require diversification, client's funds should be deposited in several banks to avoid concentration in just one bank.</li> </ul>	<ul style="list-style-type: none"> <li>- There has not been a case of insolvency or illiquidity as the regulator imposes strict solvency policies to financial institutions</li> </ul>	Systemic, Institutional, Financial






#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)
21	Providers, Clients	<b>Low Client adoption</b>	Because product is not easy to use, appropriate, reliable, affordable, understandable, available, accessible, and there is lack of client awareness, empowerment, communication and educational activities.	1. Appropriate product design and delivery, 3. Transparency		<ul style="list-style-type: none"> <li>- Improve client experience, communications, education, and marketing.</li> <li>- Reinforce service design and delivery.</li> <li>- Improve service knowledge, use, and benefits.</li> </ul>	The usual daily Tx's per day in Africa are 21-30 (e.g., Kenya 46, Uganda 30, Tanzania 31). (Source: Helix Institute, 2014)
34	Clients	<b>Clients cannot establish a beneficiary of the account</b>	In case anything happens to the client (disability/death), no beneficiary will be able to access the funds left in the account	1. Appropriate product design and delivery, 3. Transparency, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Provide clear and adequate information to clients and ask them about opt-in/opt-out options to identify beneficiaries.</li> <li>- Define mechanisms to allow clients to identify/register beneficiaries (e.g., registration process, average balance in an account to define beneficiaries). Also, offer clients the opportunity to change the beneficiaries on as needed basis.</li> </ul>	There is no evidence in DFS but here is an example in commercial banking: 'After we receive notice of death or incompetence, we may freeze the account, refuse to accept transactions, and reverse or return deposits to the account. We are also not required to release funds in the account until we receive any documents we reasonably request to verify the death or incompetence, as well as who is entitled to the funds'. (Source: Chase Bank, 2014)
35	Clients, Agents, Service Providers	<b>Government raises taxes on digital financial services</b>	A government may decide to establish/raise taxes on digital financial services due to the high volumes of Tx's of these services or number of services provided in a country. It is highly probable that this tax will be passed onto clients	4. Responsible pricing		<ul style="list-style-type: none"> <li>- Assess the impact on the service with the implementation of taxes and a marginal cost to be transferred to clients</li> </ul>	Safaricom said in May 2013 that a 10 percent tax imposed in late 2012 on transfers using its M-Pesa mobile service had forced it to absorb costs of 400 million shillings (\$4.6 million) in the 2012/13 financial year to shield consumers from the full burden. According to a spokesperson, more than 28 shillings out of every 100 shillings charged to a telecoms customer went to the taxman, making Kenya's telecoms taxes amongst the highest in the world. (Source: Reuters, 2013)

## b. Quality of Service

Risks related to quality of service and others that have not been included among top risks to be mitigated through Smart Campaign Standards

#	Who is affected ?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
22	Clients	<b>Inability to access the service</b>	Potential client cannot register to the service due to: (i) Inability to show relevant identification IDs and/or verification documents required. This makes not only registration at the agent level difficult but also CDD/KYC process cumbersome; (ii) Not clear or flexible KYC/Client Due Diligence (CDD) process	1. Appropriate product design and delivery		- Provide flexibility in the list of acceptable identifications.  - Create Tiering Regulation; without tiering registration client identification program clients cannot even access to restricted basic services.	- There is no clarity/guidance among policy makers regarding KYC/CDD process.  '- Documents required in developing countries are more stringent than in developed countries (e.g., requirements of government/state ID, proof of address/nationality/employment/income, etc.).	Operational, Reputational
23	Clients	<b>Inability to access the service</b>	Clients cannot access service due to: (i) inability to prove identification IDs or client lost password, PIN, or SIM card; or (ii) malfunctioning/lost/stolen equipment at the agent (e.g., keypads, tablets, smartphones, POS).	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		In cases where receiver cannot cash out money after a period of time then funds should return to sender and sender should receive a notification.	- There is no clarity/guidance among policy makers regarding KYC/CDD process.  - Documents required in developing countries are more stringent that in developed countries (e.g., requirements of government/state ID, proof of address/nationality/employment/income, etc.)  - Some countries like Mexico and Uganda have gone through flexible KYC/CDD process.	Operational, Reputational
24	Clients	<b>Long registration time</b>	Client due diligence (CDD) requirements are complex (e.g., regulation requires clients to have a bank account in order to have a mobile money account).	1. Appropriate product design and delivery		- Design risk-based KYC procedures that allow simplified client Due Diligence (CDD) based on the specific risk that each product may offer.  - Simplify process for registering mobile money account (e.g., tier-up registration process by using information from SIM card registration and limiting amount for transactions).  - CDD and KYC rules could be simplified if there are other risk mitigation tools such as monitoring systems and transaction limits.	We have found for example that:  - India requires all clients to have a bank account in order to sign-up for the mobile money service.  - In Sri Lanka, the regulator required the same but after testing a service eZ Pay having only 15k clients after five years of launch, eased the rules creating an eWallet account linked to a bank account and an eWallet account that had to have equivalent funds in a Bank by the mobile money provider. As of June 2013, the service had 810k registered clients.  - In Guatemala, banking agents are only able to accept documents required to open account and to process a sig-up information. Agents cannot open accounts. This is different to Peru for example where clients can sign up anywhere in the country using a mobile phone.	Operational, Reputational
25	Clients	<b>Long client registration and activation time</b>	Agents are too slow and unable to process registration swiftly OR Once the client is able to access the service and registers his/her information, his/her activation time is not known and in many cases out of control for agents.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		- Reinforce training of agents.  - Evaluate the possibility of automatic activation of account based on the specific risk that each product offers.  - Inform and educate client regarding recourse mechanisms (e.g, call center, complaint line, and resort channels) where they can inform about these agents.	For example in Tanzania, 1/3 of agents report clients can register and use the service immediately. If the service takes more than 2 days, it is likely the client will never become active (Source: Helix Institute, 2013).	Operational, Reputational

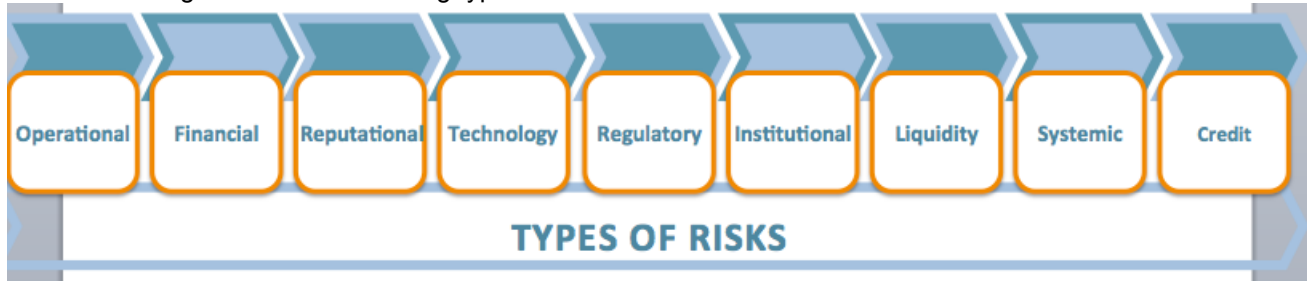
#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
26	Clients	<b>Lack of service</b>	Service downtime or unreliable service and in some cases information is lost or transaction is lost.	1. Appropriate product design and delivery, 5. Fair and respectful treatment of clients, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Establish and monitor minimum uptime service requirements to the mobile money provider.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> </ul>	According to a survey in Tanzania, 82% of agents from 2065 agents report having experienced downtime in the past (Source: Helix Institute, 2013)	Operational, Technology, Reputational
27	Clients	<b>Agent is not accessible or close by, or service not available at the agent</b>	This usually occurs in rural areas and in many cases agents work with MNOs and Financial Institutions with high market share and/or serving specific regions.	1. Appropriate product design and delivery		Build an adequate agent network, grow the network especially in areas where person-to-person transactions. A successful agent network depends on the availability of agents.	<p>-A successful case of scale of agents is mPesa Kenya.</p> <p>-Also, in Tanzania, 24% of women relative to 16% of men wanting a mobile money account cite “agents are far away” as their main reason for not trialling the service (Source: GSMA and Visa, 2013)</p> <p>-As well, In one sub-Saharan African country, a GSMA team undertaking focus groups heard customers express that there weren’t enough agents – and yet many of these customers were seated within 100 meters of an agent (Source: GSMA and Visa, 2013)</p>	Operational, Reputational
28	Clients	<b>Services are not provided in a homogeneous way by agents</b>	Not all agents provide the same service, some may just onboard clients, others may just perform transactions (e.g., cash in, cash out, bill payment, etc.), while other agents provide all services. This may cause confusion in clients.	1. Appropriate product design and delivery, 3. Transparency		Establish minimum disclosure and transparency requirements to the mobile money provider.	In Brazil for example, banks have authorized only 19% of correspondents to open new account. As of 2014 Brazil has around 400k non-banking correspondents or banking agents (Source: BFA, 2014).	Operational, Reputational
29	Clients	<b>Inability to perform reversals or transaction issues</b>	If money is sent to the wrong number, a cash reversal needs to be provided by either the agent or the provider (i.e., via client care channel). In some cases agent does not know how to or cannot do reversals and calls client center.	1. Appropriate product design and delivery, 3. Transparency, 7. Mechanism for complaint resolution		<ul style="list-style-type: none"> <li>- Clearly define who performs cash reversals and provide prompt service to clients.</li> <li>- Inform and educate client regarding recourse mechanisms (e.g., call center, complaint line, and resort channels).</li> </ul>	-Regarding potential chargebacks, there should be clarity about the grounds on which users can seek reversal of a transaction (e.g., identity theft, nonreceipt of money or goods, billing errors), any user fault standards that apply (e.g., consumer due care requirements, or delays in notification of error or theft), and the burdens of investigation and proof on the acquiring bank and the retail outlet. (Source: CGAP 2008)	Operational, Reputational

#	Who is affected?	Risk	Description of risk	Maps to Smart Campaign Principle	Potential Impact of Risk on Client	Recommendations (options and considerations)	Evidence (example and statistics)	Type of risk
30	Clients	<b>Lack of interoperable services</b>	Described in three ways: - Mobile money platform: client cannot transfer money across mobile money platforms. (wallet to wallet). This could include connections to switches, financial institutions, and companies. Conversely, it is very costly to send across platforms that do allow this service. - Distribution network: which could allow Tx to be conducted across multiple distribution networks, or electronic retail payments - SIM card or client level: this could allow a client of one MNO to use the mobile money services of any other MNO, bank, or third party	1. Appropriate product design and delivery		- There is a need for providers and policy makers to design and work together towards an interoperable environment.  - Explore open-architecture policies and interoperability within and across services.	Some countries are working on paving the way to interoperability (e.g., Mexico, Peru), with other cases being mVisa Rwanda and Selcom in Tanzania.	Operational
31	Clients, Agents	<b>Unclear AML/CFT obligations</b>	There is uncertainty about AML/CFT, licensing and regulations to agents. Moreover, there is no clarity or standards of up to what extent agents need to be regulated considering agents are not account providers.	1. Appropriate product design and delivery, 3. Transparency		- Promote risk-based KYC procedures.  - Duties should be clearly specified under the agreement between agent and mobile service provider, this will help to clearly delineate AML duties.	In Kenya, MNOs and providers of the service do not assume liability for its agents. In contrast to Peru, Colombia, Philippines, and Brazil.  There have been no cases of ML/FT through mobile money services in countries that have reached scale.	Systemic, Financial
32	Clients, Agents, Service Providers	<b>Money laundering (ML) and financing terrorism (FT)</b>	ML/FT can be perpetrated by client, agents and service providers.	1. Appropriate product design and delivery		- Implement transaction limits (i.e., limit on the number of accounts a client can hold, frequency of Tx, volume of Tx, amount that can be transferred in a certain period of time).  - Include monitoring of transactions flows.	Mobile money presents less risk than cash as transactions can be monitored and traced.	Systemic, Financial
33	Clients, Agents, Service Providers	<b>Poor oversight of providers</b>	Lack of supervision/regulation of new providers of DFS and oversight loopholes for new/existing providers of DFS. Also -in the absence of adequate regulation- there could be confusion on the responsibility among parties involved in the service.	1. Appropriate product design and delivery, 3. Transparency		Make the provider liable for both the actions that an agent or third party executes on its behalf. This will help guarantee that the provider will take care in the selection, monitor and control of the third-party providers it is working with.	There are some initiatives from a regulator-provider regulation (Philippines, Malaysia). Provision of AML/CFT training (South Africa)  In Kenya, MNOs and providers of the service do not assume liability for its agents. In contrast to Peru, Colombia, Philippines, Brazil	Systemic
36	Agents	<b>Lack of insurance and protection of agents in case of theft/robbery</b>	Agents -due to the Tx performed and amount of cash handled- can be target of thefts and robbery. This situation is aggravated when agents do not have any insurance provided by a bank, MNO, or provider; or are not self-insured.	1. Appropriate product design and delivery		- Clearly define mechanisms to provide insurance to agents either paid by them, co-paid, or financed by the provider	Brazilian banks occasionally are willing to bear the cost of armored car services—usually when an agent is deemed to be playing an important role in reducing congestion at a nearby branch. Ninety-three percent of agents in Brazil say being an agent increases the risk of being robbed, and 25 percent have been robbed in the past three	Operational

## 11. Annex B

### a. Type of risk

Risks can be categorized in the following types of risks:



- Operational<sup>2</sup>: Risk of direct or indirect loss from failed/inadequate processes, people or systems
- Financial: The probability of loss due to financing methods which may impair that ability to provide adequate and estimated returns
- Reputational: Risk to market value arising from negative public or other stakeholder opinions as a results of business practices, products, and services
- Technology: Any risk related to information and communication technologies
- Regulatory: Risk of failing to comply with regulations and rules
- Institutional: Risks that assumptions regarding institutional performance are incorrect due to market/institutional failure
- Liquidity: Risk of a client not being able to obtain funds in a reasonable time/cost to ensure financial commitments are met
- Systemic: Risk of collapse of an entire financial system or market
- Credit: Risk that involves a borrower will default on any type of debt/obligation by failing to make agreed payments

### b. Terminology

- CPPs: Client Protection Principles: seven principles put forth by the Smart Campaign to highlight client protection needs
- AML/CFT: Anti-Money-Laundering and Combating the Financing of Terrorism
- Branchless banking: an alternative delivery channel that allows MFIs to offer customers financial services beyond the frontiers of brick and mortar branches by using mobile phones of non-bank retail agents. It incorporates technology channels such as cards, POS (point of sale), and ATMs
- CICO: cash-in and cash-out transactions
- DFS: Digital financial services is the mix of mobile financial services and branchless banking
  - Mobile Financial Services refer to bank and non-bank provided financial services such as mobile payments, mobile money, mobile wallets, and mobile banking
  - Branchless Banking is the delivery of financial services outside conventional branches by using technology channels such as cards, POS, ATMs, and mobile phones
- KYC: Know Your Customer refers to the process used by a business to verify the identity of clients. Also refers to bank regulation, which governs such activities. KYC policies are becoming increasingly important globally to prevent identity theft, financial fraud, money laundering and terrorist financing.
- CDD process: Customer Due Diligence Process, which requires the bank to obtain information to verify the customer's identity and assess the risk. If the CDD inquiry leads to a high-risk determination, the bank has to conduct an Enhanced Due Diligence ("EDD").
- Loan Disbursement: The distribution of funds acquired through receipt of a loan contract
- MNO: Mobile network operator

<sup>2</sup> Adapted from Digital Financial Services Risk Assessment for Microfinance Institutions Pocket Guide, September 2014. [https://lextonblog.files.wordpress.com/2014/09/dfs\\_risk\\_guide\\_sept\\_2014\\_final.pdf](https://lextonblog.files.wordpress.com/2014/09/dfs_risk_guide_sept_2014_final.pdf)

- *Payment Types*
  - B2G Transfers: Business-to-government payment
  - B2P Transfers: Business-to-person payment
  - G2P Transfers: Government-to-person payment
  - P2P Transfers: Person-to-person payment
- Savings: Income retained; deferred consumption.
- Top-up: To replenish credit as to a mobile SIM card
- SMS: Short message service sent between mobile devices. Also known as text message.
- USSD: is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD stands for Unstructured Supplementary Services Data
- CFT: Combating the financing of terrorism
- Tx: Transactions.
- MFS: Mobile financial services.

## 12. Annex C – The Client Protection Principles and Standards

1	-	<b>Client Protection Principle 1: Appropriate Product Design and Delivery Channels</b>
1	1	The FI designs products that are appropriate to client needs and do no harm
1	2	The FI seeks client feedback for product design and delivery
1	3	The FI does not use aggressive sales techniques
2	-	<b>Client Protection Principle 2: Prevention of Over-indebtedness</b>
2	1	The FI conducts appropriate client repayment capacity analysis before disbursing a loan
2	2	The FI incentivizes quality loans
2	3	The FI uses credit bureau and competitor data, as feasible in local context
2	4	The FI Management and Board is aware of and concerned about the risk of over-indebtedness
2	5	The FI's internal audit department monitors that policies to prevent over-indebtedness are applied
2	6	The FI avoids dangerous commercial practices (i.e., avoids combining loan products to meet the same need, or restricting the loan use; sets prudent limits to allow for the renewal of a loan in case of early repayment; sets guidelines for appropriate rescheduling policies)
3	-	<b>Client Protection Principle 3: Transparency</b>
3	1	The FI fully discloses cost and non-cost information
3	2	The FI communicates proactively with clients in a way that clients can easily understand
3	3	The FI uses a variety of disclosure mechanisms
3	4	The FI leaves adequate time for client review and discloses at multiple times
3	5	The FI provides accurate and timely account information
4	-	<b>Client Protection Principle 4: Responsible Pricing</b>
4	1	The FI offers market-based, non-discriminatory pricing
4	2	The FI's efficiency is in line with its peers
4	3	The FI does not charge excessive fees
5	-	<b>Client Protection Principle 5: Fair and Respectful Treatment of Clients</b>
5	1	The FI culture raises awareness and concern about fair and responsible treatment of clients
5	2	The FI has defined in specific detail what it considers to be appropriate debt collection practices
5	3	The FI's HR policies (recruitment, training) are aligned around fair and responsible treatment of clients
5	4	The FI implements policies to promote ethics and prevent fraud
5	5	In selection and treatment of clients, the FI does not discriminate inappropriately against certain categories of clients
5	6	In-house and 3rd party collections staff are expected to follow the same practices as the FI staff
5	7	The FI informs clients of their rights
6	-	<b>Client Protection Principle 6: Privacy of Client Data</b>
6	1	The FI has a privacy policy and appropriate technology systems
6	2	The FI informs clients about when and how their data is shared and gets their consent



7 - Client Protection Principle 7: Mechanisms for Complaints Resolution	
7 1	The FI's clients are aware of how to submit complaints
7 2	The FI's staff is trained to handle complaints
7 3	The FI's complaints resolution system is active and effective
7 4	The FI uses client feedback to improve practices and products

### 13. Annex D – About the Authors

#### a. Smart Campaign

In response to a strongly recognized need to assure safe and responsible treatment of their clients, microfinance industry leaders from around the world came together in 2008 to agree on a set of Client Protection Principles to guide the microfinance industry. They recognized that when financial services are delivered in accord with the principles, clients are enabled to use financial services well and providers build a foundation for healthy operation for years to come. Launched in October 2009, the Smart Campaign was created to put the principles into action. Engaging the entire microfinance industry, the Smart Campaign has become a global movement to embed client protection into the DNA of the microfinance industry and the broader financial inclusion space. The Smart Campaign works with microfinance leaders from around the world on a common goal: to keep clients as the driving force of the industry by providing microfinance institutions with the tools and resources they need to deliver transparent, respectful, and prudent financial services to all clients. The Smart Campaign believes that protecting clients is not only the *right* thing to do, its the *smart* thing to do.

Today, the Smart Campaign is truly a global effort with a wealth of tools and resources and an ambitious action agenda. It is changing the way microfinance institutions protect their clients. Industry uptake has been overwhelmingly positive: it has garnered over 4,000 endorsers from 139 countries, including over 1,200 MFIs. At present, 15 MFIs have achieved Client Protection Certification, reaching close to 5 million clients. These institutions have met rigorous criteria for their treatment of clients, as verified by third party certifiers. The Campaign is now recognized as the go-to place for client protection, which gives it both enormous opportunity and enormous responsibility to carry its work forward.

#### a. Accion Channels and Technology

The Accion Channels and Technology (C&T) team is responsible for supporting microfinance institutions and banks in implementing and managing their digital financial service channels. C&T additionally provides advisory services to FinTech companies that offer solutions which can allow for a more efficient delivery of financial services. The expertise of C&T ranges from strategy development and planning to project management and implementation of technological and channel innovations. The team has hands-on experience increasing consumer adoption of digital financial services and enhancing its implementation. Accion has worked closely with its partners in Africa, Asia, and Latin America implementing channels such as ATM's, minibranches, mobile banking, and agent networks, and advised and supported these institutions during the stages of strategy planning, defining objectives, market research, development, testing, and launching, as well as training management and field staff. The Accion C&T Team has led in-depth demand-side projects to understand constraints to adoption and usage of a variety of technology-enabled products.

## 14. References

References used for this research are shown below:

1. <http://www.ifc.org/wps/wcm/connect/9d8d820042366e5582e1ae0dc33b630b/7.4+USAID+MFS+Risk+Matrix.pdf?MOD=AJPERES>
2. [http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/GSMA-mWomen-Visa\\_Unlocking-the-Potential\\_Feb-2013.pdf](http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/GSMA-mWomen-Visa_Unlocking-the-Potential_Feb-2013.pdf)
3. [http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/Oada1026-79fe-11e3-8963-b4b654bcc9b2\\_story.html](http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/Oada1026-79fe-11e3-8963-b4b654bcc9b2_story.html)
4. <http://paymentweek.com/2014-8-22-mastercard-visa-face-class-action-suit-target-breach-5420/>
5. [http://www.intermedia.org/wp-content/uploads/FITS\\_Tanzania\\_FullReport\\_final.pdf](http://www.intermedia.org/wp-content/uploads/FITS_Tanzania_FullReport_final.pdf)
6. <http://www.cgap.org/blog/do-mobile-money-clients-need-more-protection>
7. <http://www.reuters.com/article/2014/05/13/us-eu-google-dataprotection-idUSBREA4C07120140513>
8. <http://www.cgap.org/sites/default/files/CGAP-Technical-Guide-Agent-Management-Toolkit-Building-a-Viable-Network-of-Branchless-Banking-Agents-Feb-2011.pdf>
9. <http://www.cgap.org/blog/will-bank-run-away-women-and-mobile-banking-bihar-india>
10. <http://bankablefrontier.com/wp-content/uploads/documents/1.-Do-Banking-Correspondents-Improve-Financial-Inclusion-Evidence-from-Brazil.docx.pdf>
11. <https://www.cgap.org/sites/default/files/CGAP-Focus-Note-Being-Able-to-Make-Small-Deposits-and-Payments-Anywhere-Apr-2008.pdf>
12. [http://haiti.ciesin.columbia.edu/haiti\\_files/documents/Mobile%20Banking%20in%20Port-a-Piment%20Haiti-1.pdf](http://haiti.ciesin.columbia.edu/haiti_files/documents/Mobile%20Banking%20in%20Port-a-Piment%20Haiti-1.pdf)
13. [https://www.chase.com/online/private\\_client/document/CPC\\_branded\\_Deposit\\_Account\\_Agreement\\_102112.pdf](https://www.chase.com/online/private_client/document/CPC_branded_Deposit_Account_Agreement_102112.pdf)
14. <http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Chapter-4.pdf>
15. <http://www.slideshare.net/CGAP/branchless-banking-agents-in-brazil-building-viable-networks-2010>
16. <http://www.cgap.org/sites/default/files/CGAP-Financial-Inclusion-and-Consumer-Protection-in-Peru-Feb-2010.pdf>
17. <http://helix-institute.com/data-and-insights/agent-network-survey-tanzania-country-report-2013>
18. <http://www.reuters.com/article/2013/09/12/kenya-safaricom-idUSL5N0H808320130912>
19. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix1007231.pdf>
20. <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf>