Code of Conduct of the FinTech Industry in Uganda

Version: 30 April, 2021

Table of contents

MSC (MicroSave Consulting) led the co-creation of the Code of Conduct for the FinTech industry in Uganda, together with FITSPA and its members, with support from FSD Uganda.

1. Introduction

1.1 Background of the code

1.1.1 This voluntary Code of Conduct has been developed by the Financial Technology Service Providers' Association (FITSPA) in consultation with the Financial Sector Deepening Uganda (FSDU).

1.1.2 The code covers the provision of financial technology services including but not limited to digital and mobile payment providers, payment gateways, e-money, cross-border payment providers, digital credit or savings, InsureTechs, blockchain-based finance and crypto-assets, digital microfinance, digital pension and savings platforms, P2P lenders, and crowdfunding platforms.

1.1.3 The Code of Conduct's principal aim is to support sustainable and responsible FinTech market development by gaining trust amongst all stakeholders in Uganda, particularly customers, users, and relevant regulators.

1.1.4 The code sets out the responsibilities of financial technology service providers (FinTechs) who have subscribed to the code (code subscribers) to ensure compliance with existing laws and regulations and further strengthen prudent and reliable business conduct. Specifically, the code is designed to meet the requirements of FinTechs for:

a) clarity on the contractual arrangements that govern their relationships with clients;
b) high standards of consumer protection and transparency of prices;
c) the resilience of underlying IT systems and cybersecurity standards;
d) confidentiality of personally identifiable and sensitive information and data protection;
e) confidentiality of commercially sensitive information;
f) good governance and business conduct practices, including involvement of third-party providers;
g) fair competition;
h) reliable AML practices;
i) support in establishing literacy programs and enabling financial inclusion; and
j) appropriate and timely communication and cooperation concerning the promotion of FinTech and the dialogue with regulators and other relevant stakeholders.

1.1.5 This code focuses on improving the quality and consistency of financial technology services. These services are subject to regulatory oversight. Subscribers of the code ensure that they comply with these obligations in delivering their service commitments.

1.1.6 This code does not supersede existing regulations. The code aims to supplement regulations and provide clarity on the duties and responsibilities of FinTechs.

1.1.7 This code is meant to be continuously evolving to extend it to all other non-FITSPA-member FinTech Service Providers operating in Uganda. It aims to ultimately influence member-to-member relations, member-to-non-member relations, and member-to-client relations.

1.2 Commitment to the code – The role of subscribers

1.2.1 The code subscribers agree to all of the code commitments and demonstrate business practices that align with and support compliance with these commitments in a report to FITSPA [Appendix 1].

1.2.2 If they comply with all applicable provisions in this code, the code subscribers can display a Certificate of Compliance on their website (or any other means of communications such as a mobile application).

1.2.3 The members can display the logo if they have met all the obligations to FITSPA, especially the membership fees on an annual basis or as otherwise arranged with FITSPA.

1.2.4 All potential members of FITSPA are encouraged to participate and comply with the Code of Conduct.

1.2.5 The code subscribers shall enable their customers (and any other relevant stakeholder) to access the Code of Conduct electronically.

1.2.6 A list of current code subscribers, including the right to display the Certificate of Compliance, is held by the FITSPA and regularly updated on their website (http://www.fitspa.ug).

1.3 Code ownership and administration

1.3.1 This code is voluntary for FITSPA members.

1.3.2 The members of FITSPA jointly own this code. FITSPA holds responsibility for the administration of the code.

1.3.3 The code administrator is the Secretariat of FITSPA.

1.3.4 FITSPA members can find the details of the processes and procedures relating to code administration in Section 7 of this document.

2. General principles

2.1 The Financial Technology Service Providers Association (FITSPA) members in Uganda publish the following Code of Conduct to underline their commitment to prudent and responsible business conduct of companies active in providing financial technology services to clients in Uganda and abroad.

2.2 The FITSPA members wish to affirm their commitment to a well-functioning marketplace, which provides reliable and responsible digital technologies for financial transactions.

2.3 The FITSPA members commit themselves to the highest standards of financial technology services and products in the economy of Uganda and globally.

2.4 The FITSPA members pledge to monitor the provisions laid down in this Code of Conduct, take prudent measures to enforce the code, and report a violation of the code in a fast and transparent manner.

2.5 Through this Code of Conduct, the FITSPA members share their mutual desire to position Uganda as one of the most innovative markets for financial services, building on the widespread use of mobile and digital technologies in the population of Uganda.

2.6 The FITSPA members confirm their commitment to improve access to financial services to every citizen of Uganda and make financial inclusion a core component of their business model.

2.7 The FITSPA members promote collaboration and cooperation between firms and raise the industry standards through this Code of Conduct. Thereby they commit to continuously evaluate and update the code with the evolution of financial service technology.

3. Business conduct and governance

3.1 Licensing

3.1.1 The code subscribers shall offer a financial service with a license issued by the competent authority, or if no specific licensing regime exists, concerning any other applicable law [Appendix 3].

3.1.2 The code subscribers shall disclose information about their license (if applicable) and business contact details on their website. Suppose, instead of having a license, the code subscribers have partnered with another licensed institution (e.g., bank or mobile network operator or others). In that case, they should publish information about their partnership on their website. The code subscribers shall also disclose other information according to Part 4 of the Electronic Transaction Act.

3.2 Regulatory compliance

3.2.1 The code subscribers commit to comply with all applicable regulations governing their business fully. [Appendix 3].

3.3 Risk management and business continuity procedures

3.3.1 The code subscribers shall have in place operational risk management and business continuity procedures.

3.4 Reliance on third-party providers

3.4.1 The code subscribers that rely on third-party providers or intermediaries must ensure that the third-party provider is:

- guided by customers' interests,
- performs professional activities according to their best knowledge, in a reliable manner and with due diligence, and
- respects for the obligations arising out of laws and regulations.

3.5 Holding customers' funds

3.5.1 The code subscribers that hold clients' funds shall:

3.5.1.1 establish safeguard measures to protect the funds deposited on their account from risks that may occasion loss to beneficiaries of the funds; and

3.5.1.2 not commingle the funds deposited by clients with any other funds.

3.6 Professional standards

3.6.1 The code subscribers commit to conduct their business professionally and hire professional staff.

3.6.2 The code subscribers commit to treating employees with respect, dignity, and fairness.

3.6.3 The code subscribers do not retaliate against whistle-blowers.

3.7 Conflict of interest management

3.7.1 The code subscribers shall list any possible conflict of interest between owners or staff members and consumers' interest in the compliance report to FITSPA.

3.8 Fraud prevention

3.8.1 The code subscribers shall have mechanisms in place to prevent fraud or unlawful usage of their services.

3.8.2 The code subscribers offering payment services shall have a specially designed transaction verification system, e.g., a verification number sent to a customer's phone via SMS.

3.8.3 The code subscribers offering payment services shall prescribe the manner of recovering an equivalent amount of transfer arising from a payment instruction or settlement made in the case of fraud, mistake, error, or similar vitiating factors.

3.8.4 The code subscribers shall not delete the financial data of customers for at least ten years.

3.9 Electronic signature and data messages

3.9.1 The code subscribers commit to using electronic signature and data messages according to all electronic transactions and electronic signatures laws.

3.10 KYC and AML/CFT

3.10.1 The code subscribers commit to comply with current Know-Your-Customers Rules and Anti Money Laundering provisions specified in the laws and regulations.

3.10.2 For this purpose, code subscribers shall obtain the necessary information about their customers' identity and financial situation and apply technical solutions to counteract money laundering and terrorism financing.

3.10.3 The code subscribers who engage in electronic fund transfers shall obtain and include accurate originator information and information relating to the recipient when carrying out electronic fund transfers.

3.10.4 The code subscribers shall refuse to conclude an agreement or execute a customer's transaction in a situation in which they cannot sufficiently identify the customer.

3.10.5 The code subscribers that are not required by the law to apply KYC and AML rules independently but instead partner with another licensed entity that is subject to these requirements (e.g., a bank) shall document how the partner is subject to KYC and AML rules.

3.10.6 The code subscribers commit to cooperate with other members of FITSPA on the prevention of money laundering by sharing best practices to identify unlawful usage of the service.

3.10.7 The code subscribers shall keep the records of their clients for ten years and be willing to present them to relevant authorities upon being demanded to do so according to the law.

3.10.8 If the code subscriber cannot obtain some information on their clients as required by existing regulation, they should justify it in their compliance report to the FITSPA.

3.11 Fair competition

3.11.1 The code subscribers commit to healthy competition and shall refrain from unfair (disloyal) competition. This entails the behavior of FinTechs against their competitors that goes against good business ethics and impairs their reputation or otherwise causes harm to their business, in particular:

a) publishing false or offensive information about a competitor;
b) disseminating written or oral communications about another FinTech or market participant to damage their reputation and interrupt their business operations;
c) trademark infringement and other misrepresentations of the competitor's goodwill that occur when a FinTech uses a name, logo, or other identifying characteristics to deceive customers into thinking that they are buying a competitor's product.
d) misappropriation of trade secrets that occurs when a FinTech uses espionage, bribery, or outright theft to obtain economically advantageous information in possession of another FinTech;
e) a gift or a promise of a gift or other privileges of a significant value given to other third-party providers and other FinTechs' partners to gain a competitive advantage over the competitors.

3.11.2 The code subscribers shall respect the intellectual property of their competitors.

3.11.3 The code subscribers refrain from taking any improper actions to influence the outcomes of public authorities' decision-making concerning the awarding of business contracts. The code subscribers will refrain from promising kickbacks or any other incentives to public and private sector officials.

3.12 Cessation of business

3.12.1 A code subscriber that intends to cease to carry on the FinTech business shall give notice of cessation of business to the FITSPA at least sixty days before the date of cessation. The code subscriber has to indicate to FITSPA in a written report how and when they will meet the ongoing responsibilities.

3.12.2 The code subscribers ensure that any legal and financial requirements towards consumers continue to be fulfilled after the cessation of the business.

3.13 Market statistics

3.13.1 ***The code subscribers report every three months*** the following statistics to the FITSPA Secretary, which are then published on an aggregated level [not identifiable by subscriber]:

a) The number of active accounts/clients;
b) The volume of transactions;
c) The volumes per FinTech vertical (Example: loans, savings, digital pensions, cross-border on payments);
d) The average default rates (for digital lenders);
e) Staff levels;
f) Coverage of the services in the regions of Uganda;
g) Data on Financial Inclusion and Gender Inclusion;
h) The number of complaints received from customers; and
i) The number of complaints resolved in the last reporting period.

3.14 Accounting standards

3.14.1 The code subscribers use accepted global financial accounting standards and reporting obligations unless regulators have prescribed other accounting standards in Uganda.

4. Consumer protection

4.1 General provisions for consumer protection

4.1.1 The code subscribers targeting retail customers organize their service to ensure that the retail customer is treated fairly, with courtesy and professional respect.

4.1.2 The code subscribers shall make available a user manual on their website, app, and social media.

4.1.3 The code subscribers shall have in place mechanisms for dispute resolution in case of a dispute.

4.1.4 The code subscribers commit themselves to raise awareness of consumer rights.

4.2. Pre-contractual information

4.2.1 The code subscribers shall describe the main characteristics of services offered, which is sufficient to enable a consumer to make an informed decision on the proposed service or transaction.

4.2.2 If a code subscriber delivers services using the app, then the provider needs to make available to the consumer the terms of using that app.

4.2.3 The code subscribers shall provide a total price of the service, including all contingent fees and penalties, before entering into a contract.

4.2.4 The code subscribers shall clearly explain the circumstances that trigger contingent fees and penalties before the customer enters into a contract.

4.2.5 The code subscribers that rely on third-party providers/intermediaries shall include the commission or the intermediary's fee in their service's total price. Alternatively, they shall provide customers with clear notice that other charges may apply.

4.2.6 The code subscribers that offer digital loans, in particular, shall provide their customers with:
a) the information necessary to decide on borrowing;
b) give the customer with clear and unambiguous information on the total cost of the digital loan, the method of repayment of the digital loan, as well as the consequences resulting from a possible failure to fulfill obligations under the digital loan agreement;
c) at the customer's request, provide explanations regarding the provisions contained in the digital loan agreement.

4.3 Withdrawal rights

4.3.1 The code subscribers shall also provide a customer with an opportunity—
a) to review the entire electronic transaction;
b) to correct any mistakes; and
c) to withdraw from the transaction before confirmation.

4.4 Access to the personal record and payment notification

4.4.1 The code subscribers that process transactions and payments shall notify their customers via SMS, app notification, or email once the payment has been executed.

4.4.2 Upon request, code subscribers will provide their customers a complete record of their transactions, loans, and other products and services.

4.4.3 The code subscribers shall, upon request, make accessible information concerning individual payment transactions or loans and aggregate amounts. The release of information must be according to the law and needs to be authorized by the data subjects.

4.5 Customer complaints

4.5.1 The code subscribers are required to adopt internal procedures to respond to customer complaints. To this end, code subscribers shall provide customers with all necessary contact details and information about the complaint procedure.

4.5.1.1 The code subscriber has a dedicated staff member to handle customer complaints and has created a customer complaints guidebook for staff members to follow.

4.5.1.2 The code subscriber has at least two forms of receiving a complaint (mail, email, online form, text message, phone call, customer representatives). At least one of the forms of complaints needs to be an online form to receive customer complaints. The forms to receive customer compliant should be fully functional and accessible at all times.

4.6 Advertising

4.6.1 The code subscribers shall ensure that their advertisements are transparent, fair, and not misleading.

4.6.2 The code subscribers shall ensure that their offers and marketing activities meet the accepted market standards, particularly the readability and quality of the advertising message.

4.6.3 The code subscribers shall ensure that their advertising material accurately reflects risks associated with the product or service being offered.

4.6.4 The code subscribers shall refrain from intentionally using the lack of knowledge or experience of customers to offer unsolicited products or services.

4.6.5 The code subscribers that offer digital loans, in particular, shall refrain from offers and advertisements which result in excessive debt of their customers.

5. Cybersecurity and Data Protection

5.1 The resilience of IT systems

5.1.1 The code subscribers commit to establish and maintain well-functioning and resilient IT systems.

5.1.2 The minimum standards include VPNs and SSL certificates for secure transactions.

5.1.3 The code subscribers shall ensure that it protects customers' data against data theft and cybercrime, both internal and external threats.

5.1.4 In particular, code subscribers shall secure users' security credentials when accessing services digitally and authorizing transactions.

5.2 Data location

5.2.1 The code subscribers shall establish and maintain their primary data center concerning financial services offered in Uganda or another country with at least as stringent data protection laws and regulations as in Uganda if allowed by law.

5.2.2 The code subscribers shall store their data on an in-house server or public/private cloud provider with a data center and disaster recovery center, given that they have a backup of their data elsewhere.

5.3 Confidentiality of customer data

5.3.1 The code subscribers provide security measures necessary to process and store the customers' data with complete confidentiality and according to applicable law.

5.3.2 The code subscribers that process payments commit to design their payment algorithms to anonymize as much data as possible.

5.4 Data collection, usage, and storage

5.4.1 The code subscribers have to ensure that customers know the data being collected about them and ask customers for their consent to collect such data when they register at the website or on an app or otherwise open their account with the code subscriber.

5.4.2 The code subscribers must ensure that customers know how their data is being used and processed. The code subscribers should ask customers for their consent when they register at the website or on an app or otherwise open their account.

5.4.3 The code subscribers should let customers know where their data is being stored and ask customers for their consent when they register at the website or on an app or otherwise open their account.

5.4.4 The code subscribers that store customers' data should keep different information on the same customer in different databases and comply with other obligations laid down in Data Protection and Privacy Act.

5.5 Data disclosure

5.5.1 The code subscribers shall protect the privacy of customer information and not disclose information of a customer unless the disclosure is made in compliance with the law, an order of a court, or the customer's express consent.

5.5.2 If code subscribers rely on third-party providers or intermediaries, they may not provide them with customer data unless they receive explicit consent from the customer.

5.5.3 Suppose code subscribers rely on third-party providers or intermediaries to conduct due diligence of customers. In that case, code subscribers commit to conduct due diligence on data handling procedures of external service providers, which store or handle customer data.

5.5.4 The code subscribers refrain from manipulating data about their customers without their consent and commit to comply with other obligations set out in the Data Protection and Privacy Act.

6. Financial inclusion

6.1 The code subscribers commit to ensuring that financial services are accessible to all citizens and residents of Uganda, within the applicability of the law.

6.2 The code subscribers commit not to discriminate unfairly based on gender, age, ethnicity, place of residence, the status of literacy, citizenship, or other grounds unless required by law.

6.3 The code subscribers ensure that customers with reduced literacy fully understand the terms of using the company's service.

6.4 The code subscribers aim to translate the terms into local languages. The code subscribers explain in their compliance report which local languages they have employed.

7. Code administration, monitoring, and enforcement

7.1 Becoming a code subscriber

7.1.1 The Code of Conduct is voluntary. All full members and start-up members of the Financial Technology Service Providers Association may choose to comply with the conduct on their own volition if they are in the business of providing financial services.

7.1.2 Full members that provide advisory services (law firms, accountancy firms, consultancy firms) to financial technology service providers may also choose to comply with the code.

7.1.3 The code subscribers can indicate to FITSPA if they have outsourced services to other code subscribers. If the partner company has received the Certificate of Compliance, then the code subscriber can also apply for the same level certification.

7.2 Compliance monitoring

7.2.1 The code subscribers must report annually on the implementation of the code in their companies. The report needs to be signed by the CEO or the main principal of the company.

7.2.2 The code subscribers should report any changes in the business conduct which are not in line with the code or any changes of the responsible staff to the FITSPA secretariat.

7.2.3 The code subscribers must report any misconduct or violation of the Code of Conduct that they are aware of to the FITSPA board. This applies to violations by their staff members, competitors, or clients if they have subscribed to the Code of Conduct.

7.2.4 The reports are archived at the FITSPA office.

7.3 Complaint management and code enforcement

7.3.1 Upon receiving a notification of a violation, the Board appoints an independent third-party verifier (a reputable law firm, accounting firm, or business consultancy which is by no means involved in the alleged violation or connected to alleged infringer utilizing ownership or control) to inquire about the violation. The alleged infringer has the right to submit to the investigating party. The independent third-party submits the report to the Board and the alleged infringer within one month. The alleged infringer has the right to respond to the allegations to the Board of FITSPA within two weeks.

7.3.2 Upon receiving the report and the alleged infringer's response, the Board votes on whether the allegation is sustained. The Board will communicate its decision to the alleged infringer within one month.

7.3.3 The Board has the option to:

a) Reject the allegation of violation as ungrounded.
b) Issue a warning to the infringer with a deadline and a plan of action for remedying the violation.
c) Suspend the permission to display the Certificate of Compliance until the alleged infringer remedies the violation.
d) Suspend the membership in FITSPA until the alleged infringer remedies the violation.
e) Terminate the membership if the alleged infringer does not remedy the violation.
f) Report the violation to the competent regulator.

7.4 Evolution of the Code of Conduct

7.4.1 The Board of FITSPA ensures the continuous development of the code.

7.4.2 The Board of FITSPA appoints a Code Development Committee comprising FITSPA members. This committee will formulate the amendments to the code necessitated by changes in the

context [technological or regulatory developments]. The working group will come up with changes or additions for the Board to approve.

7.4.3 The Working Groups have the role of providing a forum to share best practices and improve industry standards.

7.4.4 All FITSPA elected officials and staff members commit themselves to confidentiality regarding any information received through the reporting requirements laid down in this Code of Conduct. They commit themselves to refrain from using any of the information for their business purposes.

7.4.5 The code subscribers aspire to adhere to the code, a prerequisite to access databases for customer verification maintained by the Government of Uganda, for instance, the National ID Database.

7.4.6 The FITSPA Board regularly discusses industry standards with both regulators and FITSPA members and conducts roundtables with relevant stakeholders.

Appendix 1: Compliance report structure

Compliance report			
FinTech name			
Periodicity	Annual	**Period**	2021-22
Attributes	**Compliance (Yes/No)**	**Remarks (if any)**	
Business conduct and governance			
A license issued by the competent authority, or if no specific licensing regime exists, with respect to any other applicable law.			
Disclose information about their license (if applicable) and business contact details on their website. Suppose, instead of having a license, the code subscribers have partnered with another licensed institution (e.g., bank or mobile network operator or others). In that case, they should publish information about their partnership on their website.			
Comply with all applicable regulations governing their business.			
Have in place operational risk management and business continuity procedures.			
Ensure that the third-party provider is guided by customers' interests, performs professional activities according to their best knowledge, in a reliable manner and with due diligence, and respects the obligations arising out of laws and regulations.			
Establish safeguard measures to protect the funds deposited on their account from risks that may occasion loss to the funds' beneficiaries.			
Not commingle the funds deposited by clients with any other funds.			
List in the compliance report to FITSPA any possible conflict of interest between owners or staff members and the interest of consumers.			
Have mechanisms in place to prevent fraud or unlawful usage of their services.			
Have in place a specially designed transaction verification system, e.g., verification number sent to a customer's phone via SMS.			
Prescribe the manner of recovering an equivalent amount of transfer arising from a payment instruction or settlement made in the case of fraud, mistake, error, or similar vitiating factors.			
…… ….. …… …..			

Appendix 2: Best practices

Applicable section	Requirement
Section 3.2 Regulatory compliance	The code subscriber has a designated staff member in charge of regulatory compliance.
Section 3.3 Risk management and business continuity procedures	The code subscriber has a designated staff member in charge of risk management and business continuity.
Section 3.5 Holding customers' funds	The code subscriber uses an escrow account held in a supervised Financial Institution [as defined in the Financial Institutions Act 2004] to safeguard funds held in trust on behalf of the consumer.
Section 3.6 Professional standards	The code subscriber has an internal system of educating and training the staff.
Section 3.8 Fraud prevention	The code subscriber shall have a designated staff member for the proactive detection, mitigation, and early resolution of fraud.
	The code subscriber cooperates with other code subscribers on setting up a voluntary database of commercial clients who have committed fraudulent behavior on a digital platform.
Section 3.10 KYC and AML/CFT	The code subscriber has two or more identifiers [passport, identity number, driving license number, mobile phone number] to approve, verify, dedupe, and authenticate customers.
	The code subscriber shall designate an AML compliance officer.
Section 3.12 Cessation of business	The code subscriber has a company designated that could honor the legal obligations towards consumers after the cessation of the business.
Section 4.2 Pre-contractual information	The code subscriber has a webpage for each product or service offered, explaining the benefits, costs, and risks of using the product or service.
	The code subscriber has a separate page on the website or within the app, which lists all the services and associated costs and fees.
Section 4.5 Customer complaints	The code subscriber has a dedicated staff member to handle customer complaints and has created a customer complaints guidebook for staff members to follow.
	The code subscriber has at least two forms of receiving a complaint (mail, email, online form, text message, phone call, customer representatives). At least one of the forms of complaints needs to be an online form to receive customer complaints.
	The code subscriber replies to customer complaints within 48 hours. In case of delays, the code subscriber needs to swiftly communicate to the customer regarding the delay.
	The code subscriber aggregates summary of the complaints as follows: a) Number of complaints received; b) Number of complaints resolved; c) Number of complaints resolved within 48 hours; and d) Number of complaints resolved beyond 48 hours
Section 5.1 The resilience of IT systems	The code subscriber adheres to the cybersecurity ISO standard.
	The code subscriber has a dedicated staff member to monitor IT systems and cybersecurity.
	The code subscriber has a training program to educate staff about the technological development of IT systems and cybersecurity.
Section 5.3 Confidentiality of customer data	The code subscriber ensures that access to databases containing the customer's sensitive personal data is only possible by at least two people jointly.
Section 5.4 Data collection, usage, and storage	The code subscriber provides customers with a possibility to request information in electronic form about all data that the company has collected about them.
Section 6. Financial inclusion	The code subscriber has a financial literacy program or financial inclusion program in place. The code subscriber can cooperate with other members on the financial literacy or financial inclusion program.

Appendix 3: Applicable regulations governing the FinTech businesses in Uganda

The National Payments System Act, 2020

The National Payments Systems Regulations, 2021

The Anti-Money Laundering (Amendment) Act, 2017

The Electronic Signatures Act

The Uganda Communications Act, 2013

The Data Protection and Privacy Act, 2019

The Registration of Persons Act, 2015

The Electronic Transaction Act, 2011

The National Information Technology Authority Uganda Act, 2009

The Tier 4 Microfinance Institutions Act and Moneylenders Act, 2016 (if applicable)

The Capital Markets Authority Act (if applicable)

The Insurance Act (if applicable)