BETTER THAN CASH ALLIANCE

GUIDELINES & BACKGROUND INFORMATION

JULY 2016

Responsible Digital Payments **Guidelines**

RESPONSIBLE DIGITAL PAYMENTS GUIDELINES

Cover Photo: © The Coca-Cola Company

Please note that slight edits were made in June 2017 to the original document.

For clients to adopt and use digital payments, they need to be treated fairly and feel protected from risks such as loss of privacy, exposure to fraud, and unauthorized fees. Therefore service providers should proactively take steps to protect their clients and that regulators should ensure a sound consumer protection regulatory framework. This is particularly important for financially excluded and underserved clients – especially women and those with low financial and technological capability who are participating in a world of rapid innovation involving new types of financial services, providers, partnerships, and distribution channels. In an inclusive digital payments ecosystem, it is important for all the stakeholders to do their part to ensure that digital payments are made responsibly.

The Better Than Cash Alliance Responsible Digital Payments Guidelines identify eight good practices for engaging with clients who are sending or receiving digital payments and who have previously been financially excluded or underserved.

The Guidelines are primarily oriented toward financial services providers in designing and delivering their payments services.
The Guidelines can also be used as a helpful checklist (subject to applicable law) for:

- Regulators in considering their rules;
- Private sector (for example, fast-moving goods or transport companies) in selecting payment providers;
- Donors and development organizations in procuring services from payment providers; and
- All stakeholders in advocating for appropriate consumer protection.

The focus of the Guidelines is on the common types of digital payments services provided to the financially underserved such as electronic money transaction accounts. The Guidelines are technology and provider neutral. They are designed to apply to current innovations in the field of digital payments, although it is recognized they may need to be reviewed and updated from time to time. Each Guideline includes examples of what a client might expect in a responsible digital payments market.

Since its launch in 2012, the Better Than Cash Alliance has engaged with stakeholders in many forums to work towards digital payments that are provided responsibly and for the benefit of both the recipient and sender. These Guidelines represent the culmination of several years of consultations with industry stakeholders, many of which occurred at a series of global meetings. These meetings included the 2013 2020 Global Financial Inclusion Forum and the Responsible Finance Forum's global deliberations on digital finance in 2014 and 2015 and its regional meeting in 2016, which were held in conjunction with meetings of the G20's Global Partnership for Financial Inclusion, at the G20's request. This builds off post-financial crisis recognition of the importance of responsible practices in financial inclusion, viz G20 Principles for Innovative Financial Inclusion (2010).

Other guidance comes from the principles, standards, and codes discussed in the 2015 *Better Than Cash Alliance Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services*[1] as well as from other recent international research and reports.[2] These Guidelines have been shared broadly in draft form for comment, and the resulting comments and feedback have been incorporated into this public document.

The Guidelines' aim is to provide a helpful tool for all stakeholders supporting responsible practices in the move from cash to digital payments in order to reduce poverty, drive inclusive growth, and contribute to greater economic participation of women.

Guidelines

1 Treat Clients Fairly

Clients need to be treated fairly if they are to trust digital payments, especially those clients with low levels of financial and technological capability.

2 Keep Client Funds Safe

Clients, especially the financially excluded or underserved, need reliable and secure access to funds in digital transaction accounts.

3 Ensure Product Transparency for Clients

Providing clients with transparent product information requires special attention in a digital environment, especially where information is only available electronically, such as on a mobile phone.

4 Design for Client Needs and Capability

Designing digital payments to address the needs, economic roles, and capabilities of clients, especially women, will increase suitability and use.

5 Support Client Access and Use Through Interoperability

While recognizing the need to balance competition and innovation, ensuring the interoperability of platforms, agents, and clients is highly desirable so customers of different schemes can make payments to each other and agents can work for different providers. This is especially important for clients living in remote rural areas.

6 Take Responsibility for Providers of Client Services Across the Value Chain

Clients are more likely to trust and use digital payments if providers take responsibility for the actions of agents, employees, and third party service providers across the value chain.

7 Protect Client Data

Protecting clients' digital data is increasingly important given the volume, velocity, and variety of data being used for marketing and credit scoring, while recognizing that use of client data can increase the range of products a client can access.

8 Provide Client Recourse

Clients need access to a fair recourse system for dealing with complaints about digital payments. This is especially necessary for complaints about innovative and unfamiliar products delivered via new channels and for clients who live remotely and may have little to no direct contact with providers.

1 Treat Clients Fairly

"We want our clients, who are mostly unbanked and new to digital payments, to feel that they are being respected and treated fairly and served with special care by our agents and service points."

MR. DASGUPTA ASIM KUMAR
ADVISOR, REGULATORY RELATIONS
BKASH LIMITED

Clients need to be treated fairly if they are to trust digital payments, especially those clients with low levels of financial and technological capability.

EXAMPLES OF TREATING DIGITAL PAYMENTS CLIENTS FAIRLY INCLUDE:

1. All **advertising and other sales information** is communicated using language and terms that are simple, clear, accurate, and not misleading.
2. Product terms provide a **reasonable balance between client and provider interests**.
3. **Clients are treated respectfully**, for example by only being sold digital products that they are really in need of.
4. **Identification requirements** are appropriate for clients so as to facilitate access.
5. Clients are treated equally so there is **no unfair discrimination**. For example, providers do not discriminate on the basis of gender, religion, ethnicity, politics, sexual orientation, age, residence, or a disability.
6. In the case of **lost or stolen access devices**, security credentials, or identity, providers compensate a client for any transaction that occurs after the client has reported the loss or theft to the provider. Compensation is also payable to the extent a transaction is above a daily or periodic limit.
7. A client is compensated for any late payment fee payable if inability to make a payment was because of a scheduled **system outage** that the client was not told of.
8. If a client initiates a digital payment in a **power outage**, the provider processes it as soon as possible.

2 Keep Client Funds Safe

"Because building trust in digital payments is crucial in driving effective adoption, appropriate and proportionate regulatory frameworks need to be in place to ensure that client funds are protected at all times."

MS. PIA ROMAN TAYAG
HEAD, INCLUSIVE FINANCE ADVOCACY
BANGKO NG PILIPINAS

Clients, especially the financially excluded or underserved, need reliable and secure access to funds in digital transaction accounts.

EXAMPLES OF SAFEGUARDING CLIENT FUNDS HELD IN DIGITAL TRANSACTION ACCOUNTS INCLUDE:

1. **Matching Funds:** For providers who are not subjected to prudential regulation, they hold in separate account(s) in prudentially regulated institutions unencumbered funds that equal, in full, all outstanding balances. Alternatively, matching funds could be invested in other permissible securities (such as government securities with an active secondary market). Ideally, accounts and investments are held for the benefit of clients (such as in a trust account). Matching funds are only used to make payments to clients and not for operational purposes. Matching funds are also protected from claims made by the provider's third party creditors. Supervisors can access account and investment records on a real-time basis, where this is feasible.
2. **System Capacity and Security:** Robust steps are taken to ensure reliable network and system capacity as well as a payments network and delivery channel that is secure from fraud, hacking, and any other form of unauthorized use.
3. **Fraud:** A client is compensated by the provider for any direct loss due to fraud by agents, employees, and third party service providers (such as their agent network managers) and for third party fraud caused by a reasonably preventable security breach. Clients are also informed promptly of any suspected fraud.
4. **Mistaken and Unauthorized Transactions:** The user interface is designed to be clear, simple, and secure. It also requires confirmation of payment details before a transaction is completed. The aim is to minimize the risk of mistaken and unauthorized transactions, as well as to facilitate easy access.

3 Ensure Product Transparency for Clients

"Anything worth providing is worth providing transparently. This is all the more important for people who may be making and receiving payments digitally for the first time. It is incumbent on providers to give people the full and clear information they need to make decisions that are right for them."

DR. BITANGE NDEMO
ASSOCIATE PROFESSOR, UNIVERSITY OF NAIROBI'S BUSINESS SCHOOL. FORMER PERMANENT SECRETARY, MINISTRY OF INFORMATION AND COMMUNICATION KENYA

Providing clients with transparent product information needs special attention in a digital environment, especially where information is only available electronically, such as on a mobile phone.

EXAMPLES OF ENHANCING PRODUCT TRANSPARENCY IN A DIGITAL ENVIRONMENT INCLUDE:

1. **Product Information:** Each client is given access (which may be in digital form) to a clear, simple, and readily comparable statement of product features, terms, fees, and any interest payable. This is done before the payments service is provided. The information is kept updated and is in a form that the client can keep and/or access, including digitally. The provider also explains the information to the client on request or if it appears that they cannot understand it (for example, if it is in a language they do not understand).
2. **Transaction and Account Records:** A client receives proof of each transaction and has easy access to clear and simple transaction and account records. These records could be digitally provided. They also need to be in a form the client can keep or access, such as a digital transaction history.

4 Design for Client Needs and Capability

"The experience of BIM's clients is that they find our product intuitive, easy to use, and transparent. This is because we designed BIM for clients' needs and capabilities."

DR. CAROLINA TRIVELLI
MANAGING DIRECTOR
PAGOS DIGITALES PERUANOS

Designing digital payments to address the needs, economic roles, and capabilities of clients, especially women, will increase suitability and use.

EXAMPLES OF ACTIONS RELEVANT TO THE DESIGN OF DIGITAL PAYMENTS SERVICES INCLUDE:

1. **Payment Service Design:** Digital payment services are designed on the basis of research as to clients' needs, preferences, and behavior. Their design also takes account of clients' likely financial and technological capability levels and, particularly in the case of underserved markets, is simple and clear. Given women's greater exclusion, it is particularly important that payment services be designed to meet women's needs and capabilities and economic roles.
2. **User Support:** Each client of a digital payments service is given:
   - **(a)** Easily understood instructions on how to use the service and safeguard their security credentials (such as passwords and PINs) in addition to an outline of related client responsibilities;
   - **(b)** Contact details for a 24-hour hotline to notify the provider about a lost or stolen access device or related security credentials, a mistaken or unauthorized transaction, or a security breach;
   - **(c)** Contact details for reaching the provider during local business hours so clients have a reliable source of information about how to use a digital financial service and its features; and
   - **(d)** Additional support to first-time users, particularly women, as needed and feasible, to support safe uptake and use.

5 Support Client Access and Use Through Interoperability

"The regulator has a role to engender interoperable payment systems to help reduce clients transaction cost and enhance convenience."

DR. SETTOR AMEDIKU
HEAD OF FINANCIAL STABILITY DEPARTMENT
BANK OF GHANA

While recognizing the need to balance competition and innovation, ensuring the interoperability of platforms, agents, and clients is highly desirable so clients of different schemes can make payments to each other and agents can work for different providers. This is especially important for clients living in remote rural areas.

EXAMPLES OF FACILITATING INTEROPERABILITY INCLUDE:

1. Encourage collaborative and industry-led interoperability initiatives to ensure that clients can make digital financial transactions regardless of where they live or who their provider is.
2. Discourage any deliberate barriers to interoperability (such as exclusive agent arrangements).

6 Take Responsibility for Providers of Client Services Across the Value Chain

"We can only earn the trust of clients if we as service providers ensure that all those in our value chain are acting responsibly–and that we have the systems and processes to ensure that happens. This is the message that needs to be given to clients–particularly those using digital payments for the first time."

MR. RAJPAL DUGGAL
OXIGEN SERVICES INDIA

Clients are more likely to trust and use digital payments if the provider takes responsibility for the actions of agents, employees, and third party service providers across the value chain.

EXAMPLES OF SHOWING RESPONSIBILITY FOR AGENTS, EMPLOYEES, AND THIRD PARTY SERVICE PROVIDERS INCLUDE:

1. **Liability:** Providers take responsibility for the acts and omissions of their agents, employees, and third party service providers.
2. **Training and Oversight:** Agents and employees, and those of third party service providers, are appropriately trained and monitored, including on product features, regulatory responsibilities, and gender-sensitive conduct. They also have the resources to competently and lawfully provide payments services.
3. **Provider Details:** Agents tell clients the name and contact details of the provider when an account is opened and on request.

7 Protect Client Data

"Along with the increases in financial inclusion, it is increasingly vital to secure the massive data that are handled by various inclusive finance providers."

DR. TAO SUN
SENIOR DIRECTOR
ANT FINANCIAL

Protecting clients' digital data is increasingly important given the volume, velocity, and variety of data being used for marketing and credit scoring, while recognizing that use of client data can increase the range of products a client can access.

EXAMPLES OF HOW CLIENT PERSONAL DATA MIGHT BE PROTECTED IN A DIGITAL ENVIRONMENT AT A BASIC LEVEL INCLUDE:

1. **Confidentiality and Security:** Reasonable measures are taken to ensure the confidentiality and security of client data relevant to digital payments. Examples of such data include identification and contract information; transaction histories; security credentials; device, mobile phone, and Internet usage data; and geolocation data. With the express and informed consent by clients, data can be used and disclosed for specific purposes, such as to market new services.
2. **Audit Trail:** A clear audit trail of transaction records is accessible to clients and supervisors.

8 Provide Client Recourse

"Mexico's experience is that effective recourse mechanisms that function in a digital environment are critical to building clients' trust in using financial services."

MS. MARÍA FERNANDA TRIGO
GENERAL DIRECTOR FOR ACCESS
TO FINANCIAL SERVICES
THE NATIONAL BANKING AND
SECURITIES COMMISSION
MEXICO

Clients need access to a fair recourse system for dealing with complaints about digital payments. This is especially necessary for complaints about innovative and unfamiliar products delivered via new channels and for clients who live remotely and may have little to no direct contact with providers.

EXAMPLES OF EFFECTIVE RECOURSE SYSTEMS FOR DIGITAL PAYMENTS CLIENTS INCLUDE:

1. **Complaints:** Clients can easily access a transparent, free or low-cost, and efficient complaints system. Such a system should be accessible to all, regardless of cultural norms, language, mobility, etc. The system is accessible by phone or digitally (such as via a website or by text message), or by visiting the provider's place of business.
2. **Disputes:** Clients also have access to an independent third party who handles disputes with providers in cases where the client's complaint has not been adequately addressed and resolved by the provider. This third party system is easily accessible (including by phone or digitally), transparent, free or low-cost, and efficient.
3. **Information about Recourse Systems:** Information about a provider's recourse system is set out in terms and conditions that are available on the provider's website and at the premises of both the provider and the agent. In addition, once a client makes a complaint they receive a copy of this information, which may be in digital form.
4. **Complaints Data:** Providers maintain records of client complaints and their response to each complaint. Regulators are also given periodic reports of complaints data. Systemic industry issues are made public but without disclosing the identity of complainants.

Background Information

GUIDELINE 1: Treat Clients Fairly

Clients need to be treated fairly if they are to trust digital payments, especially those clients with low levels of financial and technological capability.

EXAMPLES OF TREATING DIGITAL PAYMENTS CLIENTS FAIRLY INCLUDE:

1. All **advertising and other sales information** is communicated using language and terms that are simple, clear, accurate, and not misleading.
2. Product terms provide a **reasonable balance between client and provider interests**.
3. **Clients are treated respectfully**, for example by only being sold digital products that they are really in need of.
4. **Identification requirements** are appropriate for clients so as to facilitate access.
5. Clients are treated equally so there is **no unfair discrimination**. For example, providers do not discriminate on the basis of gender, religion, ethnicity, politics, sexual orientation, age, residence, or a disability.
6. In the case of **lost or stolen access devices,** security credentials, or identity, providers compensate a client for any transaction that occurs after the client has reported the loss or theft to the provider. Compensation is also payable to the extent a transaction is above a daily or periodic limit.
7. A client is compensated for any late payment fee payable if inability to make a payment was because of a scheduled **system outage** that the client was not told of.
8. If a client initiates a digital payment in a **power outage**, the provider processes it as soon as possible.

BACKGROUND

Clients needs to be treated fairly if they are to have confidence in using digital payments. This is especially important for clients who have little or no experience with financial services – a category which disproportionately includes women, given the gender access gap. A leading example of this approach is found in the *G20 High-Level Principles on Financial Consumer Protection* under Principle 3: "All financial consumers should be treated equitably, honestly and fairly at all stages of their relationship with financial service providers. … Special attention should be dedicated to the needs of vulnerable groups."[3]

1.1 Advertising and other sales information

Guideline 1.1 is similar in focus to Standard 3 of Principle 1 in the new version of The Smart Campaign's *Client Protection Certification Standards*, which calls for "A policy and documented process [that is] in place to prevent aggressive sales techniques and forced signing of contracts."

Guideline 1.1 could cover all promotional materials shared with an existing or potential client through any media and by agents and employees, as well as product information in promotional brochures.

1.2 Product terms balance client and provider interests

Part of treating clients fairly is ensuring that standard digital payments terms and conditions do not take unfair advantage of clients. Examples of unfair terms include clauses that make the client liable for all mistaken payments (even after notice is given) or that state the provider has no liability for their agents or for any failure to provide the service the client is paying for. Bank Indonesia Regulation Number 16/1/PBI/2014 Consumer Protection in Payment System (from now on referred to as the **Indonesia Regulation on Consumer Protection Payment Systems**) is an example of payments-specific regulations that address the issue of unfair terms.[4]

1.3 Clients are treated respectfully

As noted in Principle 5 of The Smart Campaign's *Client Protection Principles,* respect for clients goes hand in hand with fair treatment. There are many ways in which respect for clients can be shown. This can include

only selling clients products that suit their needs and capacity. For example, showing respect could include not pressuring a potential client to acquire a digital payments product without considering whether the product will suit their payment needs and not encouraging uptake of such products where the client does not have easy access to an agent network for cash-in and cash-out services. Another example is assessing whether a digital transaction account client can realistically repay a linked microloan before offering the loan. Finally, female clients should be treated with respect according to same respect as male clients.

1.4 Client identification requirements

Low-income clients are unlikely to possess forms of traditional identification such as a national ID, driving license, passport, birth certificate, or a street address. For this reason alone they may be denied access to digital payments services.

However, the revised 2012 *Financial Action Task Force (FATF) Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (from now on referred to as the **FATF *Recommendations***), which are the basis for national anti-money laundering and counter-terrorism laws, mandate the use of risk-based customer identification requirements.[5]

A payment service such as an electronic money account may be an example of such a product, depending on factors such as limits on transactions and balances. FATF guidelines on the requirement to verify a customer's identity also make clear that it is not necessary to rely on government issued identification documents (which many low-income customers do not have), and noted that this "flexibility is particularly relevant for financial inclusion."[6]

1.5 Discrimination

Guideline 1.5 is similar to Principle 5 Standard 2 of The Smart Campaign's *Client Protection Certification Standards* (from now on referred to as **The Smart Campaign's *Certification Standards***). In summary, they seek to limit discrimination on the basis of ethnicity, gender, age, disability, political affiliation, sexual orientation, caste, and religion.

1.6 Lost or stolen access device, security credential, or identity

Guideline 1.6 proposes compensation for any transaction that occurs after a loss or theft has been reported to the provider and in cases where the transaction amount is above a daily or periodic transaction limit. This is similar to the approach found in, for example, the ePayments Code, administered by the Australian Securities and Investment Commission (from now on referred to as the **Australia ePayments Code**), although that Code has a more complex approach to the allocation of liability.[7]

1.7 System outages

The Consultative Group to Assist the Poor's (CGAP) Focus Note on *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks* (from now on referred to as the **CGAP *Focus Note on Digital Finance***) identified "Inability to transact due to network/service downtime" as the first of seven key risks faced by consumers.[8]

System outages are a common client concern. Clients understandably expect that they should be able to access funds in digital payments accounts as needed. This is especially important for low-income clients who may not have access to other sources of funds. However, these Guidelines propose that clients can only realistically expect to be compensated for the direct loss of a late payment fee that is payable because of a system outage of which they had no prior notice (as opposed to indirect losses such as those arising from a loss of business profits).

A broader approach to the issue of system outages is provided in the Australia ePayments Code Clause 14.2, which states that a subscriber must not deny a user's right to claim consequential damages resulting from any malfunction of a system or equipment provided by any party to a shared electronic network (unless the client should reasonably have been aware of the malfunction or outage ahead of time).[9]

1.8 Power outages

Guideline 1.8 deals with the common issue of power outages that affect digital payments. In such cases clients need an assurance that payments which were initiated, but not received, will be processed as soon as possible.

GUIDELINE 2: Keep Client Funds Safe

Clients, especially the financially excluded or underserved, need reliable and secure access to funds in digital transaction accounts.

EXAMPLES OF SAFEGUARDING CLIENT FUNDS HELD IN DIGITAL TRANSACTION ACCOUNTS INCLUDE:

1. **Matching Funds:** For providers who are not subject to prudential regulation, they hold in separate account(s) in prudentially regulated institutions unencumbered funds that equal, in full, all outstanding balances. Alternatively, matching funds could be invested in other permissible securities (such as government securities with an active secondary market). Ideally, accounts and investments are held for the benefit of clients (such as in a trust account). Matching funds are also only used to make payments to clients and not for operational purposes. Matching funds are also protected from claims made by the provider's third party creditors. Supervisors can access account and investment records on a real-time basis, where this is feasible.
2. **System Capacity and Security:** Robust steps are taken to ensure reliable network and system capacity as well as a payments network and delivery channel that is secure from fraud, hacking, and any other form of unauthorized use.
3. **Fraud:** A client is compensated by the provider for any direct loss due to fraud by agents, employees, and third party service providers (such as their agent network managers) and for third party fraud caused by a reasonably preventable security breach. Clients are also informed promptly of any suspected fraud.
4. **Mistaken and Unauthorized Transactions:** The user interface is designed to be clear, simple, and secure. It also requires confirmation of payment details before transaction is completed. The aim is to minimize the risk of mistaken and unauthorized transactions, as well as to facilitate easy access.

BACKGROUND

2.1 Matching funds

The most fundamental risk faced by clients who are using a digital payments product is that the client will not be able to access their funds when needed. Indeed, the CGAP *Focus Note on Digital Finance* lists as a key risk "Insufficient agent liquidity or float, which also affects ability to transact."

There is also the risk that the provider, or their bank, will become insolvent. Finally, general operational risks could affect the client's ability to transact.[10]

In particular, the Better Than Cash Alliance Guideline 2 provides the following as examples of good practices:

- Matching outstanding balances of funds and securities should be "unencumbered," meaning they may not be used as security for any other debt.
- Matching funds could be held in an account in a prudentially regulated institution (such as a trust account) or in other permitted investments (such as government securities).
- Matching funds are only used to make payments to clients and need to be protected from claims made by third party creditors to protect against liquidity and insolvency risks.

There are numerous examples of principles, standards, and codes, as well as national legislation that address safeguarding the float for client funds held in digital payment accounts. They include:

- Guiding Principle 2 in *Payment Aspects of Financial Inclusion (PAFI)*, a report from the Committee for Payments and Markets Infrastructure and the World Bank (from now on referred to as the **PAFI report**);
- Principle 1 of the GSMA *Code of Conduct*; and
- Legislation and guidelines in countries such as Afghanistan, Kenya, Malawi, the Philippines, and Tanzania.[11]

These examples treat this critical issue in different ways but they all address the essential issue of protecting client funds.

2.2 System capacity and security

Clients understandably expect a robust and ongoing focus on the capacity and security of digital payments systems. The PAFI report emphasizes the need for reliable and high quality access points and channels (see Guiding Principle 5). The GSMA *Code of Conduct* contains detailed provisions on system security and capacity (see especially Guidelines 4 and 5), which can also be found in Guiding Principle 3 in the PAFI report and the Bill & Melinda Gates Foundation *Level One Project Guide* (from now on referred to as **the Gates *Level One Project Guide***).

Finally, these concerns have been addressed at the national level. For example, the Philippines 2009 Circular No. 649 on Electronic Money requires appropriate security policies and measures to safeguard the integrity, authenticity, and confidentiality of data and operating systems.[12] The Indonesia Regulation on Consumer Protection Payment Systems also addresses security issues in general terms.[13] Nigeria's new Consumer Protection Framework is more specific in that it provides that the Central Bank "shall specify minimum technology standards for payments platforms."[14]

Clients may also expect immediate, real-time settlement of digital payments. However, this Guideline does not deal with this issue since not all payment systems can provide real-time settlement. For guidelines on real-time settlements, see Guideline 1.2.1 of the Gates *Level One Project Guide* concerning immediate funds transfers and same day settlement as well as Guideline 1.2.1 of the GSMA *Code of Conduct*, both of which refer to the debiting and crediting of money in real time.

2.3 Fraud

Most clients expect to be compensated by the provider in case of fraud committed by employees, agents, and third party service providers. Clients may also expect compensation in the case of fraud arising from any security breach that could have reasonably been prevented (for example through a third party hacker). In some respects, Guideline 2.3 might appear to be onerous. However, fraud is a significant risk for clients, as highlighted in the 2014 *Responsible Finance Forum V: Responsible Digital Finance Outcomes Report* (from now on referred to as the ***Responsible Finance Forum V Outcomes Report***). Clients usually expect payment service providers to be responsible for any fraud committed by persons and entities that are (or should be) under their control.

As noted in the preamble to Directive (EU) 2015/2366 of The European Parliament and of The Council of 25 November 2015 on Payment Services in the Internal Market (from now on referred to as **PSD2**): "All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud."[15] PSD2 contains very strong provisions in support of users who claim they have not authorized a transaction.[16]

The need to take action to prevent fraud is also an ongoing theme addressed throughout the Gates *Level One Project Guide* and in various other forums and publications. For example, the CGAP *Focus Note on Digital Finance* identifies as a key risk "Fraud that targets customers," and the *Responsible Finance Forum V Outcomes Report* identified fraud as a key risk area that must be addressed.

2.4 Mistaken and unauthorized transactions

Most experts and commentators agree that digital payments systems should have a clear and easy-to-use interface to reduce the risk of mistaken transactions as well as to encourage the ongoing use of payments services. The CGAP *Focus Note on Digital Finance* highlights as a key risk "User interfaces that many find complex and confusing." The *Responsible Finance Forum VI: Evidence and Innovation for Scaling Inclusive Digital Finance Report* (from now on referred to as the ***Responsible Finance Forum VI Report***) also addresses the importance of user-friendly interfaces.

Unauthorized transactions are also a key concern for clients, and they expect user interfaces to be secure. PSD2 puts a heavy onus on the provider in relation to transactions that the user claims were not authorized or were incorrectly executed.[17]

GUIDELINE 3: Ensure Product Transparency for Clients

Providing clients with transparent product information requires special attention in a digital environment, especially where information is only available electronically, such as on a mobile phone.

EXAMPLES OF ENHANCING PRODUCT TRANSPARENCY IN A DIGITAL ENVIRONMENT INCLUDE:

1. **Product Information:** Each client is given access (which may be in digital form) to a clear, simple, and readily comparable statement of product features, terms, fees, and any interest payable. This is done before the payments service is provided. The information is kept updated and is in a form that the client can keep and/or access, including digitally. The provider also explains the information to the client on request or if it appears that they cannot understand it (for example, if it is in a language they do not understand).
2. **Transaction and Account Records:** A client receives proof of each transaction and has easy access to clear and simple transaction and account records. These records could be digitally provided. They also need to be in a form the client can keep or access, such as a digital transaction history.

BACKGROUND

3.1 Product information

Product information that is clear and easy to understand assists in creating informed clients who are more likely to trust, and use, digital payments. It also allows for product comparisons and can encourage competition and reduce costs. However, disclosures are not helpful if they are so lengthy and complex that clients cannot understand them.

On the other hand, information provided on a small mobile phone screen may be insufficient, as noted in the *Responsible Finance Forum V Outcomes Report*. In any event, the information needs to be accessible for future reference, for example if a client has a complaint. The product terms and conditions could be provided by email, made available via a website, or come from an agent. Guideline 3.1 is designed to reflect these considerations.

The importance of transparency is widely recognized by other international guidelines and standards. For example, a key risk identified by the CGAP *Focus Note on Digital Finance* is "Nontransparent fees and other terms," and it stresses that "Transparency of product information is key to the provision of responsible digital finance." It also highlights the importance of well-designed, comparable disclosures.

Further, all of the following stress the importance of transparency (to differing degrees):

- Guideline 6.1.1 of the GSMA *Code of Conduct*;
- Principle 3 of The Smart Campaign's *Client Protection Principles*; and
- Guiding Principles 2 and 5 in the PAFI report.

The latter Principles also note the need to use "comparable methodologies" and they suggest that information be provided on risks associated with using a product and on how to minimize costs while maximizing benefits.

There are also many examples at the national level of government as well as legislative initiatives providing for transparency of financial product information and performance. These initiatives may apply to digital payments products as well as other types of financial services.

A leading example comes from the Bureau of Financial Institutions in Mexico.[18] The Bureau publishes information on its website about a financial institution's products, fees and commissions, unfair terms, complaints, sanctions, and other information relevant to the institution's performance. Financial institutions are also required to publish this information on their own website. Other examples include transparency requirements in the Indonesia Regulation on Consumer Protection Payment Systems and the provisions requiring disclosure of fees and charges in Tanzania's Electronic Money Regulations, 2015.

3.2 Transaction and account records

Clients may expect to have continuous access to clear and simple transaction and account records. To be useful, these need to be in a form that clients can easily understand and rely on. Such records are especially important if a client has a complaint about a specific transaction. For example, there might be a complaint that a payment was made by mistake or it was not received. Records could be in a digital form, provided that the client can easily keep and/or access the information.

GUIDELINE 4: Design for Client Needs and Capability

Designing digital payments to address the needs, economic roles, and capabilities of clients, especially women, will increase suitability and use.

EXAMPLES OF ACTIONS RELEVANT TO THE DESIGN OF DIGITAL PAYMENTS SERVICES INCLUDE:

1. **Payment Service Design:** Digital payment services are designed on the basis of research as to clients' needs, preferences, and behavior. Their design also takes account of clients' likely financial and technological capability levels and, particularly in the case of underserved markets, is simple and clear. Given women's greater exclusion, it is particularly important that payment services be designed to meet women's needs and capabilities and economic roles.
2. **User Support:** Each client of a digital payments service is given:
   - **(a)** Easily understood instructions on how to use the service and safeguard their security credentials (such as passwords and PINs) in addition to an outline of related client responsibilities;
   - **(b)** Contact details for a 24-hour hotline to notify the provider about a lost or stolen access device or related security credentials, a mistaken or unauthorized transaction, or a security breach;
   - **(c)** Contact details for reaching the provider during local business hours so clients have a reliable source of information about how to use a digital financial service and its features; and
   - **(d)** Additional support to first-time users, particularly women, as needed and feasible, to support safe uptake and use.

BACKGROUND

4.1 Payment service design

As highlighted in the *Responsible Finance Forum VI Report*,[19] to be useful — and used — digital payments services need to be designed to meet the needs of target client groups. They also need to take into account clients' likely preferences and behaviors. For example, Principle 1 of The Smart Campaign's *Client Protection Principles* deals with appropriate product design and delivery, while PAFI Guiding Principle 4 refers to the need for transaction and payment products to "meet a broad range of transaction needs of the target population, at little or no cost." There is, however, no reference in the Better Than Cash Alliance Guidelines to the cost of payments, as this may limit innovation and competition. Rather, the focus is on encouraging appropriate product design. This can be achieved, for example, through client-oriented research, client focus groups, and surveys, which take into consideration sub-segments of the market, including women in their different economic roles.

4.2 User support

Underserved clients using digital payments are likely to have low levels of financial or technological capability. This may discourage them from using digital payments. Clients may also not understand the risks of sharing PINs or how to avoid mistaken transactions, or understand even the features of a digital payments service and how to use it. Building the capabilities of women is a worthwhile investment. Guideline 4 provides simple, actionable steps that might assist with these issues.

Guideline 4 does not, however, seek to cover the full range of financial capability strategies and programs that could be used for digital payments. This is because the Alliance Guidelines are intended to be specific and actionable. However, Guiding Principle 6 in the World Bank PAFI report, which deals with financial literacy issues, makes specific suggestions, including:

- Ongoing public and private sector coordinated financial literacy efforts;
- A clear focus on transaction accounts in financial literacy programs;
- A focus on providing information about the types of accounts that are available, account opening requirements, applicable fees and how to minimize costs, risks, basic security measures, and the overall obligations of providers and users; and
- Hands-on training as part of rolling out a new product.

GUIDELINE 5: Support Client Usage Through Interoperability

While recognizing the need to balance competition and innovation, ensuring the interoperability of platforms, agents, and clients is highly desirable so clients of different schemes can make payments to each other and agents can work for different providers. This is especially important for clients living in remote rural areas.

EXAMPLES OF FACILITATING INTEROPERABILITY INCLUDE:

1. Encourage collaborative and industry-led interoperability initiatives to ensure that clients can make digital financial transactions regardless of where they live or who their provider is.
2. Discourage any deliberate barriers to interoperability (such as exclusive agent arrangements).

BACKGROUND

Clients need interoperability if use of digital payments services is to develop.

Interoperability of platform, agents, and customers are related but separate concepts. CGAP research on the subject summarizes these three different forms of interoperability as follows: platform interoperability that allows for payment transactions between different service providers; agent interoperability that allows for a single agent to act for multiple service providers; and customer interoperability that would allow a customer to access any phone on the same network with a SIM card and to access multiple accounts using one SIM card.[20]

5.1 A collaborative approach

This Guideline encourages collaborative industry-led interoperability efforts that will benefit clients. Ideally this would be done under the guidance of key supervisors, especially given concerns about anti-competitive arrangements that may violate anti-trust laws. An example of such an approach is the recently launched Bim mobile money platform in Peru. This is a significant collaborative effort between Peru's Government, financial institutions, telecommunications operators, and other stakeholders. The platform enables digital payments services to be interoperable across each of the participating mobile networks and payments providers and all their agents.[21] Another leading example of such collaboration comes from the "test and learn" approach used in Tanzania. For details see the International Finance Corporation's (IFC) 2016 *Tanzania Case Study: Achieving Interoperability in Mobile Financial Services*.

In contrast to the industry-led approach, government regulations can expressly provide for interoperability. An example of this approach is found in Kenya's National Payment System Regulations, 2014, where Regulation 21.1 states that "A payment service provider shall use systems capable of becoming interoperable with other payment systems in the country and internationally." Nigeria also mandated interoperability for mobile money operators in 2012.[22]

Other international organizations promote interoperability as well. Examples include the Gates *Level One Project Guide*, which encourages interoperability for transfers and related regulatory support;[23] and Guiding Principles 3 and 5 in the PAFI report, which call for infrastructure that allows for the switching, processing, clearing, and settlement of payment instruments of the same kind, in addition to interoperable access channels.

5.2 Barriers to interoperability

It is also important that there are no artificial anti-competitive barriers to interoperability. A classic example is when a provider does not allow its agents to work for other providers. These types of exclusive arrangements can cause great inconvenience for clients of other providers in the relevant area who do not have easy access to an agent network. Another example would be an arrangement under which clients of a provider can only make payments to, or receive payments from, other clients of their provider. It is however recognized that there is a need to balance competition concerns and the need of providers to obtain a return for investment in innovation.

GUIDELINE 6: Take Responsibility for Providers of Client Services Across the Value Chain

Clients are more likely to trust and use digital payments if the provider take responsibility for the actions of agents, employees, and third party service providers across the value chain.

EXAMPLES OF SHOWING RESPONSIBILITY FOR AGENTS, EMPLOYEES, AND THIRD PARTY SERVICE PROVIDERS INCLUDE:

1. **Liability:** Providers take responsibility for the acts and omissions of their agents, employees, and third party service providers.
2. **Training and Oversight:** Agents and employees, and those of third party service providers, are appropriately trained and monitored, including on product features, regulatory responsibilities, and gender-sensitive conduct. They also have the resources to competently and lawfully provide payments services.
3. **Provider Details:** Agents tell clients the name and contact details of the provider when an account is opened and on request.

BACKGROUND

6.1 Liability

A key feature of a responsible digital payments market is one where providers take responsibility for the acts and omissions of their service providers and their effects on clients. Agents are a particular case in point, and the term "third party service provider" includes agent network managers. In some countries this liability may already arise under law, but this is not the case in all countries and the issue is a critical one.

An example of a legislative approach can be found in Regulation 37 of Tanzania's Electronic Money Regulations, 2015, which states "A payment service provider is liable to its customers for the act[s] and omissions of its agents performed within the scope of the agency agreement."

GSMA Guideline 3 also covers the issue of responsibility for agents, but does not refer to employees or third party service providers. The Indonesia Regulation on Consumer Protection Payment System provides another example, stating that a provider is responsible to its consumers for any losses arising from mistakes made by management and employees.[24]

6.2 Training and oversight

Clients may legitimately expect a provider to take responsibility for appropriately training and supervising their agents, employees, and service providers. This would include, for example, training on the features and risks of payments services, how to use the service, how to communicate with clients, security safeguards (for example in relation to PINs), customer recourse mechanisms, and prohibited practices (for example in relation to fraud and discrimination). This should also include relevant gender-sensitive conduct, for example, male agents not touching the hands of female clients when registering thumbprints for biometric IDs in India. In the case of third party service providers the relevant obligations could be imposed via the agreement with the service provider.

6.3 Provider details

It is more likely that a payment services client will primarily come in contact with an agent as opposed to the provider or even an employee of the provider. It is, however, important that a client knows who the provider is, in order to determine whether or not they wish to use that product, or if they choose to use the product, so that they know to whom to direct any complaint.

GUIDELINE 7: Protect Client Data

Protecting clients' digital data is increasingly important given the volume, velocity, and variety of data being used for marketing and credit scoring, while recognizing that use of client data can increase the range of products a client can access.

EXAMPLES OF HOW CLIENT PERSONAL DATA MIGHT BE PROTECTED IN A DIGITAL ENVIRONMENT AT A BASIC LEVEL INCLUDE:

1. **Confidentiality and Security:** Reasonable measures are taken to ensure the confidentiality and security of client data relevant to digital payments. Examples of such data include identification and contract information; transaction histories; security credentials; device, mobile phone, and Internet usage data; and geolocation data. With the express and informed consent by clients, data can be used and disclosed for specific purposes, such as to market new services.
2. **Audit Trail:** A clear audit trail of transaction records is accessible to clients and supervisors.

BACKGROUND

7.1 Confidentiality and security

Data protection and privacy in the digital environment was a key risk discussed in the *Responsible Finance Forum V Outcomes Report* and the *Responsible Finance Forum VI Report*. It is also acknowledged as a central regulatory issue in the report on G20 Principles for Innovative Financial Inclusion (2010).[25] Guideline 7.1 covers critical personal data concerns for digital payments clients. However, it does not seek to deal with all potential data issues. Additional issues not covered by this Guideline might include: access and correction rights; limits on collection and use of personal information (for example concerning the use of personal information for marketing purposes); limits on data retention periods; and a requirement to publish details of the provider's privacy policy. Guideline 7 also does not address the use of "Big Data" analytics in connection with digital payments services.[26]

There are various examples of principles, standards, and codes (as well as national legislation) that provide broad coverage of data protection issues. They include:

- The G20 Principles for Innovative Financial Inclusion (2010)
- The 2013 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*;
- The 2009 Madrid Resolution's *Joint Proposal on International Standards on the Protection of Personal Data and Privacy*;
- The Institute for Data Driven Design's 2014 *Windhover Principles for Digital Identity, Trust, and Data*;
- Guideline 6 of the Smart Campaign's *Client Protection Principles* (which also limits use of data to the primary purpose of collection, subject to consent); and
- Guideline 8 of the GSMA Code of Conduct.

There are also data protection requirements relevant to digital financial services at the national level, such as those in Indonesia and the Philippines, amongst others.[27]

7.2 Audit trail

An audit trail ensures that clients can obtain evidence of past transactions. This can be especially helpful in the case of a disputed transaction and also for supervisory purposes (for example in checking on whether there has been compliance with provisions concerning safeguarding client funds).

GUIDELINE 8: Provide Client Recourse

Clients need access to a fair recourse system for dealing with complaints about digital payments. This is especially necessary for complaints about innovative and unfamiliar products delivered via new channels and for clients who live remotely and may have little to no direct contact with providers.

EXAMPLES OF EFFECTIVE RECOURSE SYSTEMS FOR DIGITAL PAYMENTS CLIENTS INCLUDE:

1. **Complaints:** Clients can easily access a transparent, free or low-cost, efficient complaints system. Such a system should be accessible to all, regardless of cultural norms, language, mobility, etc. The system is accessible by phone or digitally (such as via a website or by text message), or by visiting the provider's place of business.
2. **Disputes:** Clients also have access to an independent third party who handles disputes with providers in cases where the client's complaint has not been adequately addressed and resolved by the provider. This third party system is easily accessible (including by phone or digitally), transparent, free or low-cost, and efficient.
3. **Information about Recourse Systems:** Information about a provider's recourse system are set out in terms and conditions that are available on the provider's website and at the premises of both the provider and the agent. In addition, once a client makes a complaint they receive a copy of this information, which may be in digital form.
4. **Complaints Data:** Providers maintain records of client complaints and their response to each complaint. Regulators are also given periodic reports of complaints data. Systemic industry issues are made public but without disclosing the identity of complainants.

BACKGROUND

8.1 and 8.2 Complaints and disputes

The CGAP *Focus Note on Digital Finance* identified "poor recourse systems" as one of seven key risks faced by consumers. Many existing principles, standards, codes, and national regulations address the need for internal and external consumer recourse systems, including Guideline 7 of the GSMA *Code of Conduct*, Guiding Principle 2 in the PAFI report, and Guideline 7 of The Smart Campaign's *Client Protection Principles.*[28]

Guideline 8 is intended to cover both client recourse systems available from a provider in addition to external dispute resolution services. Examples of the latter include an industry or statutory financial ombudsman type scheme, or a mediation service provided by a supervisor. At the country level, examples of dispute resolution entities include CONDUSEF in Mexico,[29] the new Financial Ombudsman Scheme in Malaysia,[30] the Ombudsman for Banking Services in South Africa,[31] and the Office of the Ombudsman in Rwanda.[32]

8.3 Information about recourse systems

Clients need to have an awareness of where to go if they have a complaint or a dispute. Accordingly, information about recourse systems should be widely available. This is consistent with the findings from The Smart Campaign's recent Client Voice Project, which revealed a widespread lack of awareness about recourse channels in the four countries it surveyed (Benin, Georgia, Pakistan, and Peru). This included Peru and Georgia, both of which appear to have a solid consumer protection framework.[33] In Benin only 14 percent of respondents recalled being told where to go with problems or complaints. In Georgia, Pakistan, and Peru that percentage came to 37 percent, 34 percent and 29 percent respectively.[34]

The Smart Campaign's *Client Protection Certification Standards* now require that "The [financial institution] informs clients about the right to complain and how to make a complaint."[35]

8.4 Complaints data

From the client perspective, it is important that providers keep records of progress in dealing with a complaint and the final outcome. Ideally complaints data are also reported to the relevant regulator so they can identify potential systemic issues affecting clients. To be useful to clients, such information should be published.

Guideline 8.4 does not make any provision for the identity of providers to be made public when information about systemic complaints issues is published. Yet such data may help not only consumers seeking to choose a provider but also the providers themselves since it allows them to make comparisons with their competition. The supervisor or a financial ombudsman service could provide this information. Examples include the database on complaints maintained by the Consumer Financial Protection Bureau in the United States;[36] the United Kingdom Financial Conduct Authority data about individual firms;[37] and the information published by the Bureau of Financial Institutions in Mexico.[38]

Glossary of Terms and Acronyms

AML/CTF	Anti-money laundering and counter-terrorism financing
Australia ePayments Code	ePayments Code, administered by the Australian Securities and Investment Commission
CGAP	The Consultative Group to Assist the Poor
CGAP *Focus Note on Digital Finance*	CGAP Focus Note on *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks* (2015)
FATF	Financial Action Task Force
FATF Recommendations	*Financial Action Task Force (FATF) Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (2012)
Gates *Level One Project Guide*	The Bill and Melinda Gates Foundation *Level One Project Guide: Designing a New System for Financial Inclusion* - (2015)
GSMA	Groupe Spéciale Mobile Association
GSMA *Code of Conduct*	The GSMA *Code of Conduct for Mobile Money Providers* (2014)
Indonesia Regulation on Consumer Protection Payment Systems	Bank Indonesia Regulation Number 16/1/PBI/2014
IFC	International Finance Corporation
OECD	Organisation for Economic Co-operation and Development
PAFI report	*Payments Aspects of Financial Inclusion Report* from the Committee for Payments and Markets Infrastructure of the Bank for International Settlements and the World Bank (2016)
PSD2	Directive (EU) 2015/2366 of The European Parliament and of The Council of 25 November 2015
Responsible Finance Forum V Outcomes Report	*Responsible Finance Forum V: Responsible Digital Finance Outcomes Report* (2014)
Responsible Finance Forum VI Report	*The Responsible Finance Forum VI: Evidence and Innovation for Scaling Inclusive Digital Finance Report* (2015)
The Smart Campaign's *Certification Standards*	The Smart Campaign's *Client Protection Certification Standards* (2016)
Tanzania Electronic Money Regulation	Tanzania Electronic Money Regulations, 2015

References

Afghanistan Da Afghanistan Bank Law (2003)
http://dab.gov.af/Content/Media/Documents/DABLaw211020151441970755332 5325.pdf

Afghanistan Mobile Service Providers Regulation
http://www.fintraca.gov.af/assets/pdf/money_service_providers_regulation.pdf

Australia ePayments Code (2016)
http://download.asic.gov.au/media/3798542/epayments-code-published-29-march-2016.pdf

Bank Indonesia Regulation (2014) No. 16 /1/PBI Consumer Protection in Payment System Service
http://www.bi.go.id/en/peraturan/sistem-pembayaran/Documents/pbi_160114.pdf

Centre for Financial Inclusion (2016) 'BiM The First Fully - Interoperable Mobile Money Platform: Now Live in Peru'
https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru/

Consumer Financial Protection Bureau, (2016) 'Consumer Complaints Database'
http://www.consumerfinance.gov/data-research/consumer-complaints/

CGAP (2015) 'Doing Digital Finance Right'
http://www.cgap.org/publications/doing-digital-finance-right

CGAP (2016) 'Interoperability in Branchless Banking and Mobile Money'
http://www.cgap.org/blog/interoperability-branchless-banking-and-mobile-money-0

Committee for Payments and Markets Infrastructure of the Bank for International Settlements and the World Bank Group (2016)
'Payments Aspects of Financial Inclusion Report'
http://pubdocs.worldbank.org/pubdocs/publicdoc/2016/4/963011459859364335/payment-systems-PAFI-Report2016.pdf

Financial Action Task Force (2012) 'International Standards on Combating Money Laundering and the Financing of Terrorism & Protection'
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Financial Conduct Authority (United Kingdom) (2016) 'Complaints Data'
https://www.the-fca.org.uk/firms/complaints-data

G20 (2011) 'High-Level Principles on Financial Consumer Protection'
https://www.oecd.org/daf/fin/financial-markets/48892010.pdf

G20 Global Partnership for Financial Inclusion (2016) 'Global Standard-Setting Bodies Financial Inclusion The Evolving Landscape'
http://www.gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-evolving-landscape

G20 Principles for Innovative Financial Inclusion (2010). Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group.
https://www.gpfi.org/sites/default/files/documents/Principles%20and%20Report%20on%20Innovative%20Financial%20Inclusion_0.pdf

J Greenacre and RP Buckley, University of New South Wales (2014) 'Using Trusts to Protect Mobile Money Customers'
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454

GSMA (2014) 'Code of Conduct for Mobile Money Providers'
http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/policy-and-regulation/code-of-conduct

IFC (2016) 'Tanzania Case Study Achieving Interoperability in Mobile Financial Services'
http://www.ifc.org/wps/wcm/connect/8d518d004799ebf1bb8fff299ede9589/IFC+Tanzania+Case+study+10_03_2015.pdf?MOD=AJPERES

International Conference of Data Protection and Privacy Commissioners (2009)
'Madrid Resolution International Standards on the Protection of Personal Data and Privacy'
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

Kenya The National Payment System Act, 2011 (No. 39 of 2011)
https://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf

Kenya The National Payment System Regulations (2014)
https://www.centralbank.go.ke/images/docs/legislation/NPSRegulations2014.pdf

Malawi Mobile Payments Guidelines (2011)
https://www.rbm.mw/PaymentSystems/

Nigeria (2012) Central Bank of Nigeria Direction BPS/DIR/GEN/CIR/01/014
http://www.cenbank.org/out/2012/ccd/timeline%20for%20interoperability%20&%20interconnectivity.pdf

Nigeria Consumer Protection Framework (2016)
https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf

OECD (2013) 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Philippines Central Bank E-Money Circular 649 (2009)
http://www.bsp.gov.ph/downloads/Regulations/attachments/2009/c649.pdf

Responsible Finance Forum V (2014) 'Responsible Digital Finance Outcomes Report'
https://www.responsiblefinanceforum.org/wp-content/uploads/RFFVSummaryRepor.pdf

Responsible Finance Forum VI (2015) 'Evidence and Innovation for Scaling Inclusive Digital Finance Report'
https://responsiblefinanceforum.org/wp-content/uploads/RFF6-report-5_21-final-low_res.pdf

Tanzania The National Payments System Act (2015)
https://www.bot-tz.org/PaymentSystem/NPS%20Act%202015.pdf

Tanzania The Electronic Money Regulations (2015)
https://www.bot-tz.org/PaymentSystem/GN-THE%20ELECTRONIC%20MONEY%20REGULATIONS%202015.pdf

The Bill and Melinda Gates Foundation (2015) 'Level One Project Guide: Designing a New System for Financial Inclusion'
https://www.betterthancash.org/tools-research/resources/the-level-one-project-guide-designing-a-new-system-for-financial-inclusion

The Smart Campaign (2011) 'The Client Protection Principles'
http://www.smartcampaign.org/about/smart-microfinance-and-the-client-protection-principles

The Smart Campaign (2015) 'My Turn to Speak: Voices of Microfinance Clients in Benin, Pakistan, Peru and Georgia'
http://smartcampaign.org/storage/documents/Synthesis_Report_ENG_FINAL.pdf

The Smart Campaign (2016) 'The Client Protection Certification Standards'
http://www.smartcampaign.org/storage/documents/Standards_2.0_English_Final.pdf

ID3 (2014) 'The Windhover Principles for Digital Identity, Trust, and Data'
https://idcubed.org/about/vision-mission-2/

World Bank (2012) 'Good Practices on Financial Consumer Protection'
http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf

Endnotes

1. The Better Than Cash Alliance, *Mapping of Principles, Standards, and Codes of Conduct in Digital Financial Services*, (forthcoming August 2016).
2. See, for example the *Payments Aspects of Financial Inclusion* (PAFI) report from the Committee for Payments and Markets Infrastructure and the World Bank; the World Bank's *Good Practices for Financial Consumer Protection*; The Smart Campaign's *Client Protection Principles;* the Bill & Melinda Gates Foundation *Level One Project Guide: Designing a New System for Financial Inclusion;* the 2016 G20 Global Partnership for Financial Inclusion report *Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape*; and the GSMA Code of *Conduct for Mobile Money Providers.*
3. As one example see the Indonesia Regulation on Consumer Protection Payment Systems, which specifies "equitable and fair treatment" as its first consumer protection principle (Article 3a). A second example is found under Principle 5 of The Smart Campaign's Client Protection Principles, which calls for the fair and respectful treatment of clients.
4. Article 8 of Indonesia Regulation on Consumer Protection Payment Systems.
5. See Recommendation 10 in *The Financial Action Task Force (FATF) Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (2012), which requires (amongst other things) that customer due diligence measures include "Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information," and that financial institutions "should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1." In summary, the Interpretative Notes to Recommendation 1 are to the effect that simplified measures to identify, assess, monitor, manage, and mitigate money laundering and terrorist financing risks may be used where risks are relatively low. All proposed Guidelines are, of course, subject to applicable law, including anti-money laundering laws counter-terrorism financing (AML/CTF) laws. Further, the Interpretative Notes to Recommendation 10 describe low-risk situations as those including "Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes." In addition, Guideline 2.5.1 of the Groupe Spéciale Mobile Association (GSMA) *Code of Conduct for Mobile Money Providers* (from now on referred to as the GSMA *Code of Conduct*) states that providers "may use a risk-based ['know your customer'] approach if permitted by local laws and regulations."
6. *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, (2012), Paragraph 67.
7. Chapter C of the Australia ePayments Code.
8. The CGAP *Focus Note on Digital Finance* reflects consumer research findings conducted in 16 markets: Bangladesh, Colombia, Cote d'Ivoire, Ghana, Haiti, Kenya, India, Indonesia, Nigeria, Pakistan, Peru, the Philippines, Russia, Rwanda, Tanzania, and Uganda. The *Focus Note* also presents findings from an initial lan dscaping study of relevant risk mitigation efforts by financial service providers, as well as observed consumer protection regulatory and supervision measures.
9. Clauses 14.2 and 14.3 of the Australia ePayments Code.
10. Greenacre and Buckley, *Using Trusts to Protect Mobile Money Customers*, (2014). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612454
11. Afghanistan's Da Afghanistan Bank Law and Mobile Service Providers Regulation; Kenya's: The National Payment System Act, 2011 (No. 39 of 2011) and The National Payment System Regulations, 2014; Malawi's Guidelines for Mobile Payments Systems; the Philippines BSP E Money Circular 649, 2009; Tanzania's National Payments System Act, 2015 and The Electronic Money Regulations, 2015.
12. Section 4(H) of the Philippines 2009 Circular No. 649 on Electronic Money.
13. Articles 3(c) and 14(2)(c) Indonesia Regulation on Consumer Protection Payment Systems.
14. Nigeria Consumer Protection Framework 2016 section 2.1.6.(2).
15. Paragraph 95 of PSD2.
16. Ibid., See Articles 71–74 and the definition of "strong customer authentication" in Article 4.
17. Ibid., Article 72.
18. http://www.buro.gob.mx/inicio.php?id_sector=0
19. See, for example, "Evidence Spotlight: How Commitment Products Break Down Behavioral Barriers to Savings," page 7 of the *Responsible Finance Forum VI Report.*
20. CGAP *Focus Note on Digital Finance.*
21. https://cfi-blog.org/2016/02/17/bim-the-first-fully-interoperable-mobile-money-platform-now-live-in-peru
22. Nigeria (2012) Central Bank of Nigeria Direction BPS/DIR/GEN/CIR/01/014
23. Pages 4 and 8 of the Gates *Level One Project Guide.*
24. Article 10 of the Indonesia Regulation on Consumer Protection Payment System.
25. *Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group*, page 13
26. "Big Data" has many definitions but a commonly used one is the Gartner definition: "Big Data" is high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (see the Gartner IT Glossary, available at http://www.gartner.com/it-glossary/big-data).
27. See Section 4(H) of the Philippines 2009 Circular No. 649 on Electronic Money and Articles 3(c), 14, and 15 of the 2014 Indonesia Regulation on Consumer Protection Payment Systems.
28. A country-level example of a requirement for an internal complaints scheme is section 4(F) of the Philippines 2009 Circular No. 649 on Electronic Money, which requires electronic money issuers to have an acceptable redress mechanism to address the complaints of consumers. Section 4(G) also requires that information on redress procedures be provided to consumers. Another example are the consumer redress provisions in Regulation 45 of Tanzania's Electronic Money Regulations, 2015.
29. http://www.condusef.gob.mx/index.php/english
30. http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press_all&ac=3283
31. http://www.obssa.co.za/
32. http://ombudsman.gov.rw/
33. The Smart Campaign, *My Turn to Speak: Voices of Microfinance Clients in Benin, Pakistan, Peru and Georgia*, (2015).
34. Ibid., Figure 27.
35. CPP 7 Standard 2.
36. http://www.consumerfinance.gov/complaintdatabase/
37. http://www.fca.org.uk/firms/systems-reporting/complaints-data
38. http://www.buro.gob.mx/inicio.php?id_sector=0

WWW.BETTERTHANCASH.ORG

About The Better Than Cash Alliance

The Better Than Cash Alliance is a partnership of governments, companies, and international organizations that accelerates the transition from cash to digital payments in order to reduce poverty and drive inclusive growth. Based at the United Nations, the Alliance has over 50 members, works closely with other global organizations, and is an implementing partner for the G20 Global Partnership for Financial Inclusion.