INCLUSIVE DIGITAL FINANCIAL SERVICES
A REFERENCE GUIDE FOR REGULATORS

July 2019

BILL & MELINDA GATES foundation

DISCLAIMER

This work is provided as-is, without any warranty of any kind, and for non-commercial, informational use only. Any further use may require the consent of third-party content owners. The materials are not intended to convey or constitute legal advice. You should not act upon any such information without first seeking qualified professional counsel on your specific matter.

ACKNOWLEDGMENTS

This resource has been created in consultation with individuals from numerous organizations, including (in alphabetical order) the Alliance for Financial Inclusion, the Consultative Group to Assist the Poor (CGAP), the United Nations Capital Development Fund, the Office of the United Nations Secretary General's Special Advocate for Inclusive Finance for Development, and the World Bank, and was developed with funding from the Bill & Melinda Gates Foundation. Principal drafting of this resource was led by consulting firm BFA, overseen by Jeremiah Grossman of BFA.

Contributors offered their advice and insight in their personal capacities. Any opinions expressed in this resource do not necessarily reflect the official views of any of the aforementioned organizations.

CONTENTS

INTRODUCTION

1 DFS and Financial Inclusion

2 Basic DFS Enablers

1 | DFS and Financial Inclusion

2 | Basic DFS Enablers

1 DFS AND FINANCIAL INCLUSION

- Evidence from many countries demonstrates the positive impact that the development of digital financial services (DFS) has on financial inclusion.

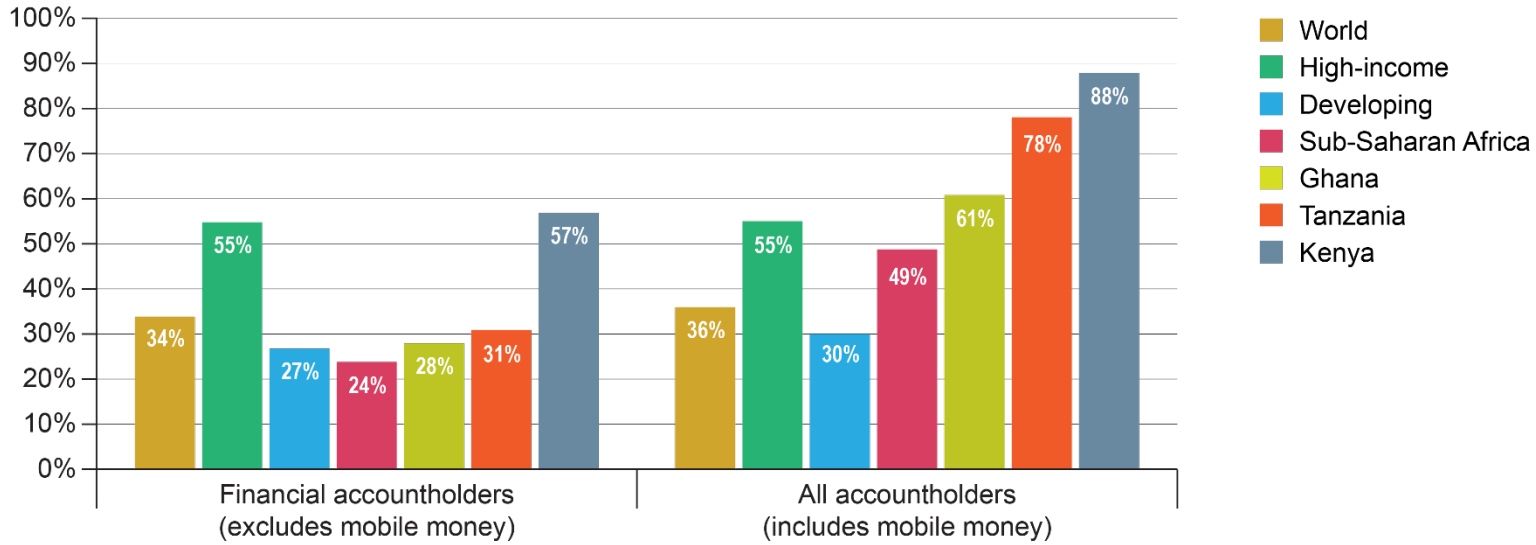
- Both banks and nonbanks (such as electronic money issuers) are playing an important role in fostering financial inclusion through DFS.

- Widespread uptake of basic DFS such as electronic money (e-money) can play an important role in expanding access to other financial services, such as credit, savings, insurance, and investment.

1 DFS AND FINANCIAL INCLUSION

USERS IN LOW-INCOME COUNTRIES ARE ADOPTING DFS

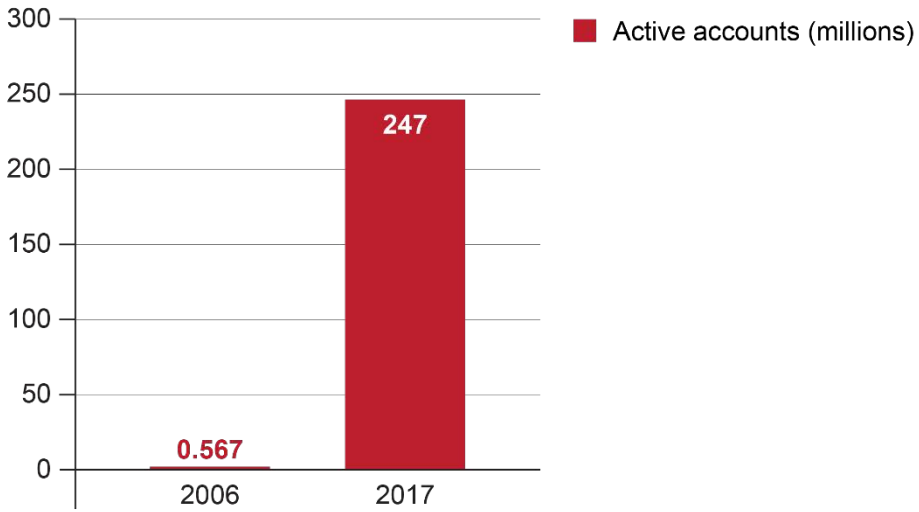
Used a mobile phone or the Internet to access an account, 2017 (% of accountholders)



Source: World Bank (2018)

1 | DFS AND FINANCIAL INCLUSION
GLOBAL ADOPTION OF DFS IS RISING

Active mobile money accounts (millions)

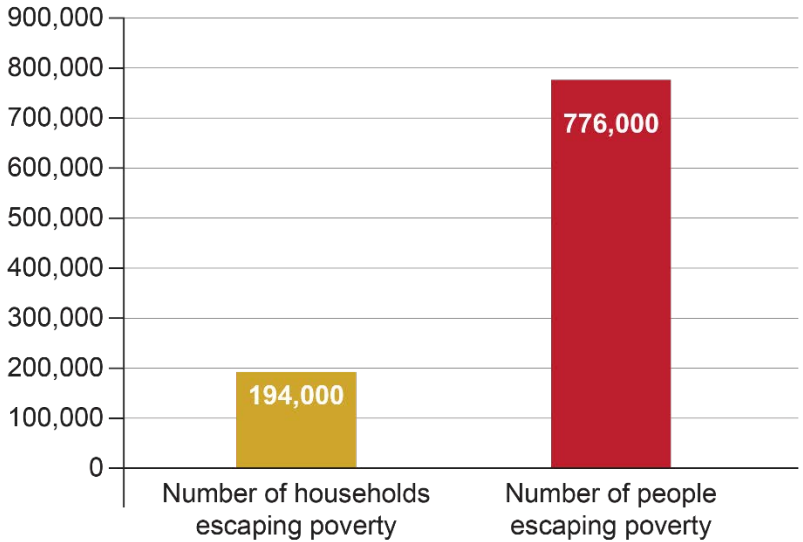


Source: GSMA (2017); GSMA (2018).

1 | DFS AND FINANCIAL INCLUSION
IMPACT OF DFS ON POVERTY

From 2008-2014, adoption of mobile money helped approximately 2% of all Kenyan households escape poverty.

Kenyans escaping poverty through adoption of mobile money, 2008-2014



Source: Suri & Jack (2016).

INDIA: REGULATORY REFORMS TO ENABLE DFS

2006

Agent

Agent regulations

2013

Client

Proportionate e-KYC for account opening

2015

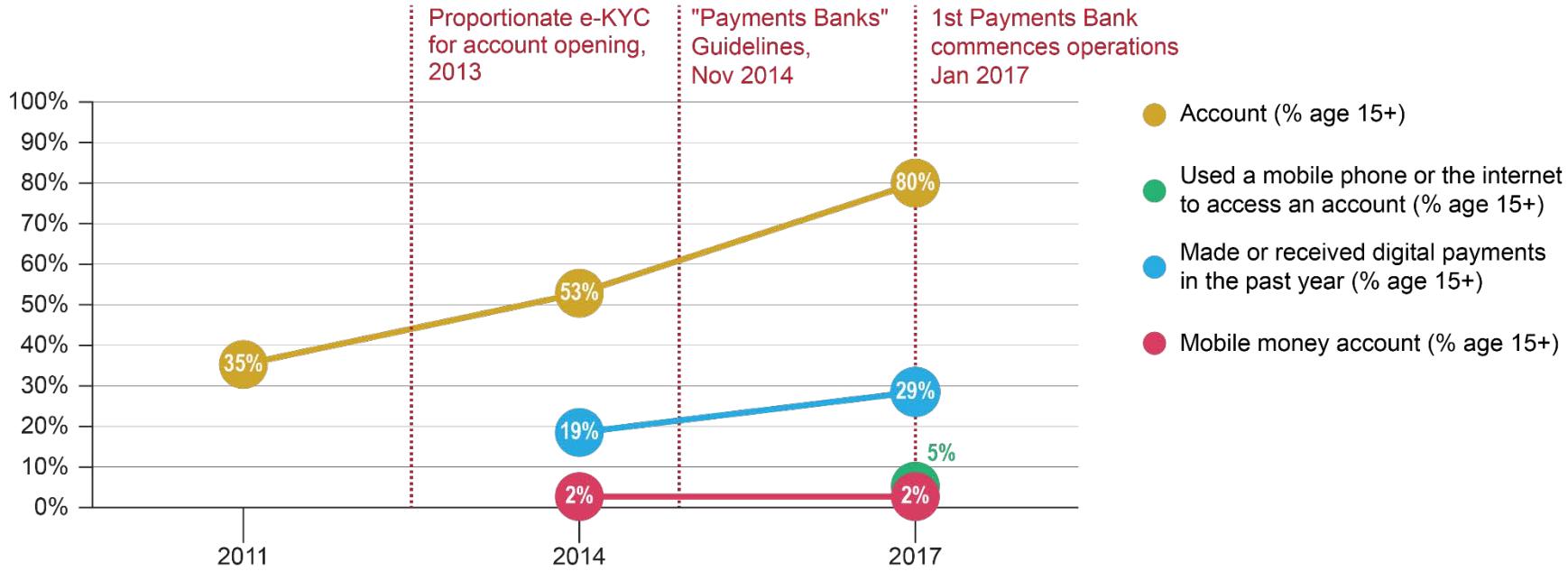
Issuer

Licensed new “payments banks”

Source: Chen (2017) (unpublished)

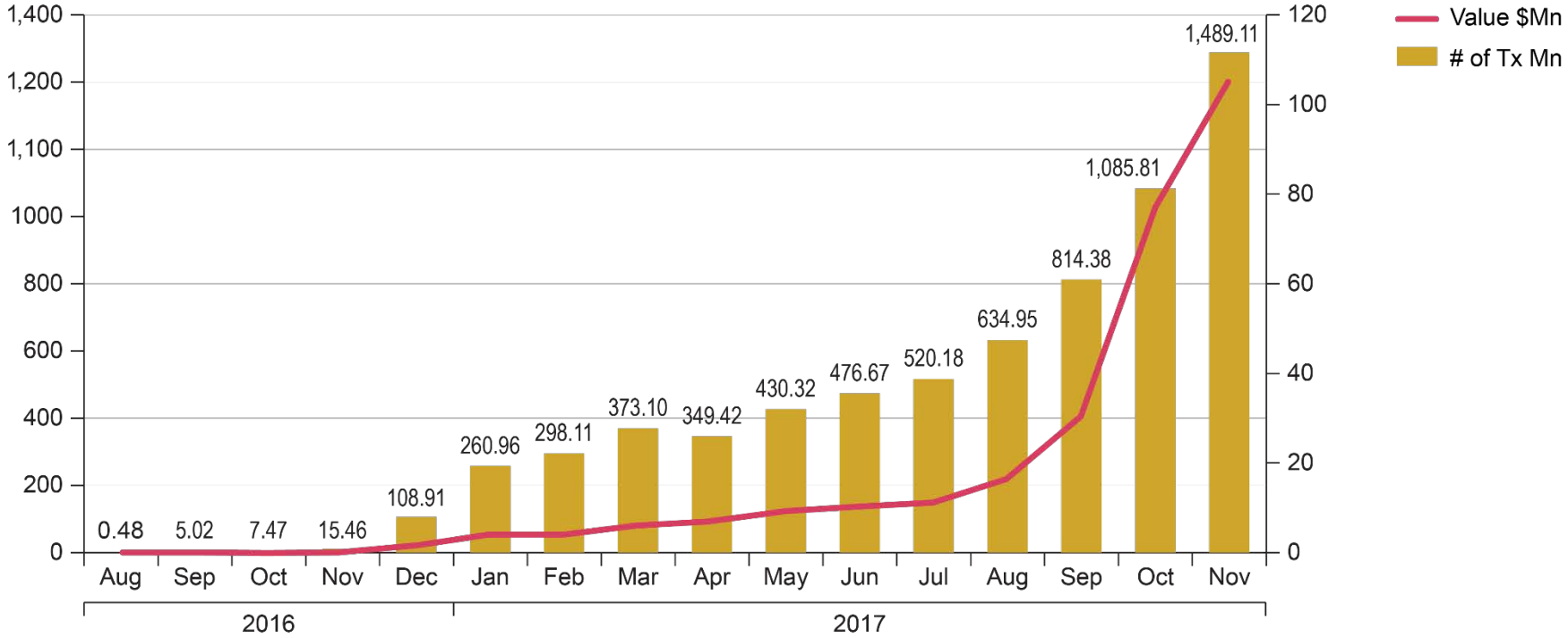
INDIA | COUNTRY EXAMPLE

Evolution of Financial Inclusion and DFS



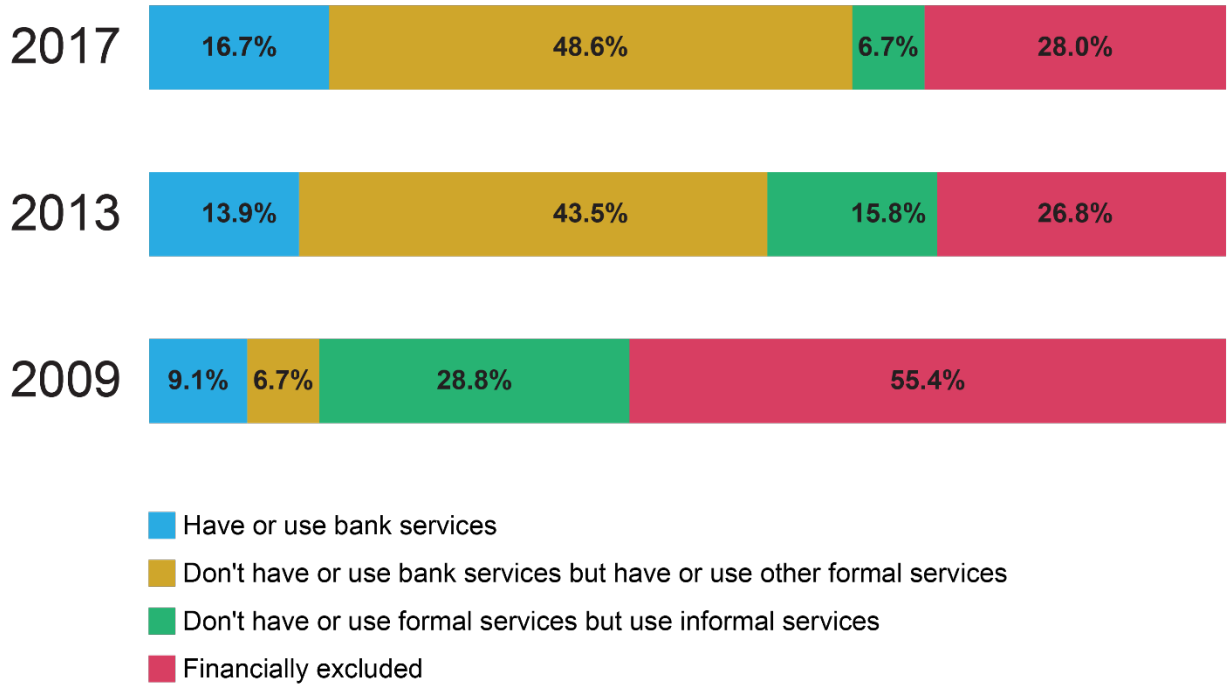
Source: World Bank (2018)

INDIA | REGULATORY REFORMS ARE DRIVING DIGITAL PAYMENTS ADOPTION



Source: Chen (2017) (unpublished)

TANZANIA | MOBILE MONEY IS DRIVING FINANCIAL INCLUSION



Source: FSDT (2017)

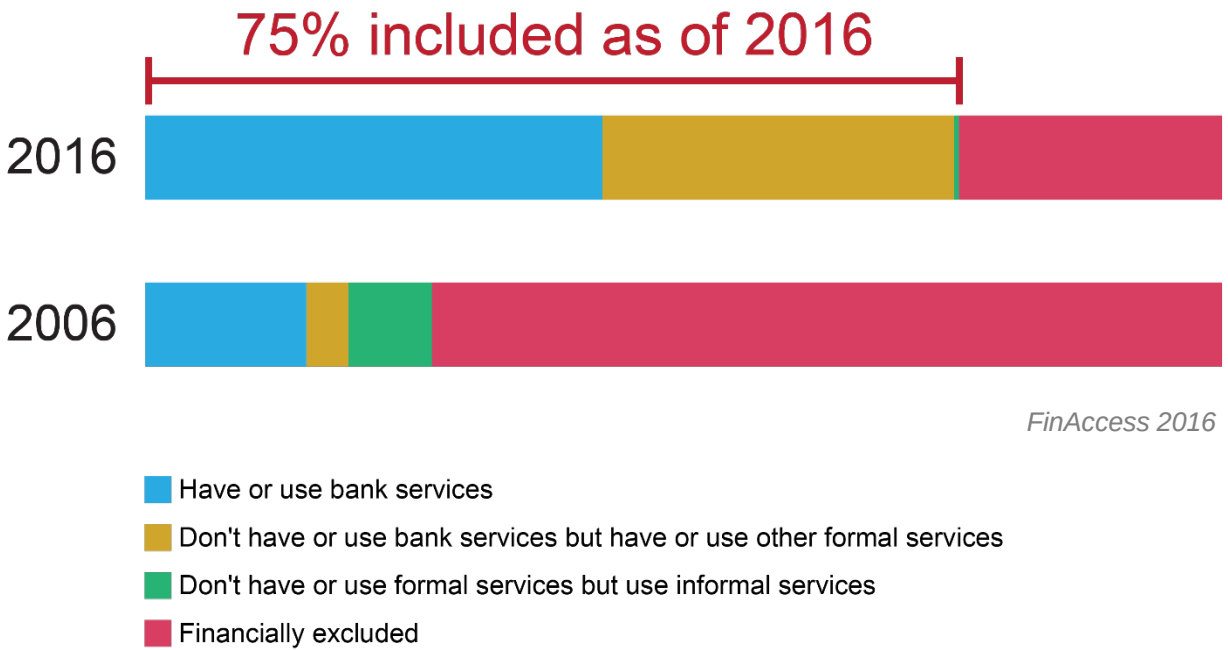
GHANA | MOBILE MONEY IS DRIVING FINANCIAL INCLUSION

	2012	2018
Registered Mobile Money Accounts	3.8 million	30 million
Active Mobile Money Accounts	345,000	11.8 million
Total Population 15+	15.9 million	18.2 million
% 15+ Population with Active Mobile Money Account	2%	65%

% 15+ population with an account increased from 29% (2011) to 58% (2017).

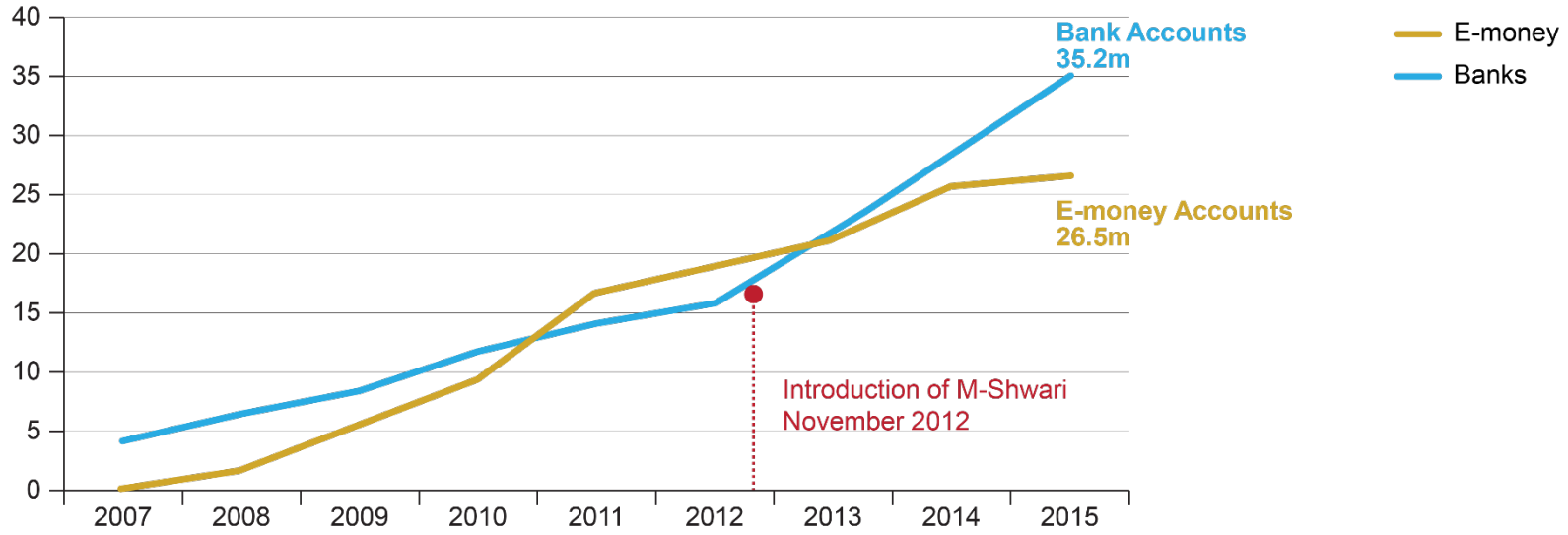
Source: B&FT Online (2018); World Bank (2018)

KENYA | MOBILE MONEY IS DRIVING FINANCIAL INCLUSION



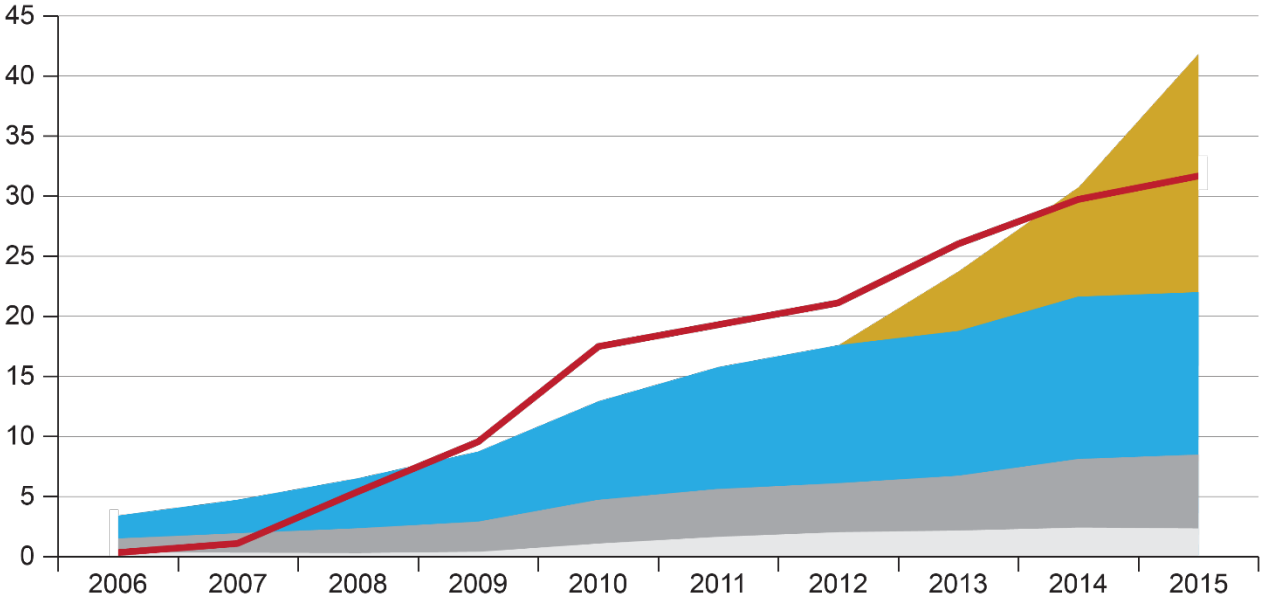
Source: FSDK (2016); Chen (2017) (unpublished)

KENYA | MOBILE MONEY AS A STEPPING STONE TO FULL BANK ACCOUNTS (CREDIT & SAVINGS)



Source: Chen (2017) (unpublished)

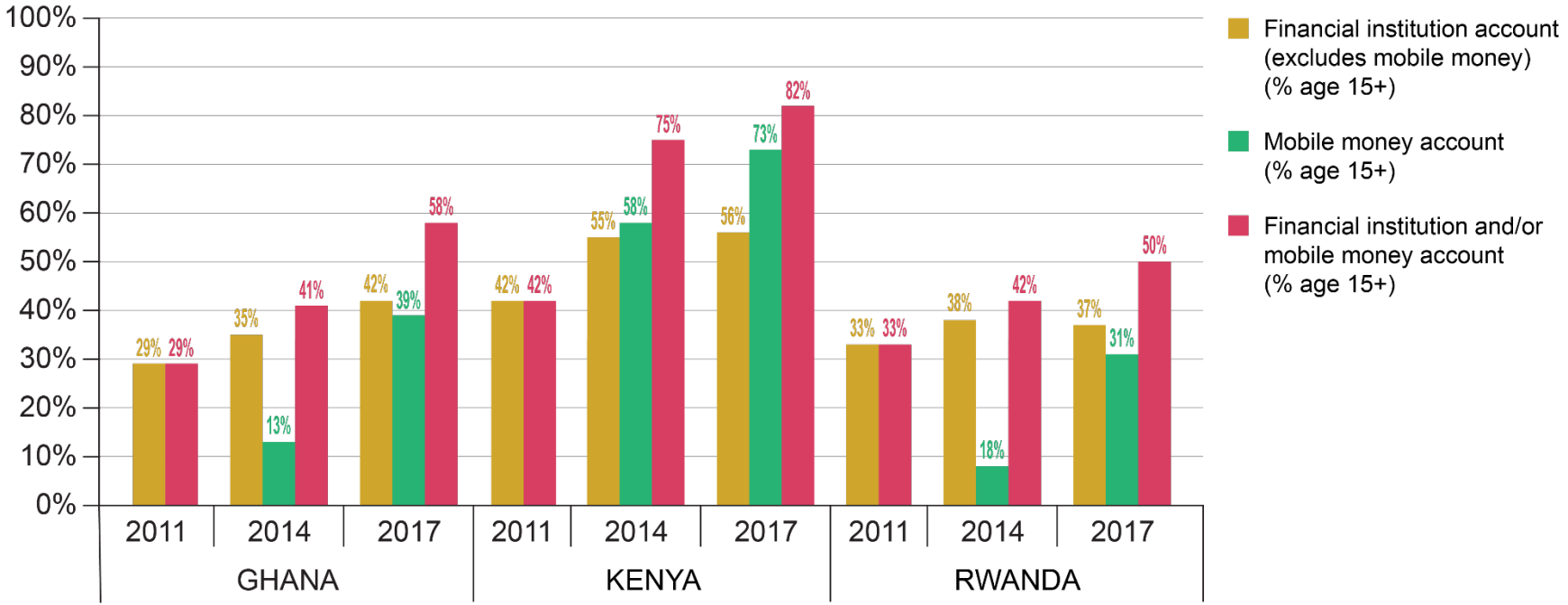
KENYA | MOBILE MONEY AS A STEPPING STONE TO FULL BANK ACCOUNTS (CREDIT & SAVINGS)



Separating traditional (blue) bank accounts from digital (gold) bank accounts, it becomes even clearer that new models are driving the growth.

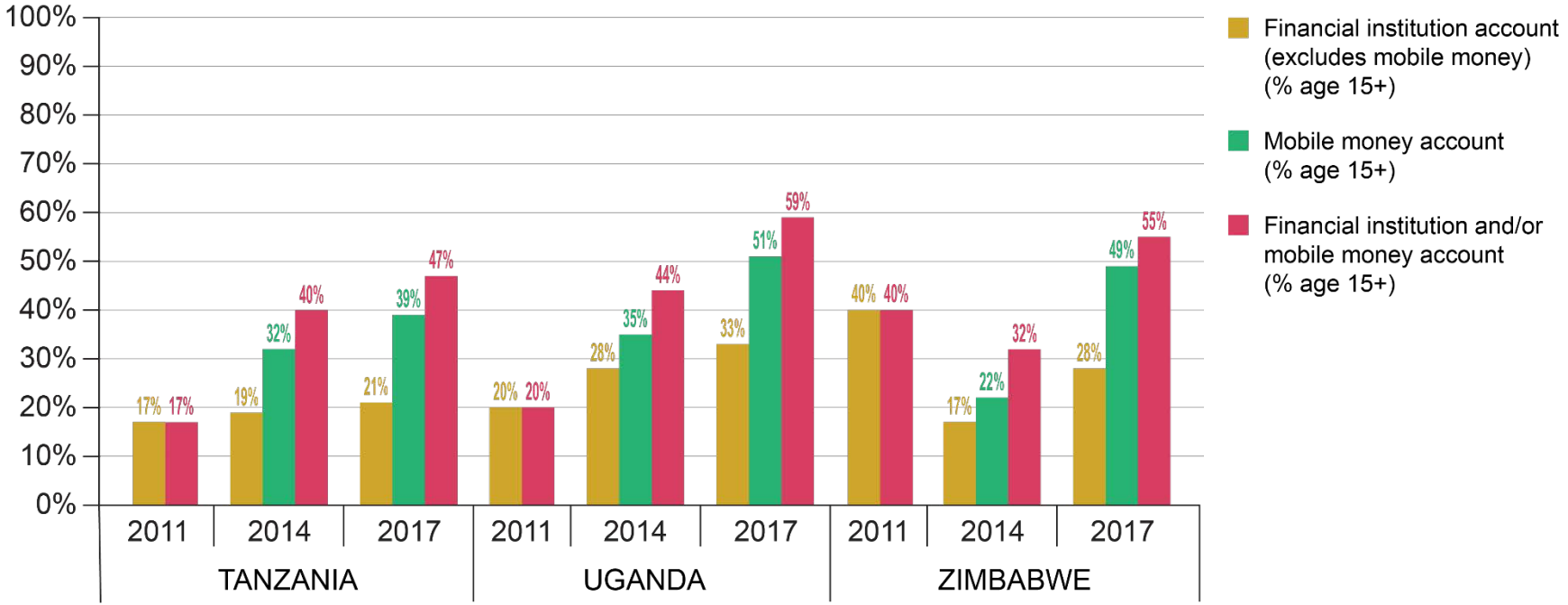
Source: Chen (2017) (unpublished)

IMPACT OF MOBILE MONEY ADOPTION ON BANK ACCOUNT ADOPTION



Source: World Bank (2018)

IMPACT OF MOBILE MONEY ADOPTION ON BANK ACCOUNT ADOPTION



Source: World Bank (2018)

1 DFS and Financial Inclusion

2 Basic DFS Enablers

1 DFS and Financial Inclusion

2 Basic DFS Enablers

Issue

The overarching legal frameworks for payment system and banking regulation impact the permissible legal models for e-money and similar DFS. The absence of clear, enabling legal frameworks typically limits innovation.

Key issues to consider

- **Legality of electronic payment instruments:** Are electronic payment instruments clearly legal?
- **Permissibility of e-money issuance by nonbanks:** Can non-banks legally offer e-money and similar DFS?
- **Mechanisms for licensing e-money issuers (EMIs):** How can regulators license provision of e-money and similar DFS by non-banks?
- **Ability to use agents:** Can banks and non-banks use agents to provide access to DFS?

2 BASIC DFS ENABLERS

Country examples: Legality of electronic payment instruments

Malawi

Prior to the passage of the Payment Systems Act, 2016, Malawi's payment system was still regulated under the Bills of Exchange Act, 1967. Under this Act, only cash and checks were accepted as legal means of payment. While the Reserve Bank of Malawi had approved various forms of DFS prior to the passage of the Payment Systems Act, as recently as 2008 this was cited by providers as a source of legal risk when considering offering branchless banking, e-money, or other DFS.

Source: World Bank (2010)

2 BASIC DFS ENABLERS

Country examples: Permissibility of e-money issuance by nonbanks

Restrictive interpretation → **Liberal interpretation**

South Africa

The Banks Act, 2007 limits deposit-taking to banks and includes a broad definition of "deposit-taking" that would appear to encompass cash-in activities. The South African Reserve Bank has interpreted the Banks Act to limit e-money issuance to banks.

19% sent or received domestic remittance via mobile phone, 2017
(% age 15+)

Source: World Bank (2018)

Namibia

While the Banking Institutions Act, 1998 also limits deposit-taking to banks and includes a broad definition of "deposit-taking", the Bank of Namibia permitted non-bank e-money issuance by treating cash-in as an advance payment for services to be rendered. The Determination on Issuing of Electronic Money expressly states that e-money funds are not deposits.

42% sent or received domestic remittance via mobile phone, 2017
(% age 15+)

Source: World Bank (2018)

2 BASIC DFS ENABLERS

Country examples: Mechanisms for licensing EMIs

Greater role for bank partner → **Lesser role for bank partner**

Uganda

Under Mobile Money Guidelines, 2013, Bank of Uganda grants "no objection" to licensed partner bank as a bank product provided in partnership with non-bank "mobile money service providers".

Tanzania

Prior to passage of National Payment Systems Act, 2015, Bank of Tanzania provided "letter of no objection" to partner bank and MNO partners. Since 2015, nonbanks are licensed directly as e-money issuers under E-Money Regulations, 2015.

Source: di Castri & Gidvani (2014)

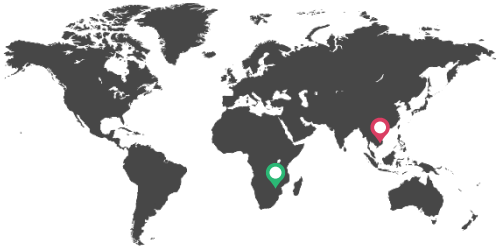
Kenya

Prior to passage of National Payment System Act, 2011 and National Payment System Regulations, 2014, Central Bank of Kenya provided "letter of no objection" directly to MNO to offer e-money services. Since 2014, nonbanks are licensed directly as e-money issuers under NPS Regulations, 2014.

Source: GSMA (2015)

2 BASIC DFS ENABLERS

Country examples: Ability to use agents



Restrictive interpretation → **Liberal interpretation**

Viet Nam

The Law on Credit Institutions states that only licensed credit institutions may conduct banking operations. The State Bank of Viet Nam has interpreted this to mean that banks are prohibited from offering cash-in and other services through agents.

2% sent or received domestic remittance via mobile phone, 2017
(% age 15+)

Source: World Bank (2018)

Zambia

While the Banking and Financial Institutions Act, 1995 contained similar language limiting the conduct of banking services to licensed banks, the Bank of Zambia concluded that this did not prevent a bank from using agents to accept deposits and other services on the bank's behalf.

29% sent or received domestic remittance via mobile phone, 2017
(% age 15+)

Source: World Bank (2018)

LICENSING

1 | Licensing Models

2 | Country Examples

3 | Regulatory Domains of Telco & Financial Regulator

1 | Licensing Models

2 | Country Examples

3 | Regulatory Domains of Telco & Financial Regulator

1 | LICENSING MODELS FOR ELECTRONIC MONEY ISSUANCE

Licensing models for e-money and similar digital financial services (hereinafter, “e-money”) tend to fall into one of four categories:

Bank-Only

E-money may be provided only by licensed commercial banks

Limited Bank

E-money may be provided by banks or “limited banks”, which typically may accept deposits but have restrictions on intermediation of funds.

Bank-Based but Nonbank-Led

Legally, e-money may be issued only by banks, but in practice nonbanks are permitted to lead e-money schemes in partnership with banks.

Non-bank Special Purpose Vehicle (SPV)

E-money may be provided either by banks or licensed nonbank e-money issuers.

1 | BANK-ONLY LICENSING MODEL FOR E-MONEY ISSUANCE

Role in delivery of e-money service	Who plays this role?	
	Bank	Nonbank
License to issue e-money	✓	
Direct communication with regulator to request authorization for, e.g., new services or revised transaction limits	✓	
Contractual agreement with customer	✓	
Branding of e-money service	✓	
Delivery of e-money service (directly and/or through agent network)	✓	
Safeguarding customer funds	✓	

BANK-ONLY

Advantages

- Banks already licensed and supervised by financial authority
- May already have sophisticated risk management and AML/CFT systems
- Can use e-money as a stepping stone to additional banking services

Disadvantages

- Banks may be unable to establish a viable business case for poor and rural population segments
- May lack understanding of unbanked and underserved market
- Few examples of major contribution to financial inclusion

Examples

Bangladesh: bKash (bank subsidiary)

South Africa: FNB eWallet

1 | LIMITED BANK LICENSING MODEL FOR E-MONEY ISSUANCE

Role in delivery of e-money service		Who plays this role?	
		Bank	Nonbank
	License to issue e-money	✓	
	Direct communication with regulator to request authorization for, e.g., new services or revised transaction limits	✓	
	Contractual agreement with customer	✓	
	Branding of e-money service	✓	
	Delivery of e-money service (directly and/or through agent network)	✓	
	Safeguarding customer funds	✓	

LIMITED BANK

Advantages

- Offers a clear mechanism for direct central bank licensing and supervision
- Lower initial minimum capital requirements may facilitate equity investment by nonbanks

Disadvantages

- Minimum capital requirements and certain other prudential requirements may not be aligned well with the business model for e-money business

Examples

India: Paytm Payments Bank

Pakistan: EasyPaisa - Telenor Microfinance Bank

1 BANK-BASED BUT NONBANK-LED LICENSING MODEL FOR E-MONEY ISSUANCE

Role in delivery of e-money service	Who plays this role?	
	Bank	Nonbank
License to issue e-money	✓	
Direct communication with regulator to request authorization for, e.g., new services or revised transaction limits	✓	
Contractual agreement with customer	✓	
Branding of e-money service		✓
Delivery of e-money service (directly and/or through agent network)		✓
Safeguarding customer funds	✓	

BANK-BASED BUT NONBANK-LED

Advantages

- Enables central bank to directly supervise banks, while (in theory) enabling non-banks to lead in the design and branding of e-money services
- Some global examples of successful services

Disadvantages

- Nonbank still requires bank approval for new products and services, changes to account limits, etc.
- Lack of direct communication between financial authority and nonbank may increase risk of undetected operational and consumer protection abuses

Examples

Uganda: Airtel Money, MTN Mobile Money

1 NON-BANK SPECIAL PURPOSE VEHICLE (SPV) LICENSING MODEL FOR E-MONEY ISSUANCE

Role in delivery of e-money service	Who plays this role?	
	Bank	Nonbank
License to issue e-money		✓
Direct communication with regulator to request authorization for, e.g., new services or revised transaction limits		✓
Contractual agreement with customer		✓
Branding of e-money service		✓
Delivery of e-money service (directly and/or through agent network)		✓
Safeguarding customer funds	✓	

NON-BANK SPECIAL PURPOSE VEHICLE (SPV)

Advantages

- Most common regulatory approach in markets with high e-money adoption.
- Enables nonbanks to lead design, delivery, and branding of e-money services while also directly licensing and supervising them through an SPV.* These entities often have the experience, assets, and incentives to reach the mass market.
- Creates legal separation between e-money issuer and parent company.

* NOTE: Historically, many countries allowed nonbanks to issue e-money without establishing an SPV. Today, most countries require an SPV.

Disadvantages

- Financial authorities may have limited capacity to supervise additional entities and may lack understanding of risks specific to nonbank e-money issuance.
- MNOs may use control of telecoms channel to restrict access among competitors.
- May pose legal challenges around central bank supervisory powers over non-banks.
- May require financial regulator to coordinate with other regulators (e.g., telco regulator) to ensure effective supervision.

Examples

Brazil: Payments Institutions

China: Alipay

Nigeria: FirstMonie (bank), Paga (nonbank)

Tanzania: M-Pesa

USA: PayPal

1 Licensing Models

2 Country Examples

3 Regulatory Domains of Telco & Financial Regulator

1 Licensing Models

2 Country Examples

3 Regulatory Domains of Telco & Financial Regulator

Bank-Only

E-money may be provided only by licensed commercial banks

Limited Bank

E-money may be provided by banks or “limited banks”, which typically may accept deposits but have restrictions on intermediation of funds.

Bank-Based but Nonbank-Led

Legally, e-money may be issued only by banks, but in practice nonbanks are permitted to lead e-money schemes in partnership with banks.

Non-bank Special Purpose Vehicle (SPV)

E-money may be provided either by banks or licensed nonbank e-money issuers.

2 | COUNTRY EXAMPLE | BANGLADESH

Licensing Model & Prudential Requirements

Licensing Model: Bank-Only (either directly or through majority-owned subsidiary of a commercial bank. Minority ownership open to other banks, NBFIs, NGOs, investment or Fintech companies (but MNOs expressly excluded).

Protection of Customer Funds:

- 100% of customer funds must be invested in a combination of trust accounts in commercial banks and government securities.
- Deposit insurance may apply if MFS offered directly by bank. Does not apply to MFS offered by subsidiary.

Source: MFS Regulations (2018)

Prudential Requirements & Competition

Capital Requirements:

- **Initial:** BDT 450 million (USD 5.3 million).
- **Ongoing:** BDT 450 million (USD 5.3 million), rising to BDT 900 million (USD 10.7 million) over time.

Agent Exclusivity: Not specified.

USSD Access: As of April 2018, each successful session (up to 90 seconds) costs BDT 0.85 (USD 0.01) for transactions and BDT 0.40 (USD 0.005) for other services (e.g., check balance).

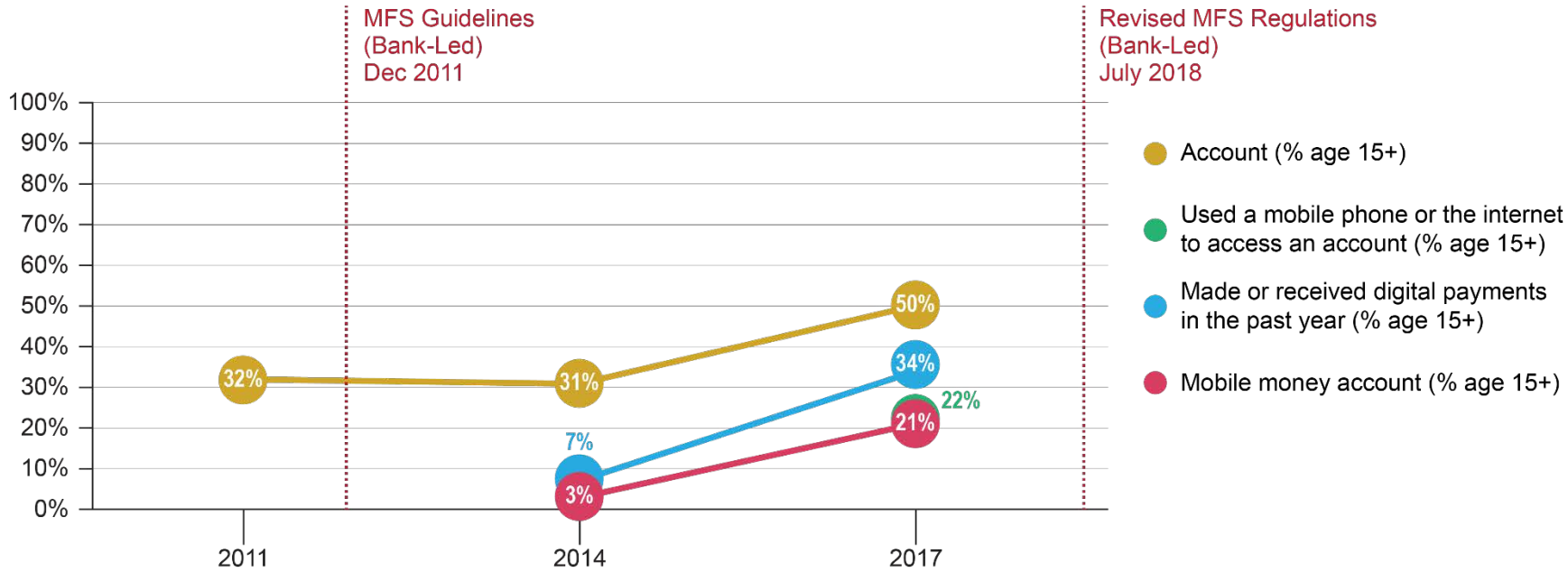
Interoperability: MFS Regulations call for MFS providers to collaborate to enable full interoperability across all MFS accounts and bank accounts.

Financial Inclusion & AML/CFT

Financial Inclusion: As of Aug 2018, draft NFIS under development was expected to be submitted in Oct 2018 for Cabinet approval and implementation in 2019.

KYC: Providers may query national ID database to verify ID cards. Full e-KYC system was launched in 2019 by Nagad.

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

Bank-Only

E-money may be provided only by licensed commercial banks

Limited Bank

E-money may be provided by banks or “limited banks”, which typically may accept deposits but have restrictions on intermediation of funds.

Bank-Based but Nonbank-Led

Legally, e-money may be issued only by banks, but in practice nonbanks are permitted to lead e-money schemes in partnership with banks.

Non-bank Special Purpose Vehicle (SPV)

E-money may be provided either by banks or licensed nonbank e-money issuers.

2 | COUNTRY EXAMPLE | INDIA

Licensing Model & Prudential Requirements

Licensing Model: Limited Bank (Payments Banks)

Protection of Customer Funds:

- At least 75% of customer funds must be invested in short-term government securities and up to 25% of customer funds may be held in commercial banks.
- Direct coverage by deposit insurance

Capital Requirements:

- **Initial:** INR 1 billion (USD 13.7 million)
- **Ongoing:** (1) 15% of risk-weighted assets; and (2) 3% leverage ratio

Source: RBI (2014); RBI (2016)

Competition & Financial Inclusion

Agent Exclusivity: Required for opening accounts, permitted for other services.

USSD Access: Telecoms Regulatory Authority established ceiling cost of INR 0.50 (USD 0.007) per USSD session and increased minimum number of stages from 5 to 8.

Interoperability: All Payments Banks are interoperable through connection to the interbank payment system managed by NPCI.

Financial Inclusion: Well-documented policies aimed at attaining universal access.

AML/CFT

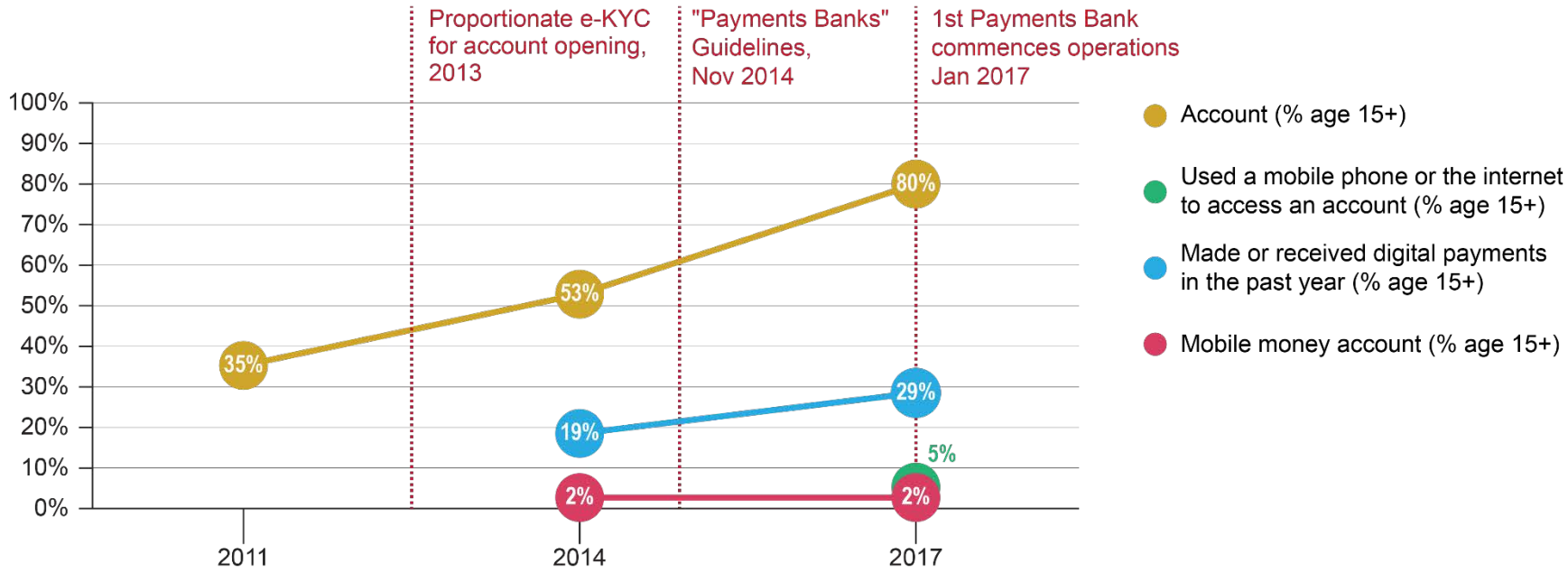
KYC: eKYC with biometric authentication (approx. 1/8 the cost of traditional KYC) possible through connection to Aadhaar national ID system.*

Account Limits: Max. balance of INR 100,000 (approx. USD 1,370)

* As of Jan 2019, the permissibility of using Aadhaar for e-KYC was uncertain following a decision by India's Supreme Court stating that requiring Aadhaar to open a bank account was disproportionate.

2 | COUNTRY EXAMPLE | INDIA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | MEXICO

Licensing Model & Prudential Requirements

Licensing Model: Limited Bank (Niche Banks)

Protection of Customer Funds: Direct coverage by deposit insurance, funds must be invested in liquid assets

Capital Requirements:

- **Initial:** MXN 215 million (USD 11.1 million)
- **Ongoing:** 8% of risk-weighted assets

Competition & Financial Inclusion

Agent Exclusivity: Permitted

USSD Access: Not specified

Interoperability: All banks are connected to the inter-bank electronic payments system (SPEI), and most mobile accounts are connected to SPEI.

Financial Inclusion: In 2016, Mexico launched a Financial Inclusion Strategy aimed at achieving full financial inclusion.

AML/CFT

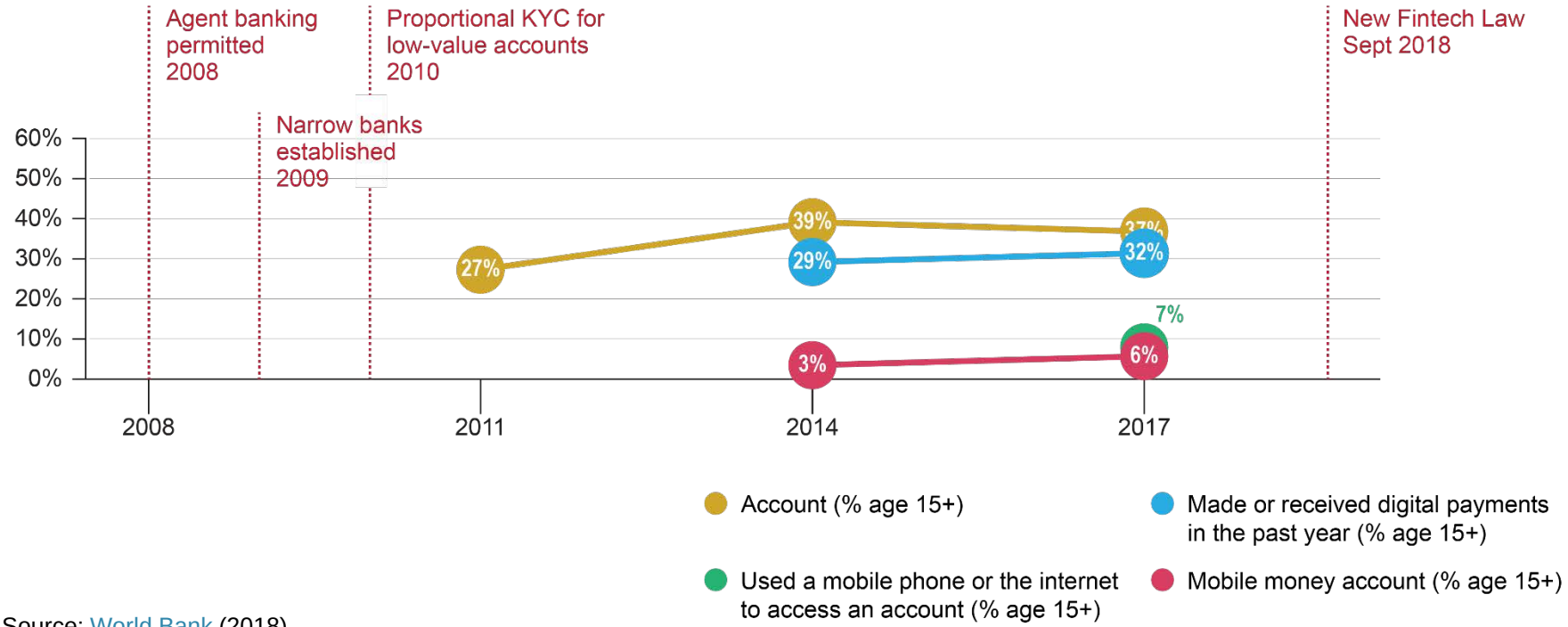
KYC:

- Accounts with aggregate monthly deposits of up to MXN 11,934 (USD 615): Full name, date of birth, and residential address.
- For all other accounts: Full KYC, including name, date and place of birth, nationality, address, phone number, e-mail, identity code, taxpayer code.

Source: SHCP (2009)

2 | COUNTRY EXAMPLE | MEXICO

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLES

Bank-Only

E-money may be provided only by licensed commercial banks

Limited Bank

E-money may be provided by banks or “limited banks”, which typically may accept deposits but have restrictions on intermediation of funds.

Bank-Based but Nonbank-Led

Legally, e-money may be issued only by banks, but in practice nonbanks are permitted to lead e-money schemes in partnership with banks.

Non-bank Special Purpose Vehicle (SPV)

E-money may be provided either by banks or licensed nonbank e-money issuers.

2 | COUNTRY EXAMPLE | UGANDA

Licensing Model & Prudential Requirements

Licensing Model: Bank-Based but Nonbank-Led (Mobile Money Service Providers)

Protection of Customer Funds: Funds equal in value to outstanding e-money issued must be held in an escrow account in one or more partner banks, with daily reconciliation. Funds may not be commingled and must remain unencumbered.

Capital Requirements:

- **Initial:** Not specified
- **Ongoing:** Not specified

Source: BoU (2013)

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: Not specified. MMSPs may not engage in practices that "*would be likely to substantially inhibit competition*."

Interoperability: Providers must use systems that are capable of becoming interoperable with other payment systems, but interoperability is not mandated.

Financial Inclusion: Bank of Uganda has a Financial Inclusion Project focusing on financial literacy, consumer protection, innovation, and data/measurement.

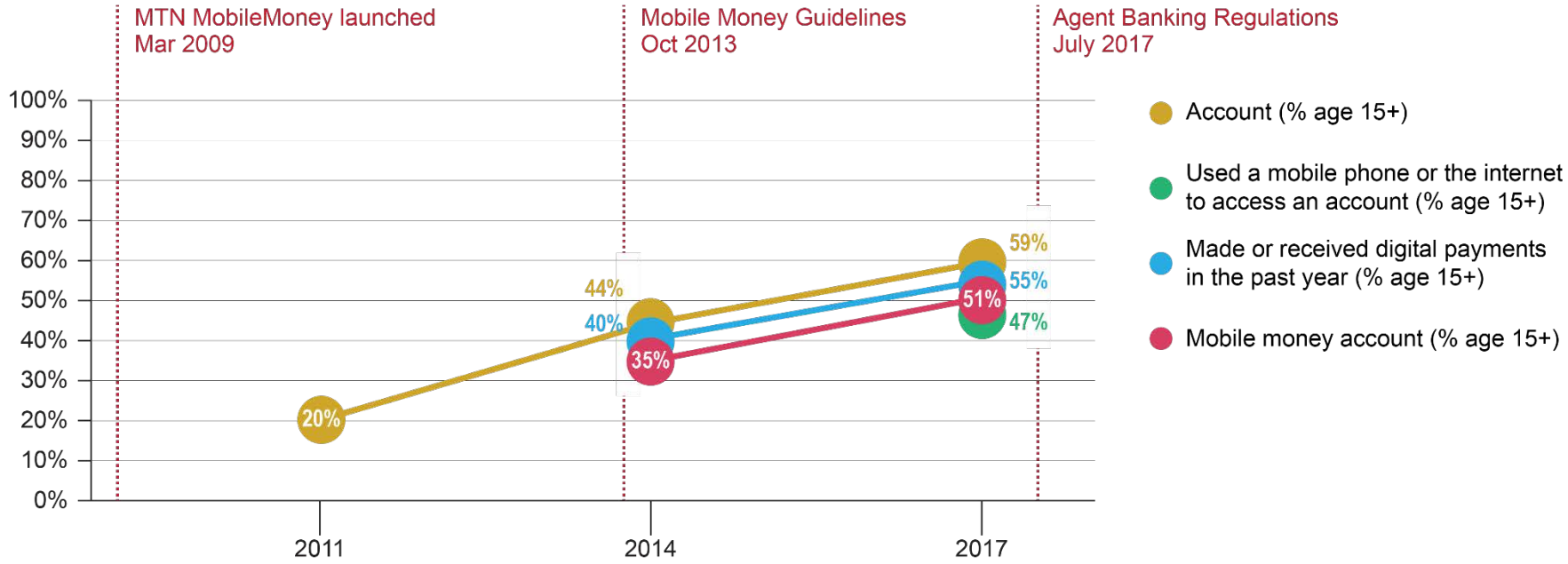
AML/CFT

KYC:

- **Mobile money accounts:** National ID number or national ID card (citizens), passport (non-resident foreign nationals), or refugee ID card (refugees).

2 | COUNTRY EXAMPLE | UGANDA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

Bank-Only

E-money may be provided only by licensed commercial banks

Limited Bank

E-money may be provided by banks or “limited banks”, which typically may accept deposits but have restrictions on intermediation of funds.

Bank-Based but Nonbank-Led

Legally, e-money may be issued only by banks, but in practice nonbanks are permitted to lead e-money schemes in partnership with banks.

Non-bank Special Purpose Vehicle (SPV)

E-money may be provided either by banks or licensed nonbank e-money issuers.

2 | COUNTRY EXAMPLE | BRAZIL

Licensing Model & Prudential Requirements

Licensing Model: Non-bank SPV (Payments Institutions)

Protection of Customer Funds:

Customer funds must be stored in Central Bank of Brazil or invested in government securities. Funds cannot be seized by creditors or used as collateral.

Capital Requirements:

- **Initial:** BRL 2 million (USD 540,000)
- **Ongoing:** Greater of (i) 2% of average monthly transaction value over the past 12 months; or (ii) 2% of outstanding liabilities.

Competition & Financial Inclusion

Agent Exclusivity: Permitted

USSD Access: E-money issuers must provide non-discriminatory access to payments infrastructure.

Interoperability: Interoperability is considered to be a key objective but is not initially mandated.

Financial Inclusion: In 2011, Brazil launched the National Partnership for Financial Inclusion (NPFI). In 2012, the NPFI published an Action Plan aimed at strengthening the institutional environment for financial inclusion.

AML/CFT

Simplified KYC:

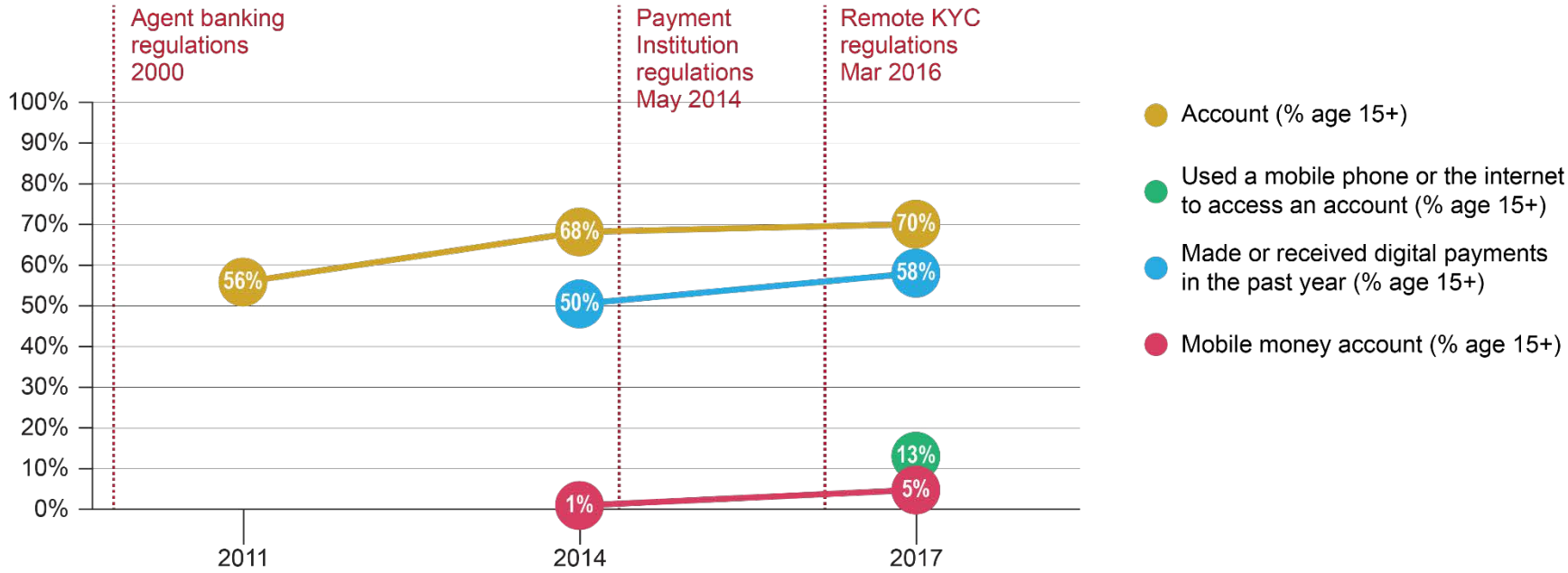
- Full name and Registration number from Registry of Natural Persons

Full KYC:

- Full name
- Mother's full name
- Date of birth
- Registration number
- Residential address
- Phone number

Source: BCB (2013)

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | COLOMBIA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (Specialized Deposit and Electronic Payment Companies, SEDPEs)

Protection of Customer Funds: Funds equal in value to outstanding e-deposits must be held in current accounts in the Central Bank or another financial institution. These funds are covered by direct deposit insurance.

Capital Requirements:

- **Initial:** COP 6.94 billion (USD 2.2 million) as of Jan 2018
- **Ongoing:** 2% of average outstanding electronic deposits

Competition & Financial Inclusion

Agent Exclusivity: Permitted

USSD Access: MNOs with SEDPE subsidiaries must offer non-discriminatory channel access. In addition, other operators of low-value payment systems must make their infrastructure (e.g., ACH, ATMs, PoS devices) available to SEDPEs on non-discriminatory terms.

Interoperability: No explicit interoperability mandate.

Financial Inclusion: In 2014, Colombia launched its National Financial Inclusion Strategy and passed a Financial Inclusion Law.

AML/CFT

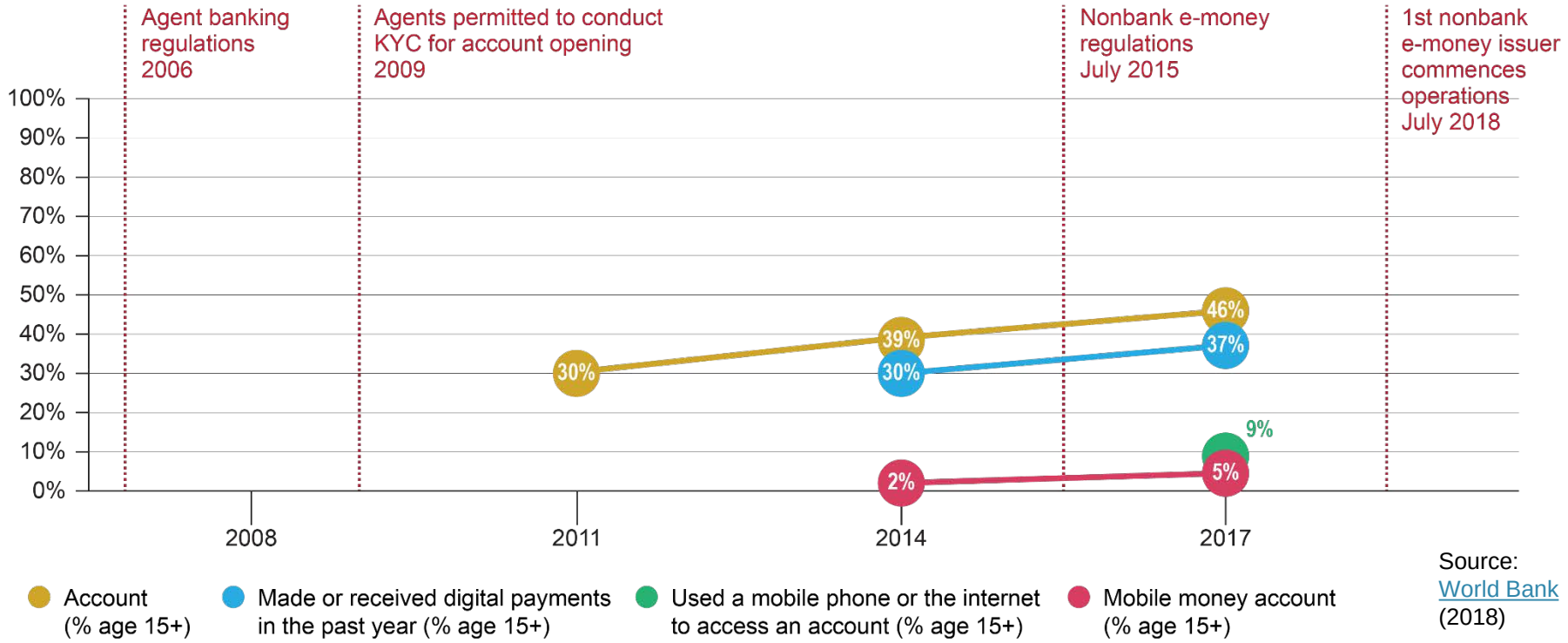
KYC:

- **Simplified electronic deposit accounts:** Name; type of identity document; number of identity document; expiration date of identity document.
- **Ordinary deposit accounts:** Name; type, number, and expiration date of identity document; place and date of birth; home phone and address; occupation/description of primary economic activity; workplace contact info; income, expenses, assets, and liabilities; signature, fingerprint, and date.

Source: *Ley No. 1735* (2014); *Decreto 1491* (2015)

2 | COUNTRY EXAMPLE | COLOMBIA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | EUROPEAN UNION

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Funds: Two options:

1. Funds must be held in a separate account or invested in low risk assets. Funds may not be commingled and must be insulated from creditor claims in event of insolvency.
2. Funds must be covered by insurance or guarantee for equivalent amount.

Capital Requirements:

- **Initial:** EUR 350,000 (USD 400,000)
- **Ongoing:** 2% of average outstanding liabilities

Competition & Financial Inclusion

Fintech Access: Payment aggregators and payment initiators are subject to lesser regulation requirements and may access customer data from banks (XS2A). In addition, data portability further bolsters Fintechs' ability to compete.

Interoperability: E-money interoperability not mandatory but is possible through credit card rails or Single European Payments Area (SEPA) instant payment scheme.

Financial Inclusion: The Payment Accounts Directive gives all EU citizens the right to open a basic payment account.

AML/CFT

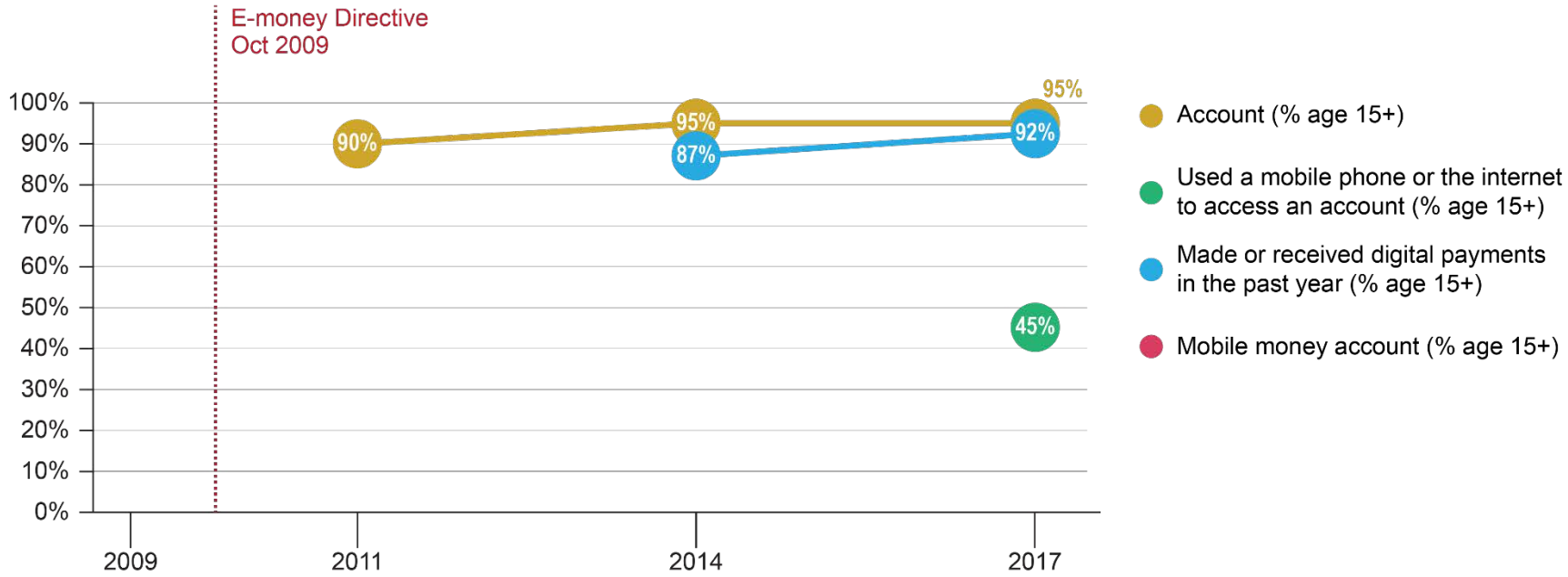
KYC: Exemption for e-money products from certain KYC requirements if products are used exclusively for purchase of goods/services and balance is less than EUR 250 (USD 285). In addition, EU Member States can implement simplified due diligence for certain low-risk e-money products.

Account Limits: Can be set by individual EU member states in their implementing legislation.

Source: E-Money Directive (2009); Revised Payment Services Directive (2015)

2 | COUNTRY EXAMPLE | EUROPEAN UNION

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | GHANA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Customer Funds: Funds must be invested in cash held at universal banks or other assets permitted by BoG and not commingled. Float may not exceed 15% of bank's net worth. Once deposit insurance is implemented, funds should be eligible.

Capital Requirements:

- **Initial:** GHS 5 million (USD 1 million)
- **Ongoing:** Not specified

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: Not specified

Interoperability: Unlike the 2008 *Branchless Banking Guidelines*, which required full interoperability, the 2015 E-Money Guidelines do not include specific requirements with respect to e-money interoperability.

Financial Inclusion: No documented national financial inclusion strategy exists, though one was under consideration as of early 2019.

Source: E-Money Guidelines (2015)

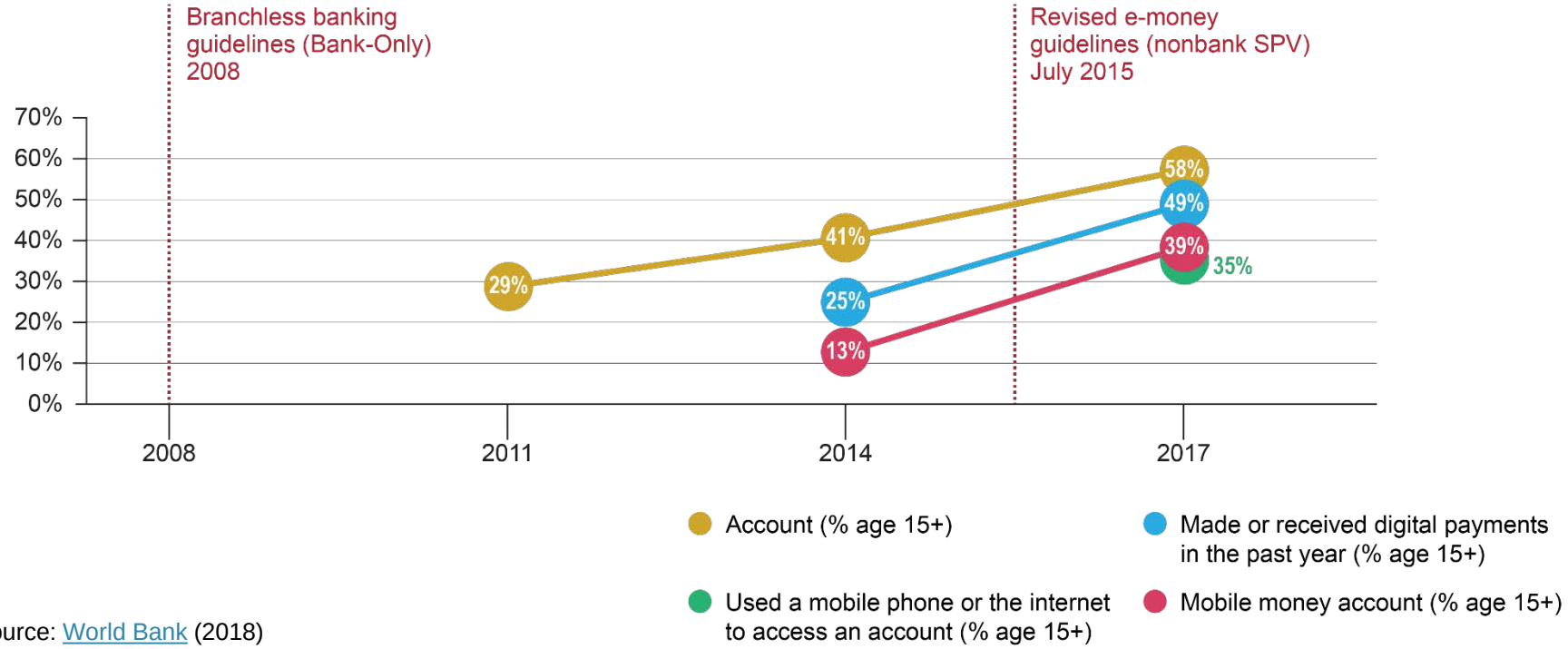
AML/CFT

KYC:

- **Minimum KYC accounts:** Name, date of birth, address, phone number, any photo ID that can reliably identify customer.
- **Medium KYC accounts:** Same as above, except ID must be national ID, voter ID, driver's license, NGIS ID, SSNIT ID, or passport.
- **Enhanced KYC accounts:** Same as Medium, plus proof of address, which must be verified.
- **Over-the-counter transactions:** Same as Medium, except for low-value transactions with introduction from customer with acceptable ID.

2 | COUNTRY EXAMPLE | GHANA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | KENYA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Customer Funds: Funds equal in value to outstanding e-money must be held in non-commingled trust accounts in at least four commercial banks (of which at least two must be “strong rated”) and managed by a trustee. Pass-through deposit insurance envisioned in legal framework, implementation pending.

Capital Requirements:

- **Initial:** KES 20 million (USD 200,000))
- **Ongoing:** Not specified

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: Following intervention by the Competition Authority, Safaricom agreed in 2017 to reduce USSD session charges from KES 5 (USD 0.05) to KES 1 (USD 0.01).

Interoperability: In May 2017, the country’s e-money providers agreed to interoperate**.** As of October 2018, interoperability was mostly operational.

Financial Inclusion: The Vision 2030 Second Medium Term Plan 2013-2017 included a limited number of high-level financial inclusion-related targets.

AML/CFT

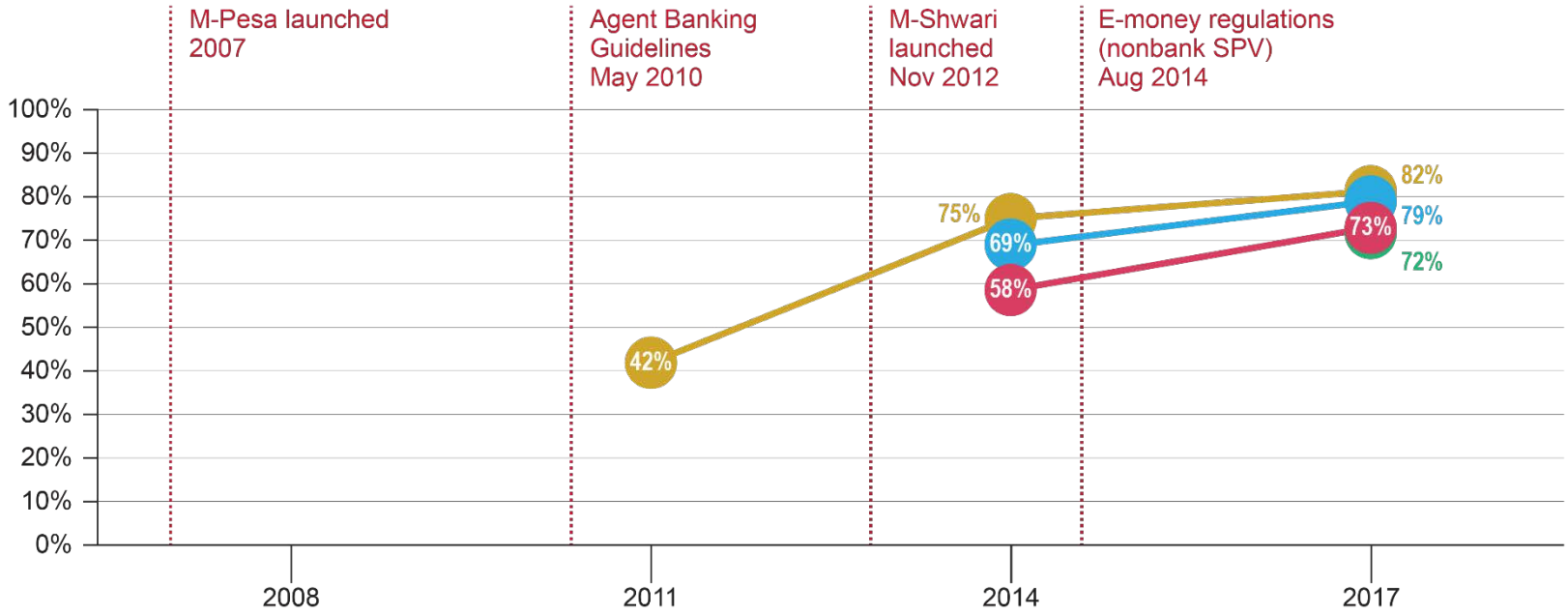
KYC:

- **Individual accounts:** Name and identity card or passport (verified through Integrated Population Registration System).

Source: NPS Regulations (2014)

2 | COUNTRY EXAMPLE | KENYA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | MALAYSIA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Customer Funds: Funds equal in value to outstanding e-money must be held in a trust account in a licensed institution and invested in deposits, government securities, or other approved assets. Funds may not be commingled.

Capital Requirements:

- **Initial:** MYR 5 million (USD 1.2 million)
- **Ongoing:** 8% of average outstanding e-money liabilities

Competition & Financial Inclusion

Agent Exclusivity: Not specified

USSD Access: Not specified, although BNM's draft Interoperable Credit Transfer Framework would mandate fair and open access to shared payment infrastructure.

Interoperability: No current mandate, but BNM's draft Interoperable Credit Transfer Framework would mandate interoperable credit transfers and waive fees for most retail transfers.

Financial Inclusion: Financial Inclusion Framework outlines vision, desired outcomes, and strategies to achieve desired outcomes.

AML/CFT

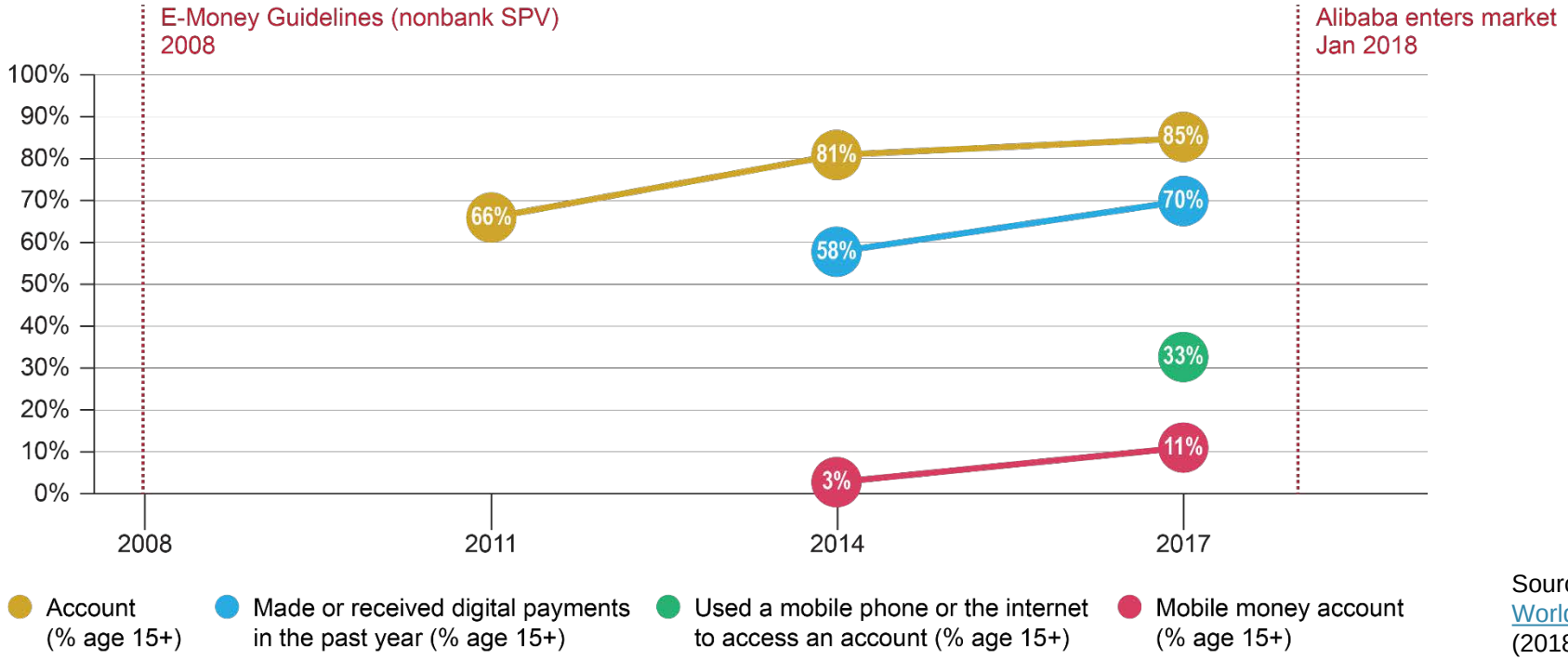
KYC:

- **No CDD (purchases only, no cash-out):** None.
- **Simplified CDD (purchases or transfers, no cash-out, funded by existing bank or payment account):** Name; identity number of NRIC, passport, or other official photo ID; residential and mailing address; date of birth; nationality; phone number; purpose of transaction. Name or NRIC must be verified with source of funds.

Source: Guideline on E-Money (2008)

2 | COUNTRY EXAMPLE | MALAYSIA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | MYANMAR

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (MFS Providers)

Protection of Customer Funds: Funds equal in value to outstanding e-money issued must be held in trust in current accounts held at one or more commercial banks (or in other approved liquid assets). Funds may not be commingled and must remain unencumbered.

Capital Requirements:

- **Initial:** MMK 3 billion (USD 1.9 million)
- **Ongoing:** Not specified

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: Not specified

Interoperability: MFS Providers must provide services that are capable of becoming interoperable at the agent, customer, or mobile platform level, but interoperability is not explicitly mandated.

Financial Inclusion: The Financial Inclusion Roadmap 2014-2020 aims to increase financial inclusion from 30% to 40% by 2020.

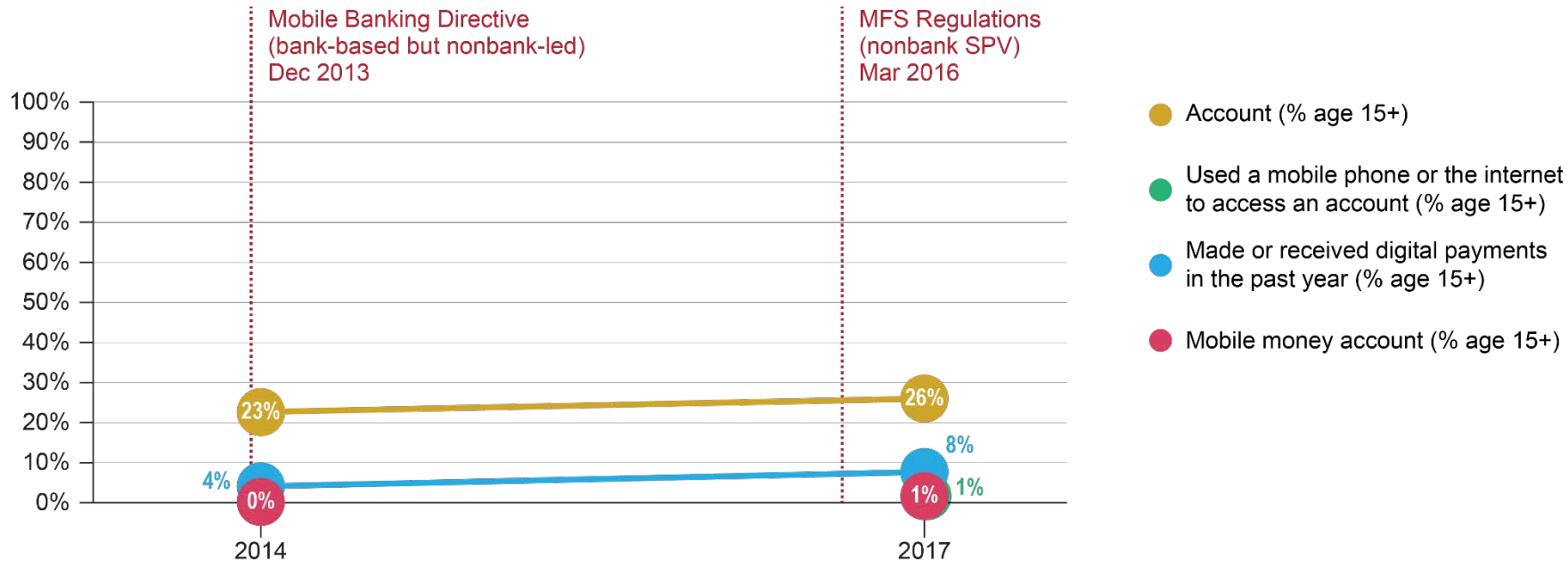
Source: Regulation on Mobile Financial Services (2008)

AML/CFT

KYC:

- **Level 1 accounts:** May be opened remotely without proof of identity, but a national ID, driver's license, or passport is required for certain cash-in/cash-out or OTC services.
- **Level 2 accounts:** Requires one of the Level 1 ID documents.
- **Level 3 accounts:** Business registration certificate and full identification requirements for opening business bank accounts.
- **Over-the-counter:** Requires one of the Level 1 ID documents .

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | PERU

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Customer Funds: Funds equal in value to outstanding e-money issued must be held in trust or another mechanism prescribed by the financial supervisor.

Capital Requirements:

- **Initial:** PEN 2.4 million (USD 722,090)
- **Ongoing:** 2% of outstanding e-money liabilities

Source: *Ley 29985* (2013); *Decreto Supremo 090-2013-EF* (2013); SBS (2013)

Competition & Financial Inclusion

Agent Exclusivity: Permitted

USSD Access: Telecommunications regulator requires MNOs to offer non-discriminatory pricing for USSD access.

Interoperability: While the central bank and financial supervisory authority reserve the right to intervene with respect to interoperability, no such requirement currently exists.

Financial Inclusion: In 2015, Peru launched a National Financial Inclusion Strategy aiming for 75% of adults to have access to a transaction account by 2021.

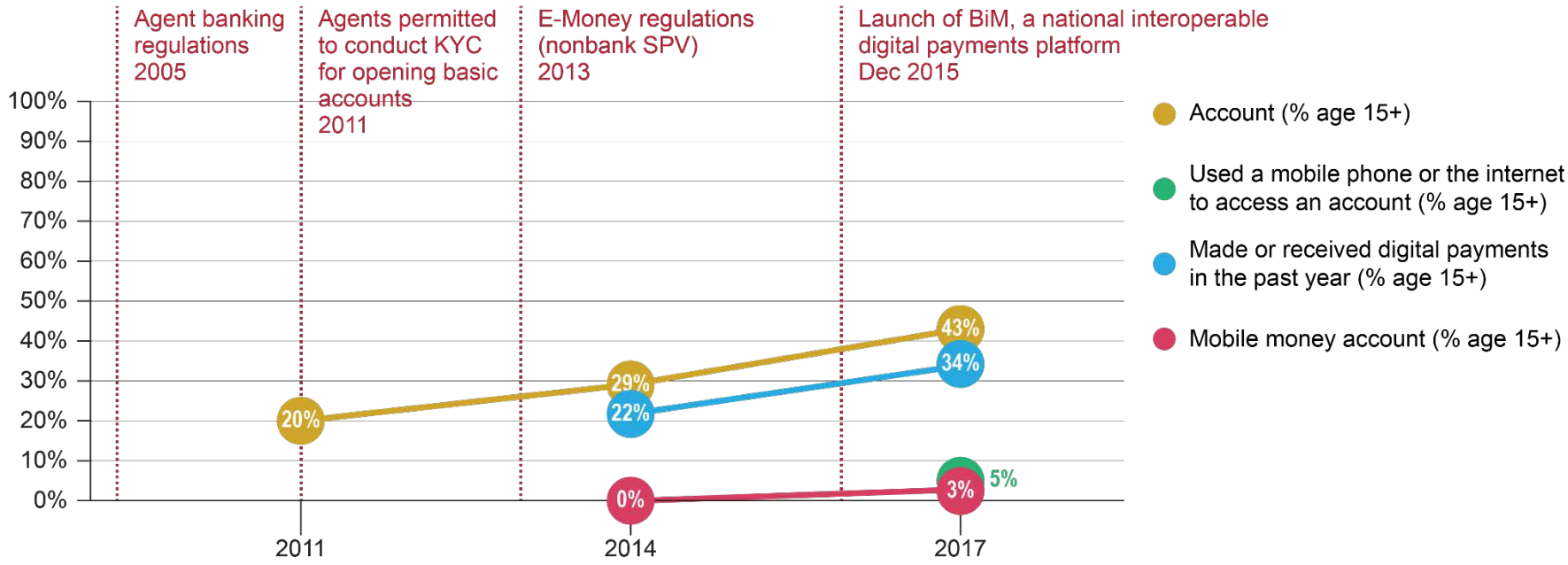
AML/CFT

KYC:

- **Simplified e-money accounts:** Full name, identity document number (must be National Identity Document), and mobile phone number. Information must be verified using central government database.
- **Regular e-money accounts:** Must also collect and verify full name, type and number of identity document, nationality and residence, address, phone number and/or e-mail address, purpose of financial relationship, and occupation.

2 | COUNTRY EXAMPLE | PERU

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | RWANDA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (E-Money Issuers)

Protection of Customer Funds: Funds equal in value to outstanding e-money must be isolated, unencumbered, and held in trust in bank deposits and short-term government securities. Max 25% of float may be stored in a single bank, and float may not exceed 25% of that bank's core capital.

Capital Requirements:

- **Initial:** RWF 100 million (USD 115,970)
- **Ongoing:** Not specified

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: MNOs must provide access to all 3rd parties, but price is left for negotiation.

Interoperability: After initially setting strict timelines for interoperability, the NBR is working with e-money issuers to promote interoperability through a market-driven approach.

Financial Inclusion: Rwanda is aiming at financially including 90% of adults by 2020. 89% of adults were included by 2016, surpassing the country's goal of 80% by 2017.

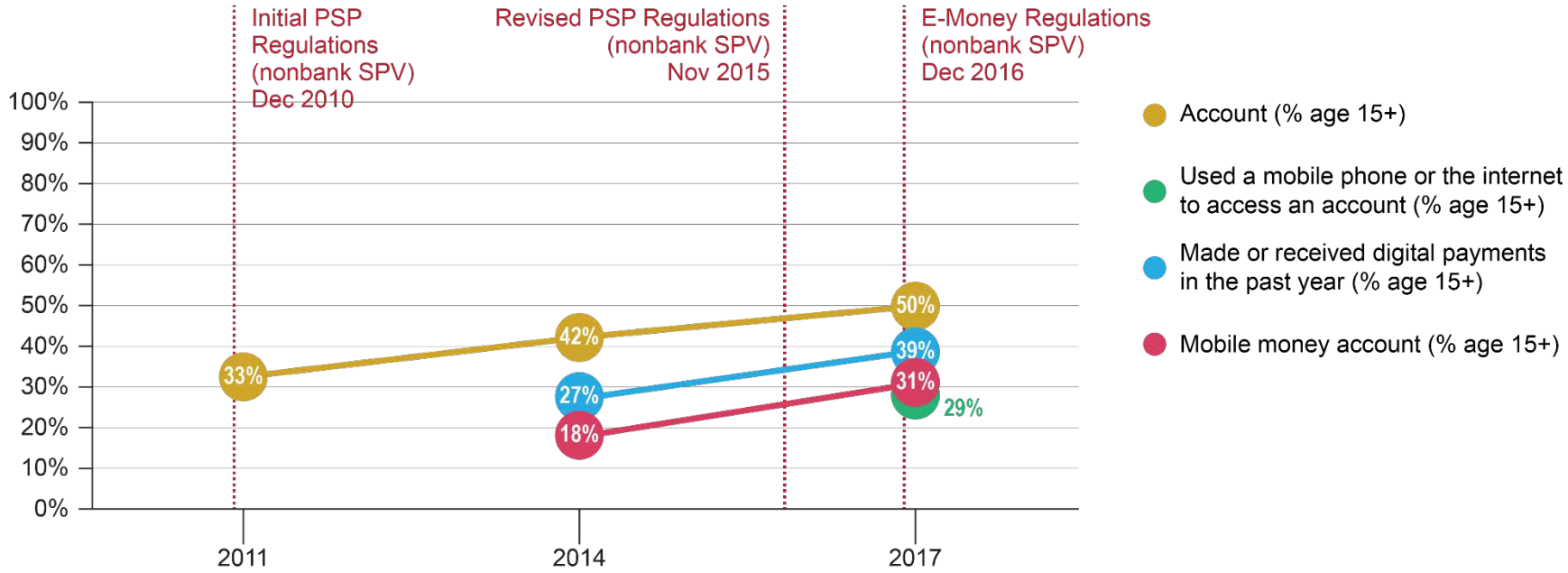
AML/CFT

KYC:

- **Tier I (individuals, e-KYC):** Registered phone number and e-money account, acceptable photo ID.
- **Tier II (individuals, physical registration):** Registered phone number and e-money account, acceptable photo ID.
- **Tier III (legal entities), Tier IV (retail agents, Tier V (super agents), and Tier VI (merchants):** Full KYC, with specific requirements tailored to type of entity.

Source: Regulation Governing the E-Money Issuers (2016)

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | SRI LANKA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (Mobile Payment Service Providers)

Protection of Customer Funds: Funds equal in value to outstanding e-money must be held in one or more “custodian accounts” in commercial banks. These funds may not be claimed by creditors if the service provider becomes insolvent.

Capital Requirements:

- **Initial:** LKR 150 million (USD 872,000)
- **Ongoing:** Not specified

Source: Mobile Payments Guidelines (2011)

Competition & Financial Inclusion

Agent Exclusivity: Not specified

USSD Access: Not specified.

Interoperability: While banks offering mobile payment services are were required to join the Common Mobile Switch by 2017, this is not yet required for non-banks.

Financial Inclusion: In Jan 2018, the IFC and Central Bank of Sri Lanka announced plans to develop the country’s first National Financial Inclusion Strategy.

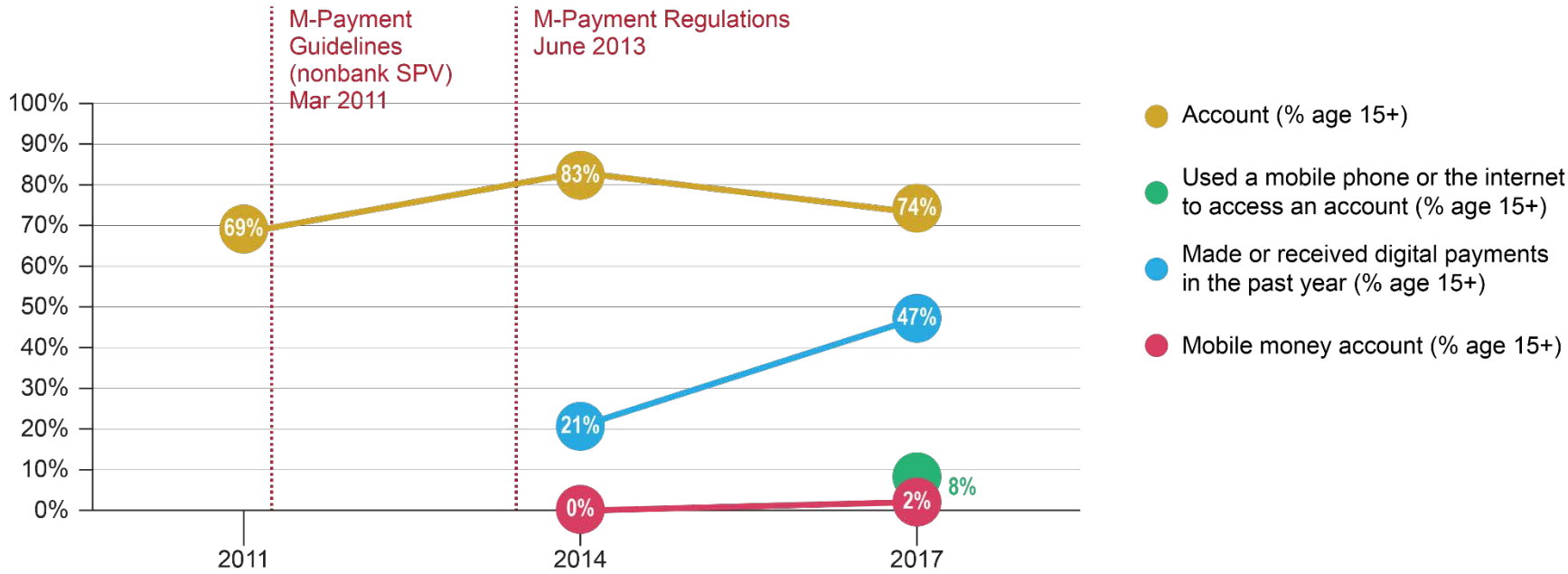
AML/CFT

KYC:

- **Individual Customers:** Full name; photo ID; address; phone number and e-mail address (if applicable); date of birth; nationality; occupation and name/location of employer; purpose for opening account; expected turnover; expected transaction modes; reference (if applicable). Providers must obtain copies of photo ID and address verification document.

2 | COUNTRY EXAMPLE | SRI LANKA

Evolution of Financial Inclusion and DFS



Source: World Bank (2018)

2 | COUNTRY EXAMPLE | TANZANIA

Licensing Model & Prudential Requirements

Licensing Model: Non-Bank SPV (Electronic Money Issuers)

Protection of Customer Funds: Funds equal in value to outstanding e-money must be held in non-commingled trust accounts in at least four commercial banks and managed by a separate legal entity trustee.

Capital Requirements:

- **Initial:** TZS 500 million (USD 218,570)
- **Ongoing:** Not specified

Source: E-Money Regulations (2015)

Competition & Financial Inclusion

Agent Exclusivity: Prohibited

USSD Access: Not specified.

Interoperability: TCRA required MNOs' systems to have the capacity to be interoperable and to adhere to international standards. With encouragement from the BoT, TZ's three major EMIs voluntarily interoperated (Airtel and Tigo in Feb 2015, with Vodacom joining in 2016).

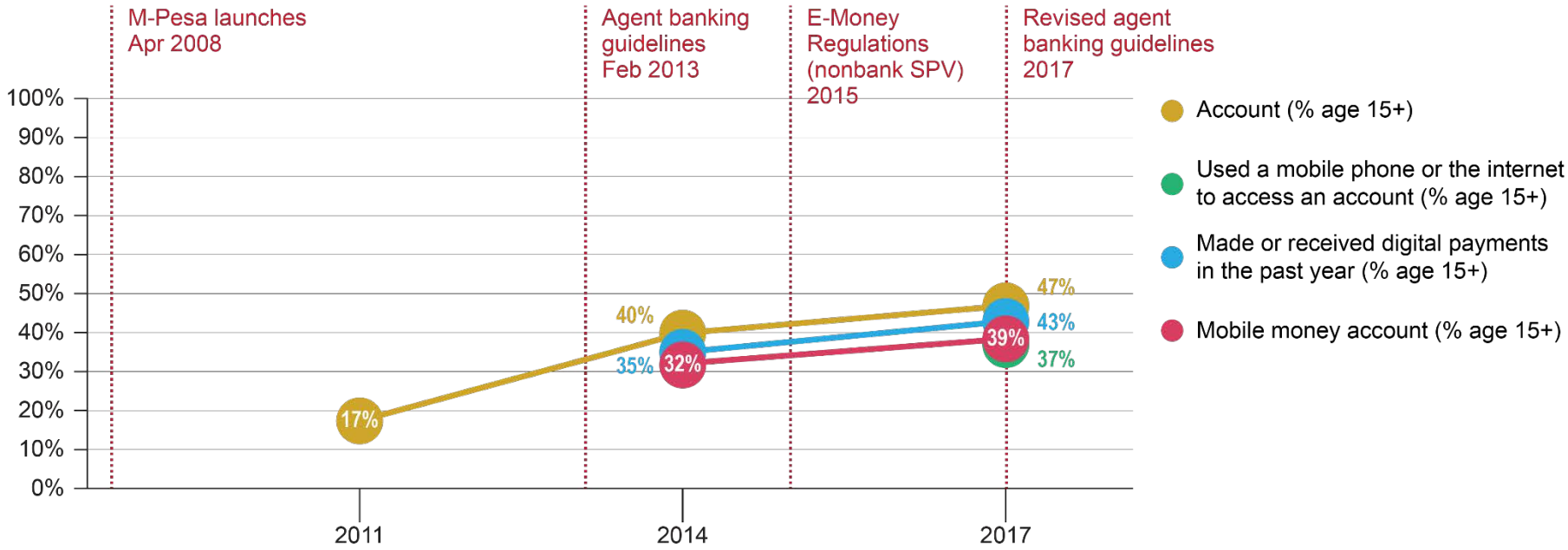
Financial Inclusion: The 1st National Financial Inclusion Framework (NFIF) was implemented from 2014-16 and has been followed by a 2nd NFIF (2018-2022).

AML/CFT

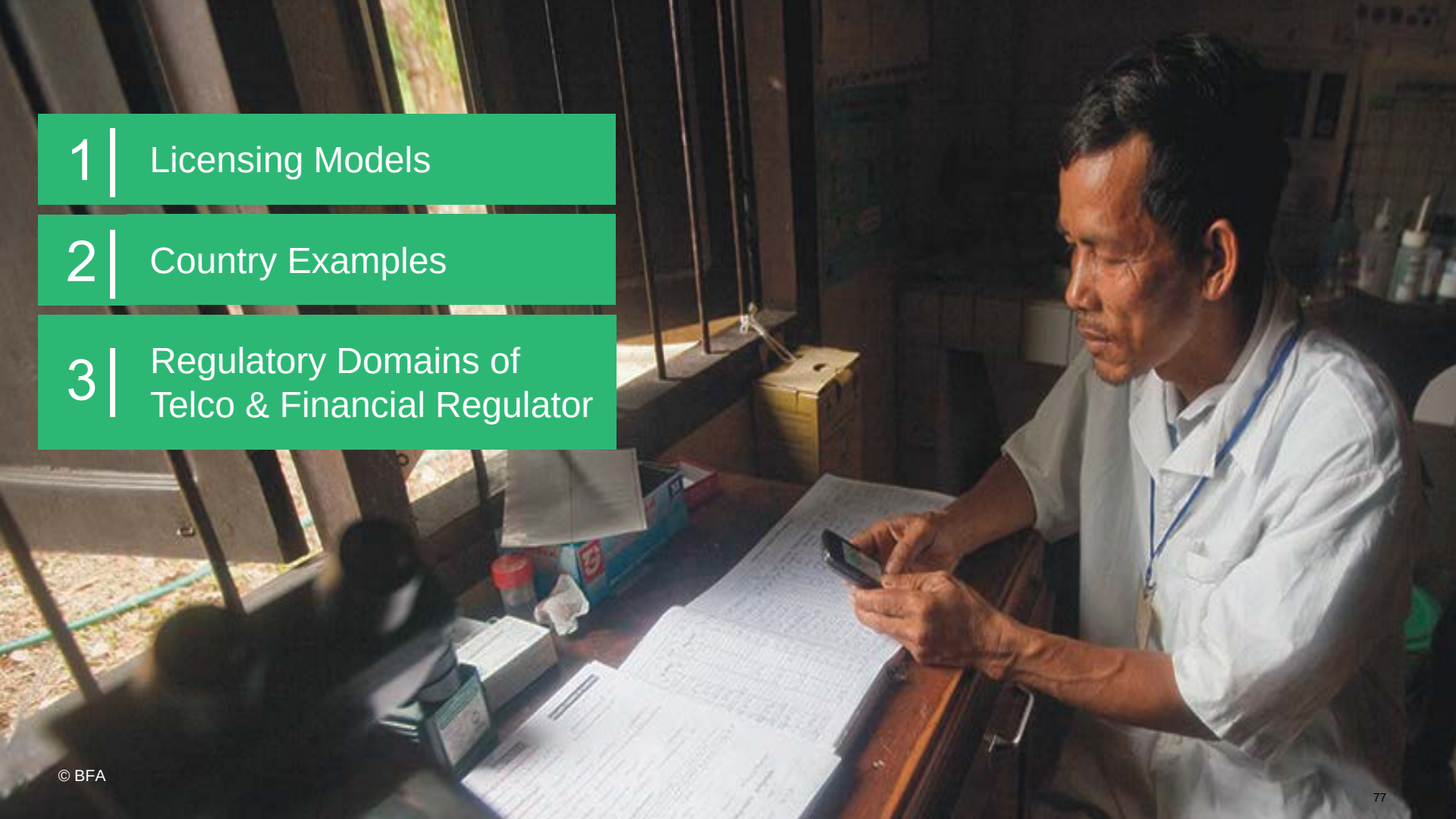
KYC:

- **Tier I (electronically registered):** Registered phone number, registered e-money account number, acceptable photo ID
- **Tier II (electronically and physically registered):** Same as above, plus storage of KYC documentation in customer account registry.
- **Tier III (SMEs):** Full KYC plus TIN, business license number, VAT registration, and other verification documents.
- **Tier IV (retail agents):** Similar requirements to Tier III, tailored to needs of retail agents.

Evolution of Financial Inclusion and DFS



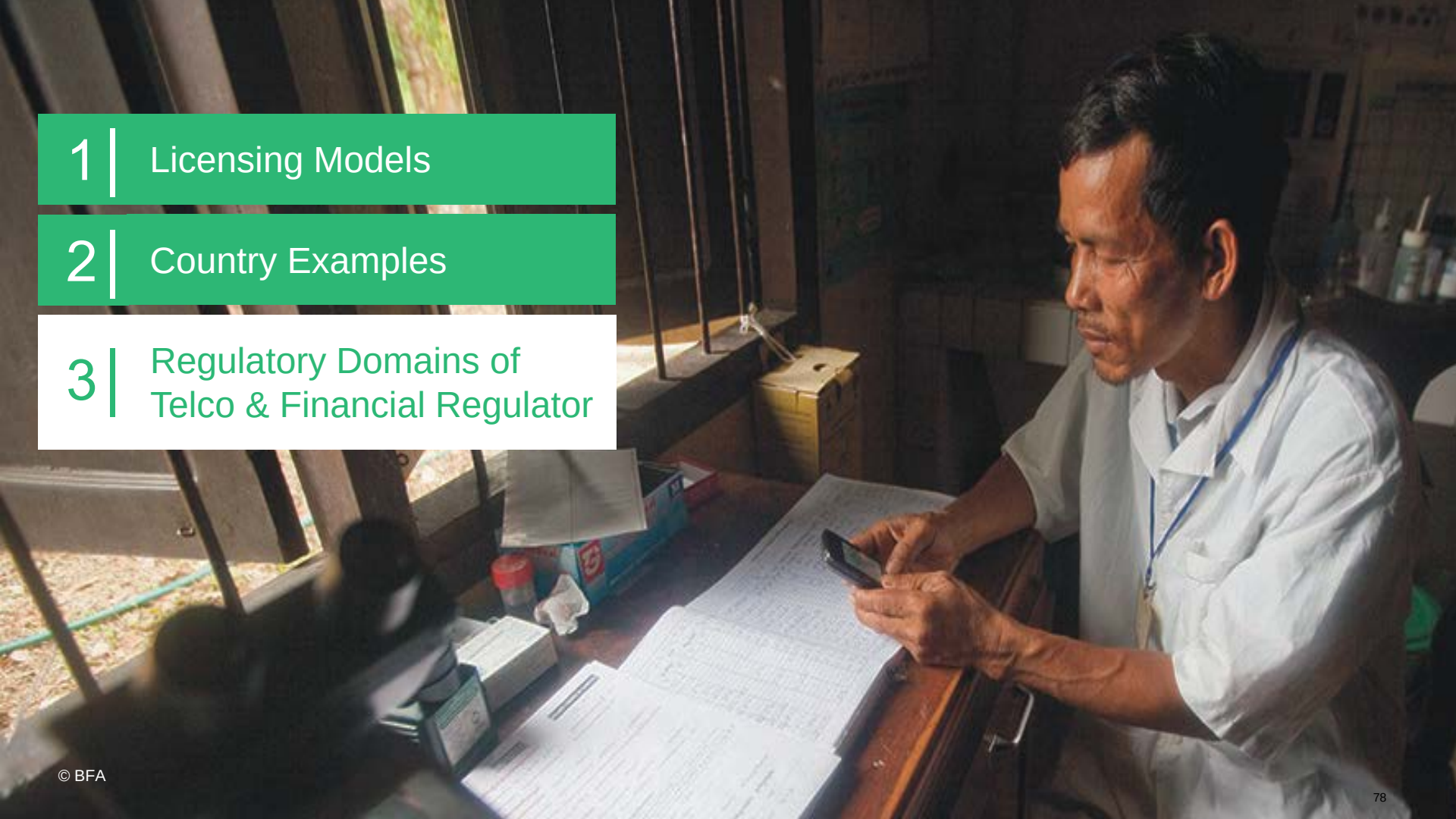
Source: World Bank (2018)



1 | Licensing Models

2 | Country Examples

3 | Regulatory Domains of Telco & Financial Regulator



1 | Licensing Models

2 | Country Examples

3 | Regulatory Domains of Telco & Financial Regulator

Issue

There is a need to clarify the respective responsibilities of the telecommunications regulator and the financial regulator when MNOs are permitted to establish a subsidiary to issue e-money or offer similar services.

Delineation of responsibility

- The telco regulator could be responsible for authorizing MNOs to:
    1. establish a subsidiary for e-money business as a value-added service; and
    2. apply for a license from the financial regulator.
- The financial regulator could be responsible for licensing and regulating the e-money subsidiary.

Issue

There is a need to clarify the respective responsibilities of the telecommunications regulator and the financial regulator when MNOs are permitted to establish a subsidiary to issue e-money or offer similar services.

Considerations

- Requiring MNOs to establish a subsidiary specifically for e-money business would limit the potential risk to the telco parent in the event of the e-money subsidiary's insolvency. This subsidiary EMI would be licensed by the financial authority.
- Having two separate business entities would also clearly delineate jurisdictions of the telco regulator (MNO license) and financial regulator (e-money license). See next slide.

3 REGULATORY DOMAINS OF TELCO & FINANCIAL REGULATOR

Issue	Financial regulator	Telco regulator
Fair access to USSD and other communication channels		✓
Fair access to retail payment infrastructure	✓	
E-money agent exclusivity	✓	
E-money interoperability	✓	
E-money prudential risks	✓	
E-money non-prudential (market conduct) risks	✓	
Permission to own and apply for a license for a e-money subsidiary from the financial regulator		✓
Licensing of e-money subsidiary	✓	

PRUDENTIAL REGULATION & SUPERVISION

1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

4 Systemic Risk

5 Reconciliation & Settlement

1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

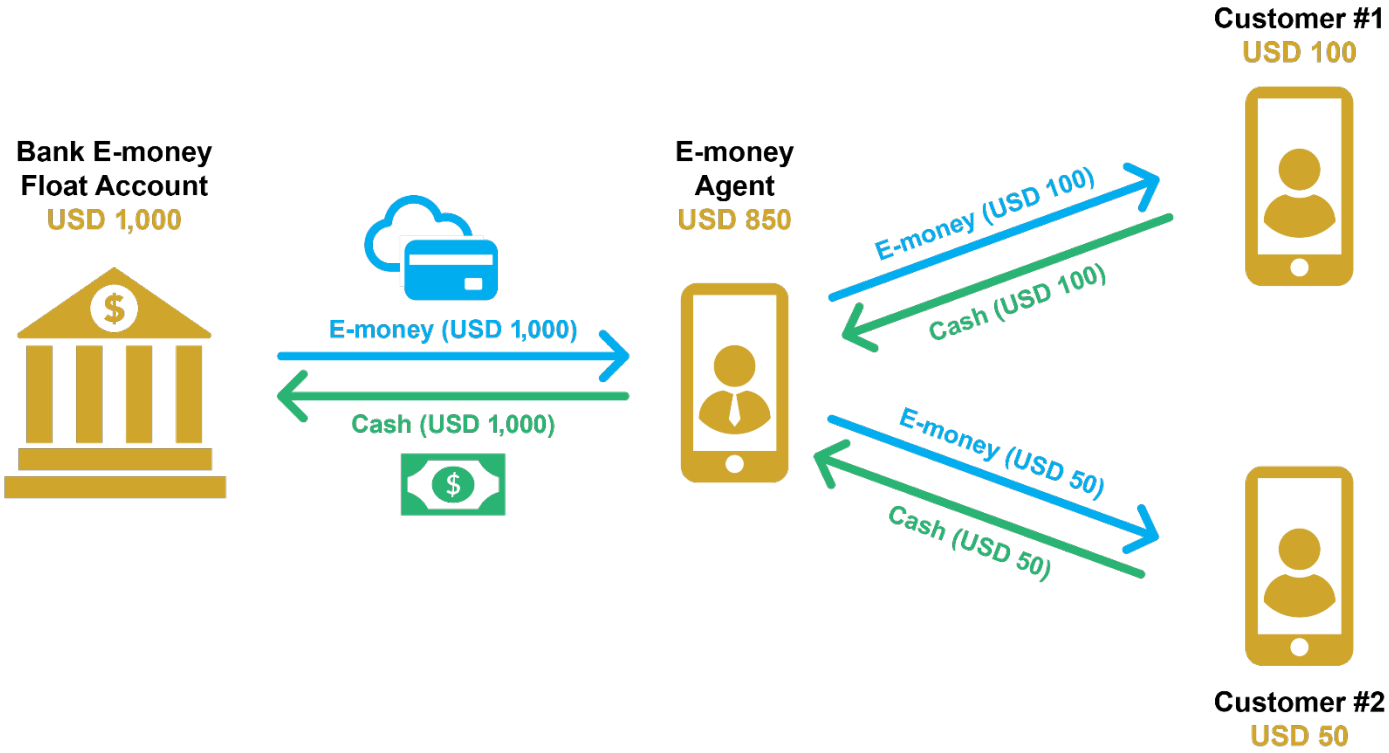
4 Systemic Risk

5 Reconciliation & Settlement

1 | SAFEGUARDING CUSTOMER FUNDS

Risk	Possible solutions
Liquidity: Insufficient funds set aside in safe, liquid investments to repay customers.	**Prefunding:** Require e-money issuer to set aside funds equal to 100% of outstanding e-money liabilities in licensed banks and/or other safe, liquid investments.
Issuer insolvency: Insufficient assets to repay customers in event of issuer's (or trustee/ fiduciary's) insolvency.	**Fund isolation:** Require e-money issuer to hold funds set aside to repay customers in trust (or similar fiduciary instrument). Providers could be required not to commingle customer funds with issuer's funds and to legally ring-fence customer funds (i.e., only used to repay customers and protected against credit claims in event of issuer's insolvency).
Bank insolvency: Insufficient assets to repay customer in event of bank's insolvency.	**Deposit insurance:** Provide for customer funds to be covered by direct or pass-through deposit insurance (or take other measures to mitigate bank insolvency risk).

1 | SAFEGUARDING CUSTOMER FUNDS – LIQUIDITY
HOW PREFUNDING WORKS



1 | SAFEGUARDING CUSTOMER FUNDS – LIQUIDITY

Country examples: Funds held in safe, liquid investments

Colombia

E-money issuers are required to deposit all customer funds in a demand deposit account in the Central Bank or another financial institution.

Source: *Decreto 1491* (2015)

European Union

Either (i) 100% of customer funds must be isolated from the e-money issuer's other funds and deposited in a separate account in a credit institution or invested in "secure, low-risk assets"; or
(ii) the e-money issuer must obtain insurance covering the full value of outstanding e-money liabilities.

Source: E-Money Directive (2009); Revised Payment Services Directive (2015)

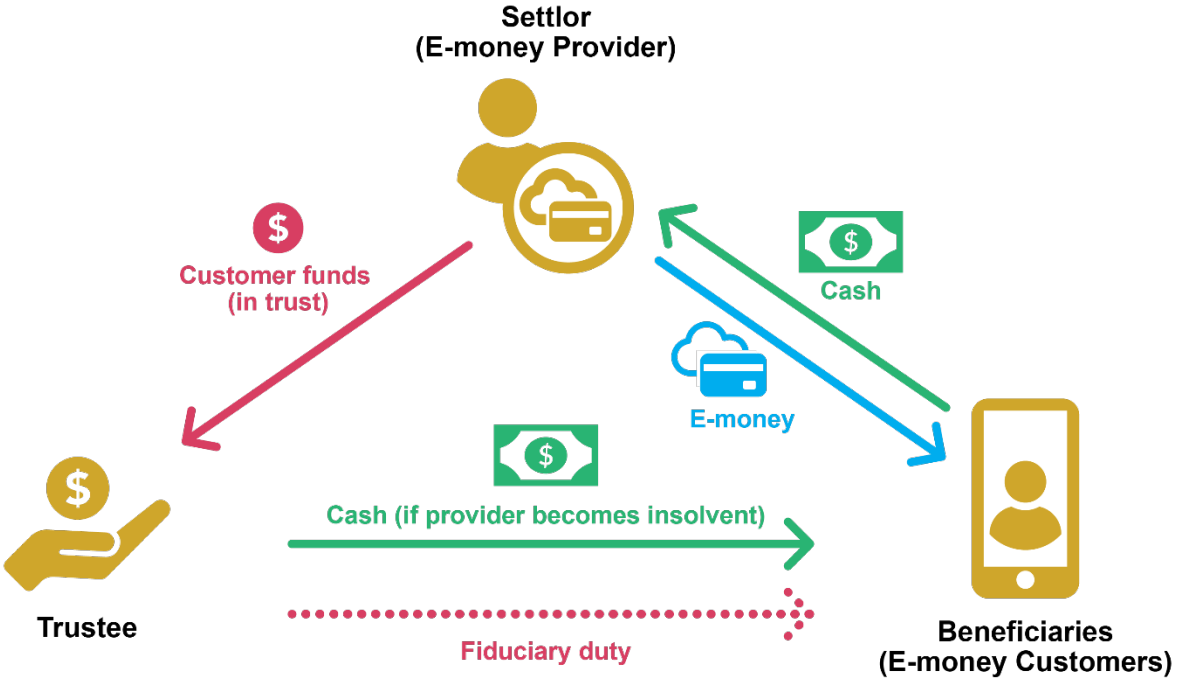
India

Except for funds held with the central bank to meet Cash Reserve Ratio requirements, at least 75% of customer funds must be invested in short-term government securities and up to 25% of customer funds may be held in commercial banks.

Source: RBI (2014)

1 | SAFEGUARDING CUSTOMER FUNDS – ISSUER INSOLVENCY

HOW TRUST ARRANGEMENTS WORK



Source: GSMA (2016)

1 SAFEGUARDING CUSTOMER FUNDS – ISSUER INSOLVENCY

Country examples: Funds held in trust or similar fiduciary instrument

Paraguay

E-money issuers are required to store customer funds in autonomous funds managed by one or more fiduciaries, which are limited to banks, financial companies, or specially authorized fiduciary companies.

Source: BCP (2014); *Ley 921* (1996)

European Union

If funds are safeguarded through investment of funds (as opposed to via an insurance policy), funds must be protected against claims from other creditors of the e-money issuer in accordance with national law, particularly with respect to insolvency.

Source: E-Money Directive (2009); Revised Payment Services Directive (2015)

Namibia

Outstanding e-money liabilities must be held in trust in one or more licensed banks, subject to a written instrument under the Trust Moneys Protection Act.

Source: Determination on Issuance of E-Money (2012); BoN (2019)

1 | SAFEGUARDING CUSTOMER FUNDS – BANK INSOLVENCY

Approach	Advantages	Disadvantages
Direct deposit insurance	• E-money balances insured • Payout may be simpler than for pass-through insurance	• Requires e-money issuers to become members of deposit insurance system • Requires deposit insurers to reassess risk and possibly raise premiums
Pass-through deposit insurance	• E-money balances insured • No need for e-money issuers to become direct members of deposit insurance system	• Strict requirements for payout (see next slide) • Operational challenges for reimbursing many e-money accountholders with tiny balances • Requires deposit insurers to reassess risk and possibly raise premiums
Float held at Central Bank	• E-money balances protected • No need to address deposit insurance challenges	• Central Banks may lack infrastructure to efficiently play role of float-holding bank • Appropriate role for Central Bank? • Inability to promote financial inclusion and financial sector development through intermediation and distribution of interest

1 | SAFEGUARDING CUSTOMER FUNDS – BANK INSOLVENCY

REQUIREMENTS FOR IMPLEMENTATION OF PASS-THROUGH DEPOSIT INSURANCE

Legal Requirements

Existence of custodial account

Individually identifiable sub-accounts

Customer ownership of funds held in custodial account

Operational Requirements

Insurer's access to records to ID balances of each sub-accountholder

Aggregation of user accounts within one institution for purposes of applying insurance coverage limit

Adequate insurer resources for expansion of coverage to include digital stored-value products

OPERATIONALIZING PASS-THROUGH DEPOSIT INSURANCE FOR DFS

Issues	Possible Solutions
 If funds are held in custodial accounts in multiple banks and one bank fails, which customer accounts are associated with the failed bank?	Requiring EMIs to have a **clear policy** on how customer funds are allocated across custodial accounts could help to ensure that customer names and associated account balances can be retrieved in the event of custodial bank insolvency.
 Can deposit insurance cover e-money accounts without requiring individual e-money customers to cash-out in the event of failure of a custodial bank?	Establishing procedures to enable **transfer of custodial account** to an assuming bank could help to avoid any disruption to the e-money service.

1 | SAFEGUARDING CUSTOMER FUNDS – BANK INSOLVENCY

Advantages and disadvantages of other (non-deposit insurance) mechanisms for mitigating bank insolvency risk

Approach	Advantages	Disadvantages
Private insurance	• Could provide protection in countries that lack deposit insurance scheme	• Cost and availability of insurance (and financial strength of private insurers) will vary from country to country
Guarantee from bank's parent group	• Could provide protection in countries that lack deposit insurance scheme	• Available only in countries with competitive banking sector and multinational banks • Strength of guarantee depends upon financial strength of parent group
Float diversification	• Reduce total loss in event of bank failure	• Funds not protected, so e-money issuer must cover losses through own capital
Bank strength requirement	• Reduce risk that funds are held in weak bank	• Bank failure difficult to predict • Signaling risk to market
Minimum capital requirements	• Ensure e-money issuers can cover losses and remain solvent	• High requirements could affect sustainability • Insufficient to cover losses in event of catastrophic bank failure

1 SAFEGUARDING CUSTOMER FUNDS – BANK INSOLVENCY

Country examples: Deposit insurance

Direct application of deposit insurance to e-money accounts:

Colombia

Funds held by *Societies Specializing in Deposits and Electronic Payments (SEDPEs)* are considered to be deposits and are directly covered by deposit insurance in the event of the institution's insolvency.

Source: *Ley 1735* (2014)

India

Funds held by Payments Banks are directly covered by deposit insurance in the event of the institution's insolvency.

Source: RBI (2014)

Indirect application of deposit insurance ("pass-through"):

United States

Funds held in a pooled account are eligible for deposit insurance on a pass-through basis if all of the following apply:

a. The e-money issuer has identified the account as a custodial account, with funds held on behalf of the underlying customers;

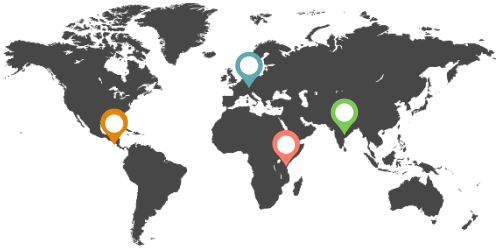
b. The issuer, bank, or another third party maintains records identifying each beneficial owner and the amount owed to each; AND

c. The underlying customers legally own the funds in question.

Source: New General Counsel's Opinion No. 8 (2008)

1 | SAFEGUARDING CUSTOMER FUNDS – BANK INSOLVENCY

Country examples: Other approaches to mitigate bank insolvency risk



Float held in Central Bank

El Salvador
Customer funds must be 100% backed by a non-remunerated deposit in the Central Bank.

Source: *Decreto 72* (2015)

Private insurance

European Union
As an alternative to setting aside funds equal to 100% of outstanding e-money liabilities, e-money issuers may obtain private insurance covering the full value of these liabilities.

Source: E-Money Directive (2009); Payment Services Directive (2015)

Float diversification and bank strength requirement

Tanzania and Kenya
E-money issuers must diversify float among a minimum of four banks once it exceeds USD 45,000 in Tanzania and USD 1 million in Kenya. Kenya also requires at least half of these funds to be held in "strong rated" banks.

Source: NPS Regulations (2014); E-Money Regulations (2015)

Minimum capital requirements

India
Payments banks must maintain capital equal to a minimum of (i) 15% of risk-weighted assets; and (ii) 3% of outstanding liabilities.

Source: RBI (2014)

Considerations

Liquidity risk: Financial authorities could require e-money issuer (EMI) to set aside funds equal to 100% of outstanding e-money liabilities in licensed banks and/or other safe, liquid investments.

Issuer insolvency risk: Financial authorities could require EMI to hold funds set aside to repay customers in trust (or similar fiduciary instrument) in the name of the EMI's customers. These funds should only be debited for settlement of customer obligations and should not be used as collateral in credit agreements.

Bank insolvency risk: Ideally, financial authorities could provide for customer funds to be covered by direct or pass-through deposit insurance. If not possible in the short term, authorities could take other measures to mitigate bank insolvency risk, such as:

- Requiring float to be privately insured;
- Requiring a guarantee from the bank's parent group;
- Mandating diversification of float across multiple banks; and/or
- Applying proportional ongoing capital adequacy requirements (see next section).


1 Safeguarding Customer Funds
2 Capital Requirements
3 Distribution of Interest
4 Systemic Risk
5 Reconciliation & Settlement

Issue

Regulators typically require e-money issuers to meet **initial and ongoing minimum capital requirements** to protect the firm against unexpected losses and serve as a source of growth**.**

Initial requirements aim to ensure that new entrants have sufficient capital to build a sustainable e-money business and mitigate key risks such as unexpected losses.

Ongoing requirements aim to ensure that the e-money issuer retains a sufficient capital buffer as the business grows.

MINIMUM CAPITAL REQUIREMENTS FOR EMIS & SIMILAR ENTITIES

Country	Initial requirements	Ongoing requirements
India	USD 13.7 million	(i) 15% of risk-weighted assets; and (ii) 3% leverage ratio
Mexico	USD 11.1 million	8% of risk-weighted assets
Nigeria	USD 5.5 million (MMOs) USD 13.8 million (PSBs)	Not specified (MMOs) 10% of risk-weighted assets (PSBs)
Bangladesh	USD 5.3 million	USD 5.3 million, rising to USD 10.7 million (to be built up over time from retained earnings)
Congo, DR	USD 2.5 million	Greater of (i) USD 2.5 million; or (ii) current or six-month average of outstanding e-money liabilities.
Colombia	USD 2.2 million	2% of 30-day average outstanding electronic deposits
Myanmar	USD 1.9 million	Not specified
Philippines	USD 1.9 million	Not specified
Malaysia	USD 1.2 million	Greater of (i) USD 1.2 million; or (ii) 8% of outstanding e-money liabilities
Ghana	USD 1 million	Not specified

NOTE: Capital requirements and exchange rates as of 25 October 2018

MINIMUM CAPITAL REQUIREMENTS FOR EMIS & SIMILAR ENTITIES

Country	Initial requirements	Ongoing requirements
Sri Lanka	USD 872,000	Not specified
Peru	USD 722,090	2% of outstanding e-money liabilities
Brazil	USD 540,000	Greater of (i) 2% of average monthly transaction value (past 12 months); or (ii) 2% of outstanding liabilities.
WAEMU	USD 522,380	Greater of (i) USD 522,380; or (ii) 3% of outstanding e-money liabilities
EU	USD 400,000	2% of outstanding e-money liabilities
Tanzania	USD 218,570	Not specified
Kenya	USD 200,000	Not specified
Namibia	USD 174,000	Greater of (i) USD 174,000; or (ii) 2% of outstanding e-money liabilities
Rwanda	USD 115,970	Not specified

NOTE: Capital requirements and exchange rates as of 25 October 2018

Considerations

Initial requirements: Initial minimum capital requirements vary widely from country to country. When setting these requirements, regulators may wish to consider the following:

- How much capital is needed to build the **required infrastructure** for sustainable e-money business and demonstrate an EMI's **financial capacity and commitment?**
- Are capital requirements sufficient to enable the EMI to cover **unexpected losses?**

In practice, initial minimum capital requirements may vary significantly depending upon, e.g., (i) the size of the addressable market; and (ii) core infrastructure costs in a particular country.

Ongoing requirements: Requiring EMIs to maintain the initial minimum capital in unimpaired form could serve as a base ongoing capital requirement. In addition, tying the capital base to outstanding e-money liabilities could help to ensure that sufficient capital is available as the EMI grows.

Regulators could consider requiring EMIs to maintain **the greater of** (i) the initial minimum capital; or (ii) a percentage of outstanding e-money liabilities (several countries have set this percentage in the 2-3% range). It is worth noting that while this represents common practice, the adequacy of these requirements has not been extensively tested in practice.

Source: Basel Committee on Banking Supervision (2016)

1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

4 Systemic Risk

5 Reconciliation & Settlement

1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

4 Systemic Risk

5 Reconciliation & Settlement

3 DISTRIBUTION OF INTEREST

Customer funds held in pooled accounts often generate interest. Deciding how to distribute this interest has been a subject of considerable debate.

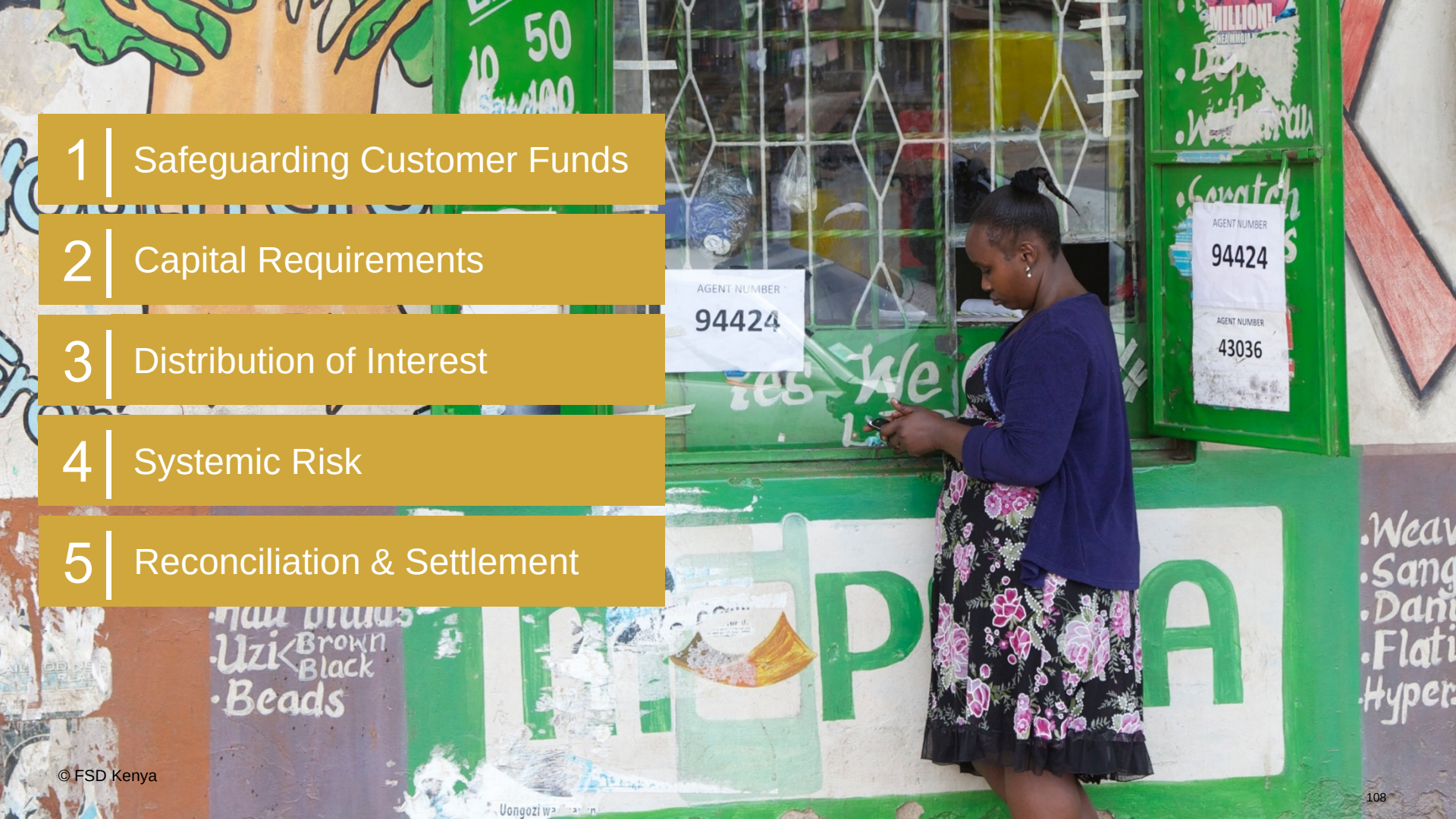
Arguments for requiring distribution of interest to e-money customers (including agents)	Arguments for allowing e-money issuers to decide what to do with interest	Arguments for prohibiting distribution of interest to issuers or customers
Customer benefit: Since the value of pooled accounts is based upon outstanding e-money liabilities, customers should benefit from any interest earned these accounts.	**Market efficiency:** In a competitive market, alternate uses of funds may be more beneficial to customers than direct distribution of interest. For example, interest can help to defray costs of administering pooled accounts and offering e-money services, which can help reduce cost of services to customers.	**Legal compliance:** Depending upon the country's legal framework, collecting funds from customers and then distributing interest earned from the pooled account could be deemed "*banking business,*" which would be prohibited for nonbanks.
Incentivizing adoption: Paying interest could boost e-money adoption by encouraging **customers** to keep more funds on the account and **agents** to maintain more e-money float.		
Legal compliance: Some financial authorities have concluded that distributing interest is not engaging in "banking business," as e-money issuers are merely distributing interest earned on a single pooled account, not offering individual interest-based accounts.		

3 | DISTRIBUTION OF INTEREST | COUNTRY EXAMPLES

Approach	Rationale & Country example
Must be donated to charity	Distinguish from banking business (Kenya)
May not pay interest to customers	Distinguish from banking business but permit providers to benefit from float income (Afghanistan)
Must indirectly benefit customers	Provide lots of flexibility while ensuring customers benefit (Lesotho)
Must directly benefit customers	Provide some flexibility while ensuring customers benefit (Tanzania)
Must pay out 80% of interest	Ensure that most of funds are passed on to customers (Ghana)
Provider decides how to use interest	Give providers maximum flexibility over use of float (India)

Considerations

- Financial authorities will first need to determine whether local banking law permits EMIs to **(1)** open interest-bearing settlement accounts; and **(2)** distribute the interest earned on such accounts to their customers.
- If financial authorities determine that this is permissible, they would then need to decide whether to require EMIs to distribute some or all of the interest earned on the settlement accounts to their customers.
- Requiring EMIs to distribute interest to their customers could incentivize DFS adoption and encourage customers and agents to keep more money in e-money accounts.
- Allowing EMIs to decide whether to distribute interest could help promote competition, as some might distribute interest to incentivize uptake, others might use these funds to invest in better infrastructure, and others might reduce fees for using the service.


1 Safeguarding Customer Funds
2 Capital Requirements
3 Distribution of Interest
4 Systemic Risk
5 Reconciliation & Settlement
AGENT NUMBER
94424
AGENT NUMBER
94424
AGENT NUMBER
43036
Uzi Brown Black Beads


1 Safeguarding Customer Funds
2 Capital Requirements
3 Distribution of Interest
4 Systemic Risk
5 Reconciliation & Settlement
AGENT NUMBER
94424
AGENT NUMBER
94424
AGENT NUMBER
43036
Uzi Brown Black Beads

Issue

In countries with high volumes of e-money usage, a disruption in the e-money service could affect much of the population (see next slide).

Such an event could be considered systemic from the perspective of the financial authorities.

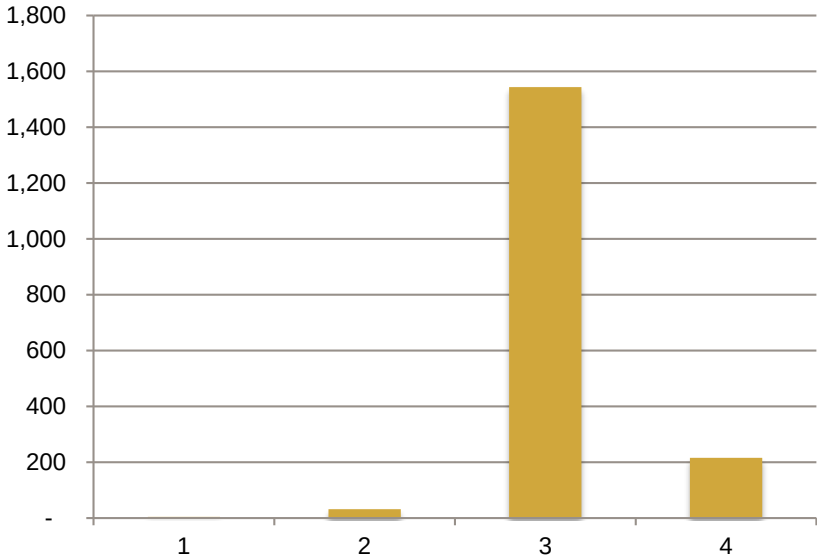
Other Impacts of E-Money on Stability

Usage of e-money for savings and credit could strengthen financial stability by increasing aggregate savings in the formal financial sector and enabling financial institutions to diversify their depositor base and loan portfolios.

On the other hand, rapid credit expansion without proper controls could reduce financial stability through over-indebtedness and high non-performing loan ratios.

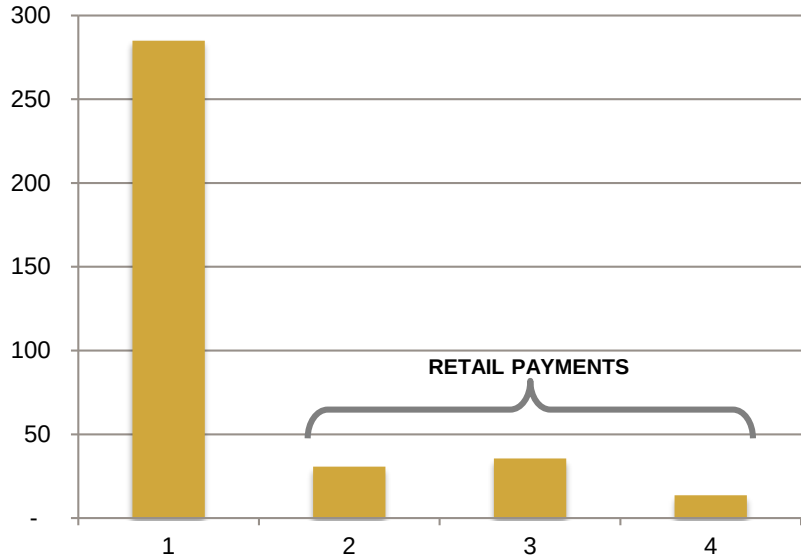
KENYA'S NATIONAL PAYMENTS LANDSCAPE

2017 Transaction volume (millions)



KENYA'S NATIONAL PAYMENTS LANDSCAPE

2017 Transaction value (USD Billions)



Source: Central Bank of Kenya (exchange rate as of 31 Dec 2017)

Considerations

Monitoring e-money transaction growth (volume and value) over time could help mitigate systemic risk to the financial system and operational risk to the national payment system.

If high adoption of e-money leads to a large increase in NPS transaction volume, regulators could take steps to ensure that the NPS infrastructure is able to keep pace, such as:

- Increasing server capacity;
- Increasing network redundancy and resilience;
- Hiring additional staff; and
- Reviewing and updating business continuity and disaster recovery plans.

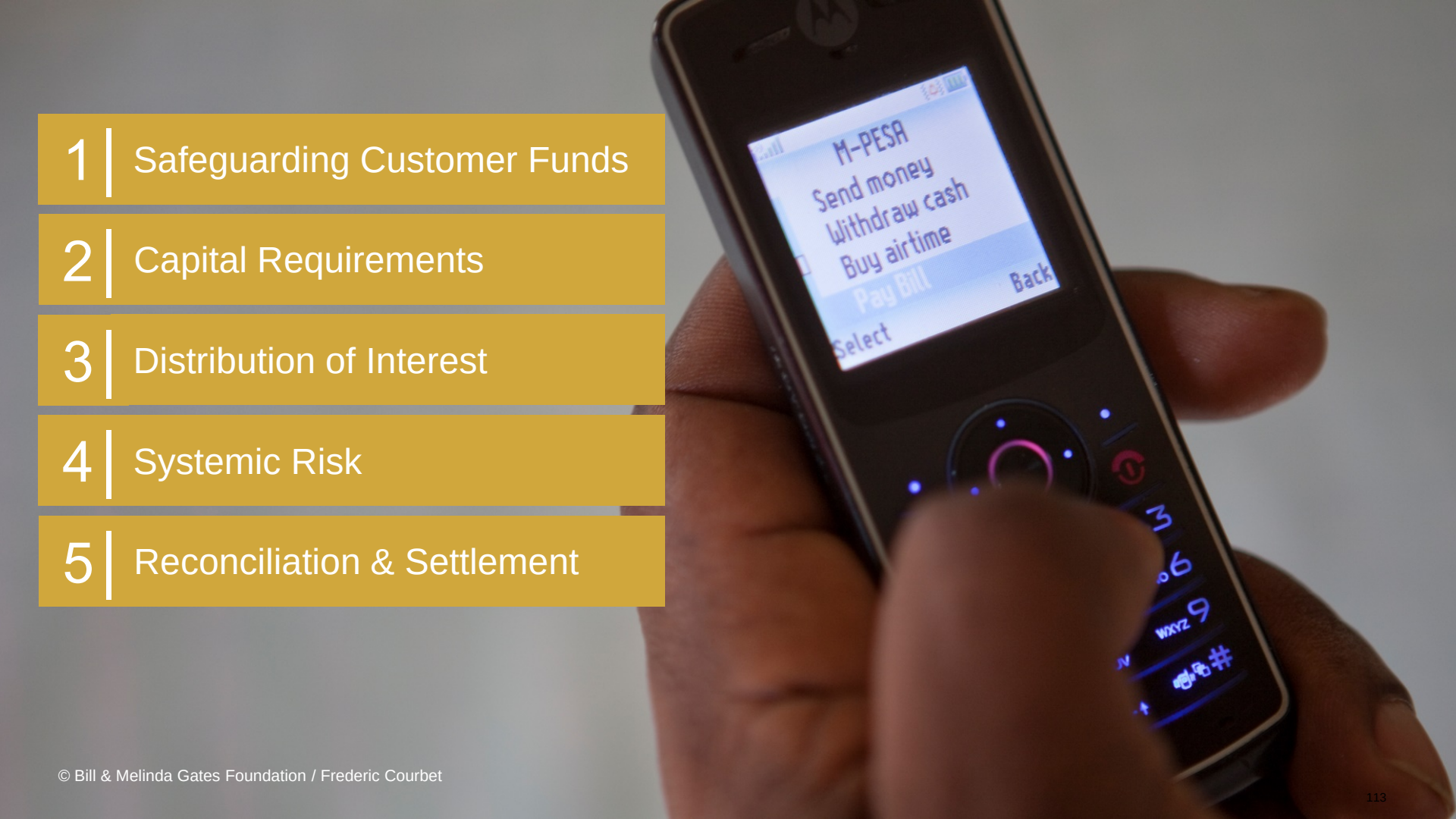
1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

4 Systemic Risk

5 Reconciliation & Settlement



1 Safeguarding Customer Funds

2 Capital Requirements

3 Distribution of Interest

4 Systemic Risk

5 Reconciliation & Settlement

Issue

In the absence of clear rules governing settlement and reconciliation, allowing non-bank entities to issue e-money could create risk.

- Sound e-money issuance is based upon the principle that all issued e-money is fully covered by funds held in banks and/or other safe, liquid investments (see Safeguarding Customer Funds).
- Proper reconciliation and settlement procedures must be followed whenever e-money is issued or redeemed, such as when:
    - Agents purchase e-money (cash-in) or withdraw funds (cash-out);
    - Users cash-in or cash-out through the national retail payment system; or
    - EMIs cash out transaction fee income.
- Frequent reconciliation of the balances of issued e-money and funds held by EMIs reduces the risk of fraud and loss of within and by the EMI.
- In the absence of clear rules governing settlement and reconciliation, internal fraudsters could create excess e-money in their systems or embezzle customer or EMI funds (see country examples).

5 E-MONEY RECONCILIATION AND SETTLEMENT
COUNTRY EXAMPLES

Theft of customer e-money

Uganda

In 2011, MTN Uganda lost millions of dollars due to poor internal controls and inadequate settlement and reconciliation procedures. Internal fraudsters created fictitious accounts and stole money from the suspense account (used for disputed, erroneous, or incomplete transactions).

Source: The Observer (2015)

Theft of EMI funds

Rwanda

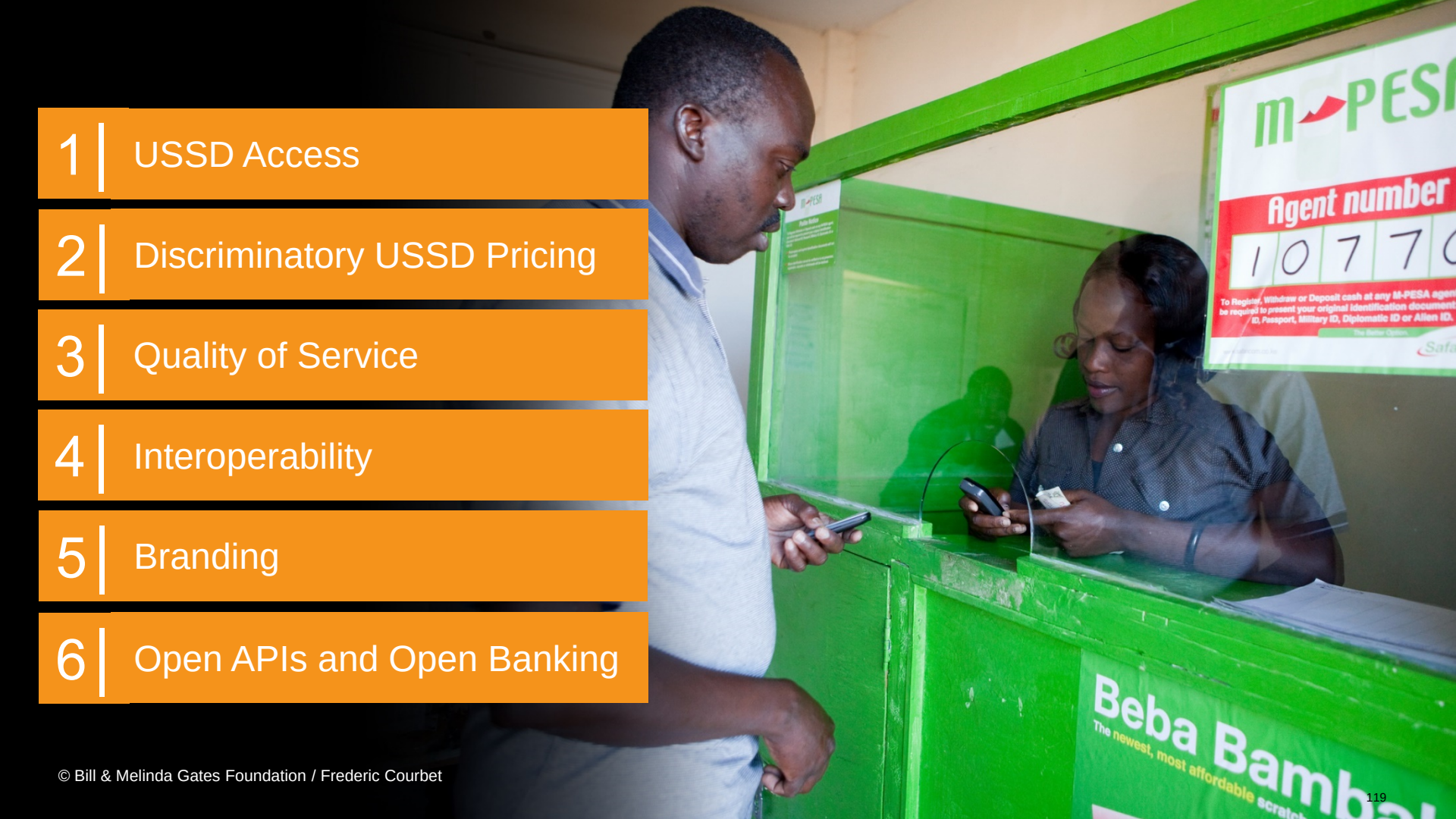
In 2014, a Tigo Rwanda employee colluded with two “super agents” to embezzle over USD 700,000 in company funds. While Tigo Cash customer and agent funds were unaffected, it took over a year for the fraud to be detected.

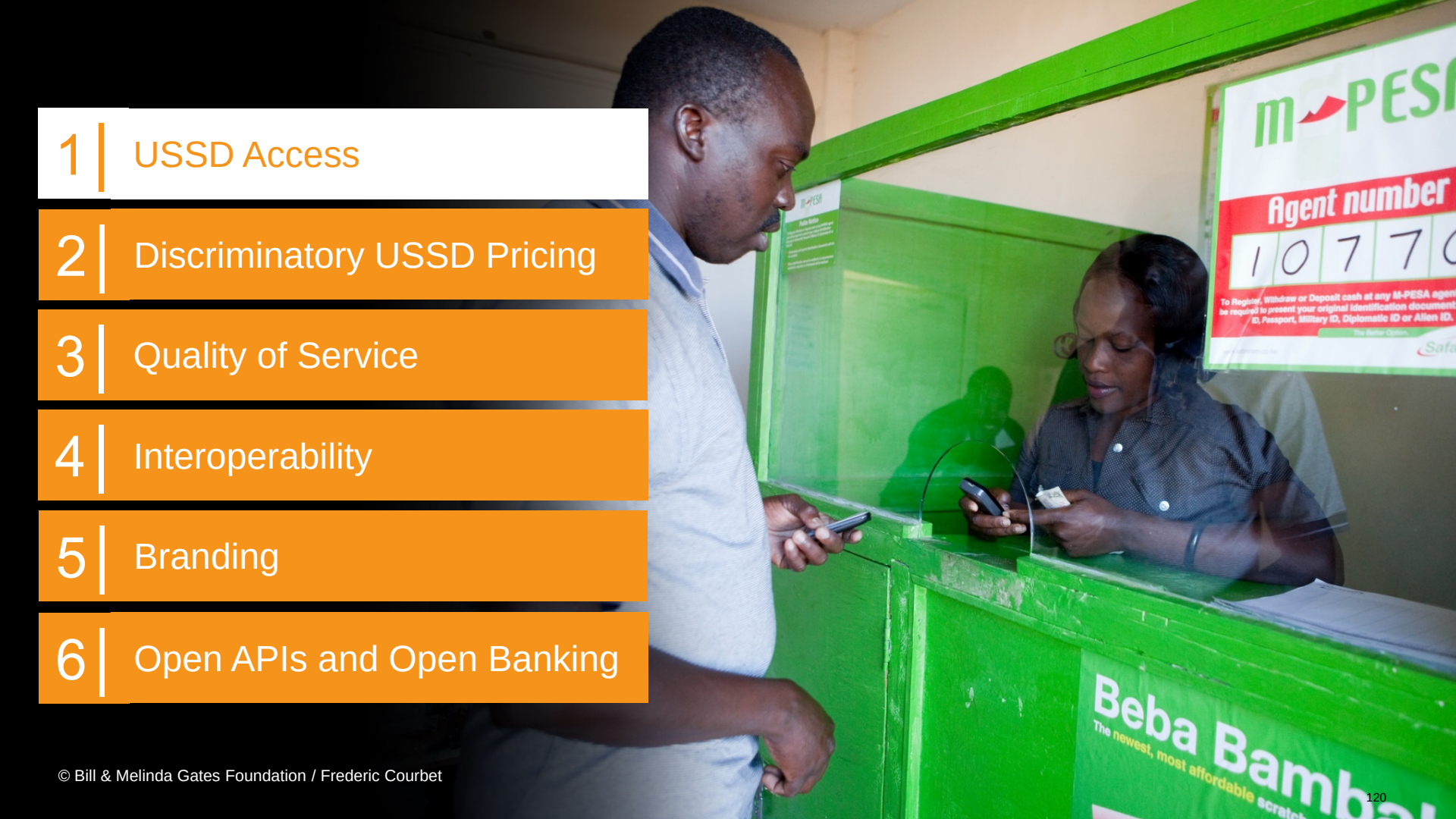
Source: Rwanda National Police (2014)

Considerations

- Frequent reconciliation of the total amount held in banks and/or other safe, liquid investments against the total e-money balance in the EMI's system is a crucial check to ensure that the customers' funds are safeguarded.
- Each of the three fund flows that result in issuance or redemption of e-money (direct cash-in or cash-out by agents or other third parties, settlement of payment system obligations, and cash-out by the EMI) should be accounted for separately.
- EMIs participating in the national retail payment system, whether directly or through a sponsor institution, should provide their own funds to guarantee transaction settlement; funds backing e-money should not be used as security.
- Active oversight of reconciliation and settlement procedures by supervisors is critical.
- Establishing ongoing minimum capital requirements that are tied to outstanding e-money liabilities can help ensure that EMIs maintain sufficient capital to cover any losses due to internal fraud.

COMPETITION ISSUES





Issue

All non-MNO EMIs require access to MNO-owned communication services (typically SMS, USSD, and/or data) to offer mobile-based services to customers. Failure to gain access to these services could affect DFS development.

If an MNO is directly competing in or has a direct or indirect financial interest in the EMI market, refusal to supply communications services could harm competitors.

Data is typically only useful for smartphones. Most e-money services not delivered via smartphones use USSD, which displays as an interactive menu on the mobile (see next slide).

USSD access is governed by agreements between EMIs and MNOs, most of which are bilateral commercial agreements. In many countries, this access has been an issue (see country examples).

1 | USSD ACCESS | EXAMPLE OF A USSD TRANSACTION

User enters USSD short code (e.g., *159#) and presses ‘phone’ to ‘call’ the USSD number. The menu then displays:

User enters 2 for Send Money and presses ‘Reply’

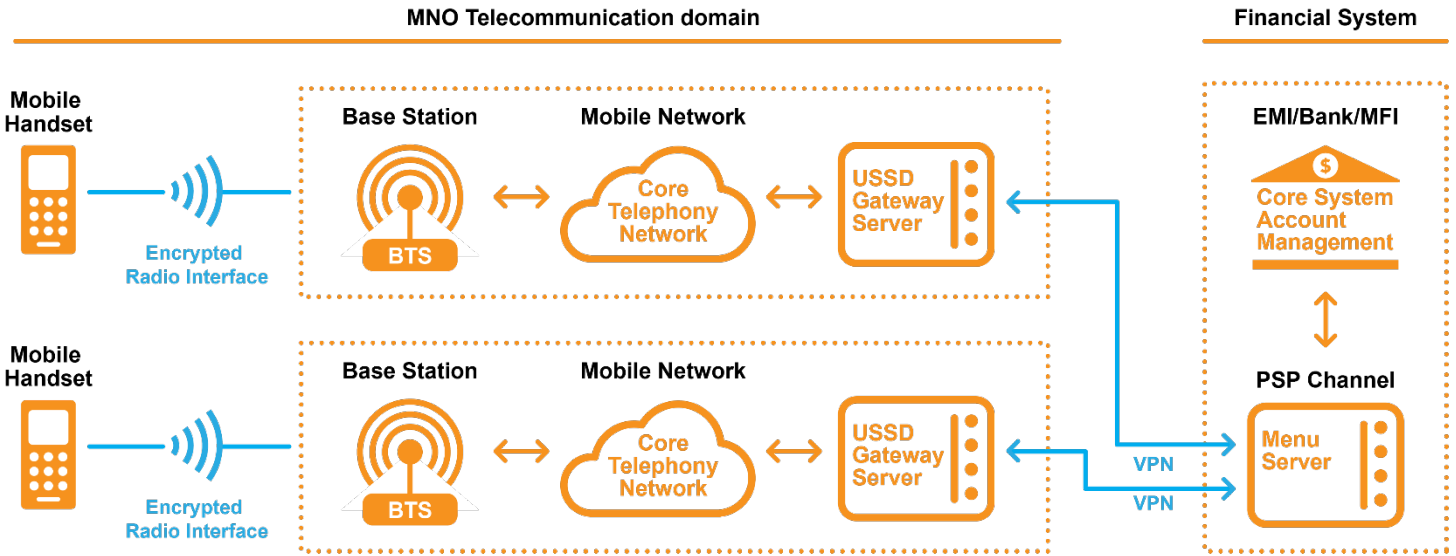
User enters ‘0739572185’ and presses ‘Reply’

User enters ‘800’ and presses ‘Reply’

User enters PIN and presses ‘Reply’

1 USSD ACCESS

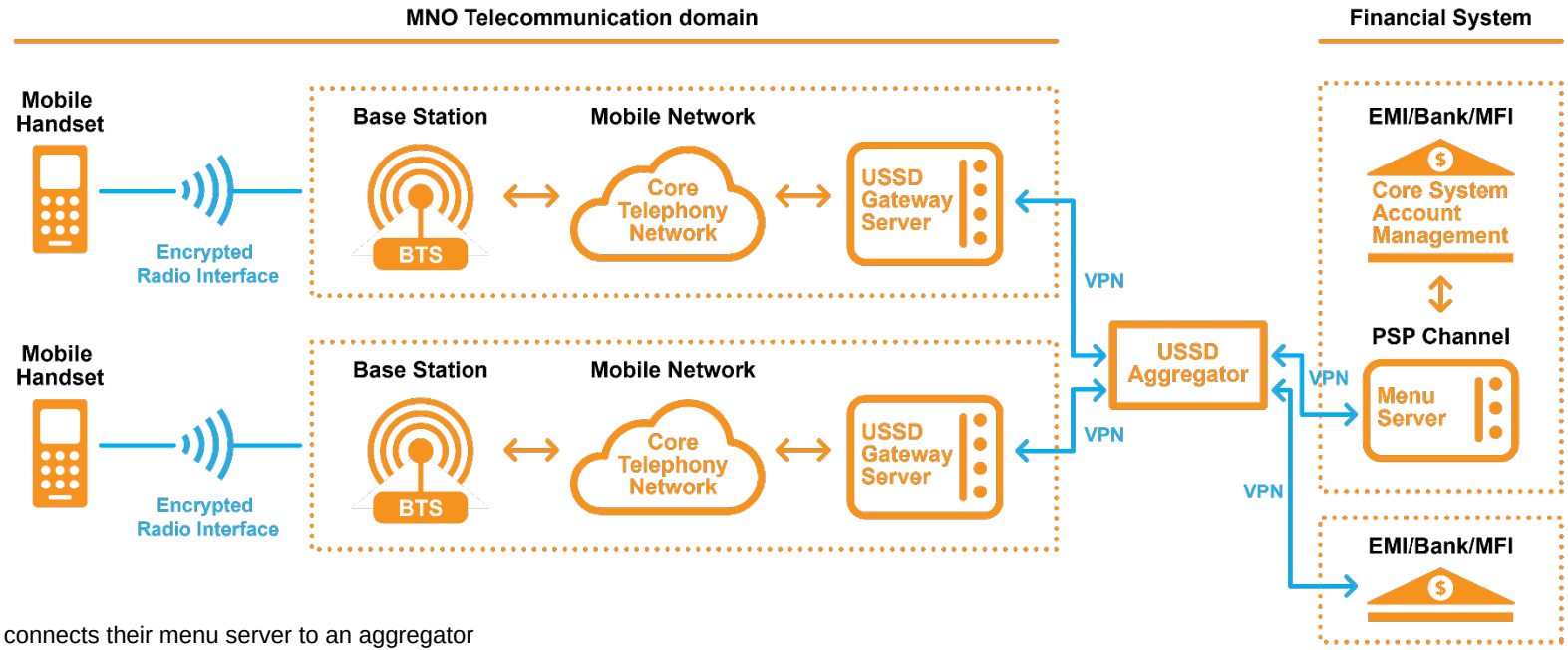
The system elements involved in USSD – direct FI-to-MNOs connection



The EMI connects its menu server directly to the USSD gateway of each MNO.
Traffic is encrypted from the EMI to the MNO and from the base station antenna to the handset, but not within the MNO.
The EMI signs a separate (bilateral) service agreement for USSD with each MNO and then directly integrates with each MNO.

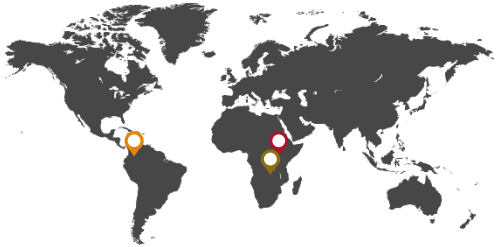
1 USSD ACCESS

The system elements involved in USSD – MNOs connected via an Aggregator



The EMI connects their menu server to an aggregator
Traffic is encrypted from the EMI to the aggregator and then from the aggregator to the MNO and again from the base station antenna to the handset, but not within the MNO or the aggregator
The EMI signs a single service agreement for USSD with the aggregator who then contracts and integrates with each MNO
Multiple EMIs can connect to the aggregator

1 | USSD ACCESS | COUNTRY EXAMPLES



Colombia

The telco regulator mandated that the MNOs provide USSD access to all financial institutions after extensive negotiations between banks and MNOs proved unsuccessful.

Source: ITU (2017)

Uganda

Ezee Money sued the MNO MTN for refusing access to its USSD gateway. The Commercial Court determined that MTN violated its duties under the Communications Act, ordered MTN to pay a fine, and issued a permanent injunction against such anti-competitive behavior in the future.

Source: ITU (2017)

Zambia

Zoona sued the MNO MTN for refusing access to its USSD gateway. The case is ongoing.

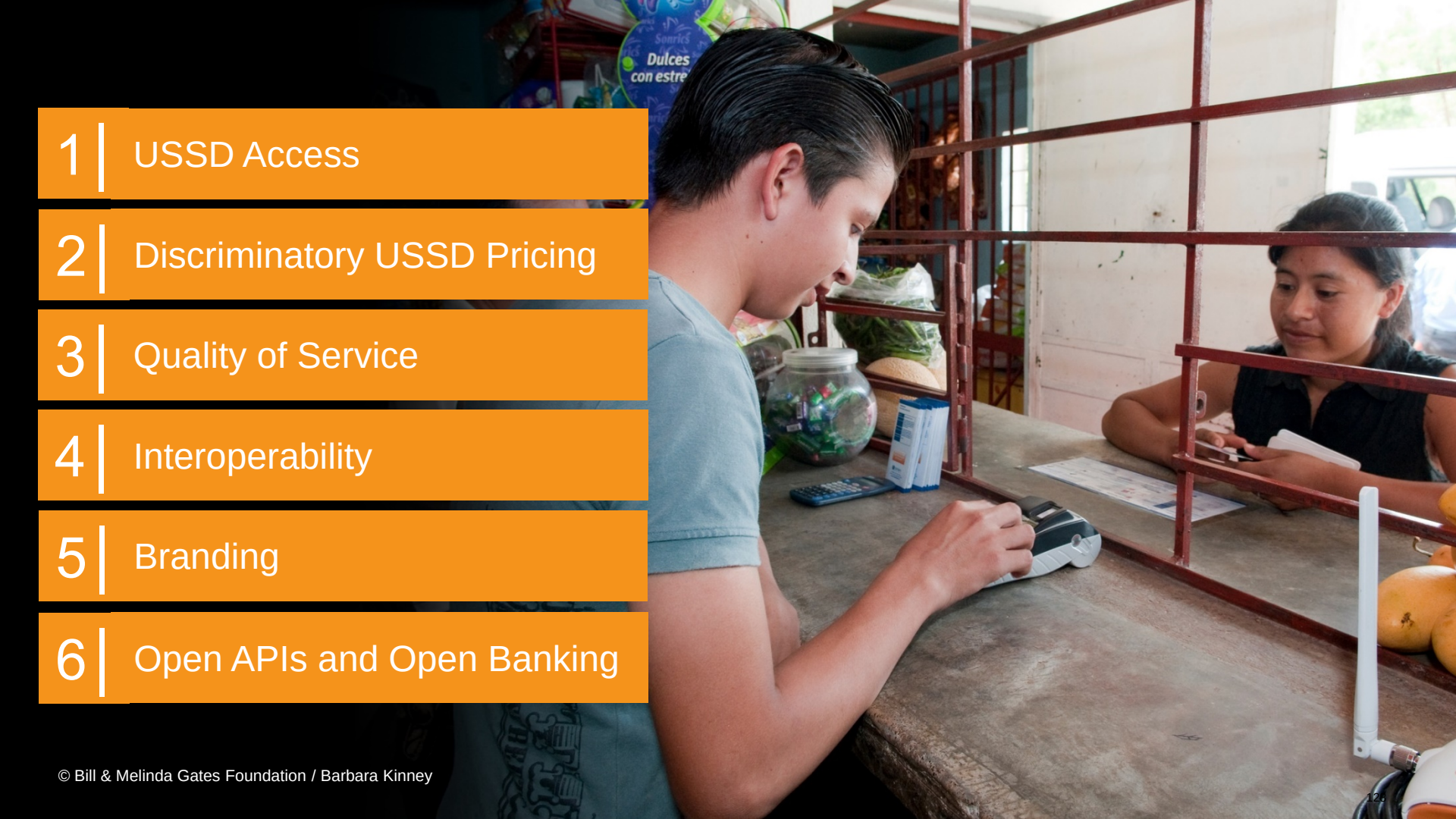
Source: ITU (2017)

1 | USSD ACCESS – ISSUES AND POSSIBLE RESPONSES

Issue:	Possible to address by:
• EMI unable to obtain commercial access to USSD services from MNOs.	• Telco regulator regulates access and pricing for EMIs.
• EMI lacking technical and operational expertise and/or scale to justify connecting to all the MNOs in the country.	• EMI contracts an aggregator who connects the EMI's systems to all MNOs. This enables USSD access to the EMI by its customers from all MNOs' networks.
• Multiple EMIs and payment service providers (PSPs) need access to USSD, but MNO lacks the capacity to deal with all the PSPs.	• MNO appoints an aggregator or aggregators to implement and manage the multiple connections.
• Aggregator gateways located out-of-country on congested and unreliable data links.	• Aggregation services hosted locally, enabling more reliable USSD for the MNOs, financial institutions, and/or EMIs.

1 USSD ACCESS – ISSUES AND POSSIBLE RESPONSES

Issue:	Possible to address by:
• MNOs may disrupt the mobile channel provision market by providing better-performing USSD services to their own EMI operations than to their mobile money competitors.	• MNOs applying for an EMI License (whether directly or through a subsidiary) could be required to contractually commit to equal service provision with respect to USSD access and service (and for SMS and data as well) for related and unrelated EMIs. • Specifically, the MNO in its role as a telecommunication provider could be required to contractually commit to supply the same USSD service to its EMI competitors as the MNO supplies to its own operations.
• MNOs with existing EMI licenses provide discriminatory services to other EMIs using the MNO's USSD and SMS services.	• Where competition law can be applied, the activities of an MNO in its role as telecommunication services provider can be subjected to scrutiny for discriminatory provision and vertical integration.
• MNOs exploit points of arbitrage between the financial and telecommunication regulators to provide lesser-quality telecommunication services to their EMI competitors.	• Financial and telco regulators may wish to sign an MoU governing e-money cooperation (see here for a template).



1 | USSD Access

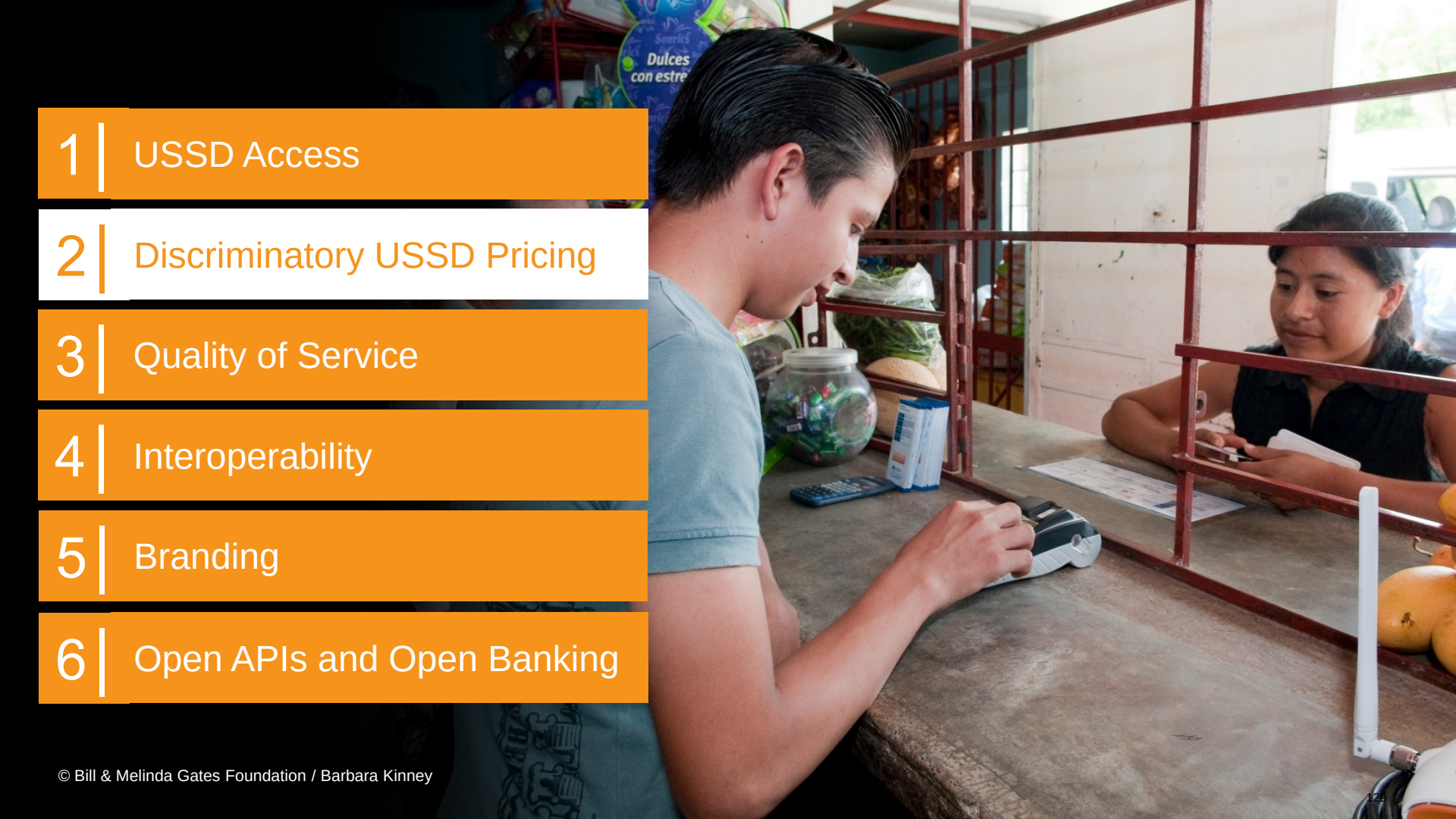
2 | Discriminatory USSD Pricing

3 | Quality of Service

4 | Interoperability

5 | Branding

6 | Open APIs and Open Banking



2 DISCRIMINATORY USSD PRICING

MNOs set prices for USSD access, typically either for a fixed monthly access fee or on a per-session basis (for each transaction, e.g., money transfer, balance inquiry, etc.).

Risk

Discriminatory pricing can be abusive if undertaken by a firm with significant market power. MNOs with such market power may engage in discriminatory USSD pricing to:

- Discourage competition in the e-money sector by:
  1. offering low- or no-cost USSD services to affiliates; and
  2. charging high prices to competitors.
- Maximize profits by charging high prices for access to a required resource for offering e-money to the mass market.

2 DISCRIMINATORY USSD PRICING
COUNTRY EXAMPLES

In **Kenya** in 2014, the cost of providing a USSD channel session was a fraction of a Kenyan Shilling, yet Safaricom, which had dominant market share, was charging most banks and third parties KES 4-10 (see next slides).

Source: CGAP (2016)

In **Zimbabwe**, Econet initially refused USSD channel access to banks for P2P mobile banking and then charged much higher prices than for Ecocash customers.

Source: Chronicle (2014)

MNOs in **Kenya** and **Tanzania** are zero-rating USSD costs for partner banks while charging competitors full price.

Source: CGAP (2016)

In **Uganda**, an inquiry commissioned by the Communications Commission concluded that Airtel and MTN's USSD prices "*are set at excessive rather than competitive levels…*"

Source: Macmillan Keck (2017)

2 DISCRIMINATORY USSD PRICING IN KENYA

Table 1: Survey of costs of USSD access paid by MFS providers to MNOs in Kenya (August 2014)

	MNO 1		MNO2		MNO 3		MNO 4	
	Cost (Ksh)	Duration (seconds)	Cost (Ksh)	Duration (seconds)	Cost (Ksh)	Duration (seconds)	Cost (Ksh)	Duration (seconds)
Bank 1	5	180	Monthly access fee		Monthly access fee		Monthly access fee	
Bank 2	4	120	1	180	Not used		Not used	
Bank 3	5	180	No charge		Not used		Not used	
Bank 4	5	180	3	180	Not used		Not used	
Bank 5	5	180	Not used		Not used		Not used	
Bank 6	5	180	Not used		Not used		Not used	
3rd Party 1	5	180	3	180	3	180	2	180
3rd Party 2	10	180						
3rd Party 3 Prepaid	10	180	3	180	3	180	2	180

Cost for USSD access from dominant MNO 1 is 3-5x higher than cost for USSD access from competitors

Source: CGAP (2016)

2 | DISCRIMINATORY USSD PRICING IN KENYA (CONT.)

Table 1: Survey of costs of USSD access paid by MFS providers to MNOs in Kenya (August 2014)

	MNO 1		MNO2		MNO 3		MNO 4	
	Cost (Ksh)	**Duration (seconds)**	**Cost (Ksh)**	**Duration (seconds)**	**Cost (Ksh)**	**Duration (seconds)**	**Cost (Ksh)**	**Duration (seconds)**
3rd Party 3 Postpaid	0.5-1.5	180	3	180	3	180	2	180
Set-Up Costs (where assessed)	100,000		75,000		30,000		50,000	
Monthly Costs (where assessed)	100,000		50,000		10,000		20,000	

While competitors charge same cost for prepaid and postpaid services for user "3rd Party 3", MNO 1 charges 7-20x more for prepaid services.

Source: CGAP (2016)

2 DISCRIMINATORY USSD PRICING
COUNTRY EXAMPLES

Negotiate Pricing with Individual MNOs

In 2017, following intervention by **Kenya's** Competition Authority, Safaricom agreed to reduce USSD session charges from KES 5 (USD 0.05) to KES 1 (USD 0.01).

Source: Business Daily Africa (2017)

Require Non-Discriminatory Pricing

In **Peru**, the telecommunications regulator (Osiptel) requires MNOs to offer non-discriminatory pricing for USSD access. To help ensure this, Peru requires MNOs to set up a separate legal entity for e-money issuance.

Source: ITU (2017)

In **Colombia**, MNOs must provide access to their channels (including USSD) to e-money issuers on a non-discriminatory basis. The telco regulator can accept and review complaints regarding price and quality on a case-by-case basis.

Source: GSMA (2015); ITU (2017)

Set Prices for USSD Sessions

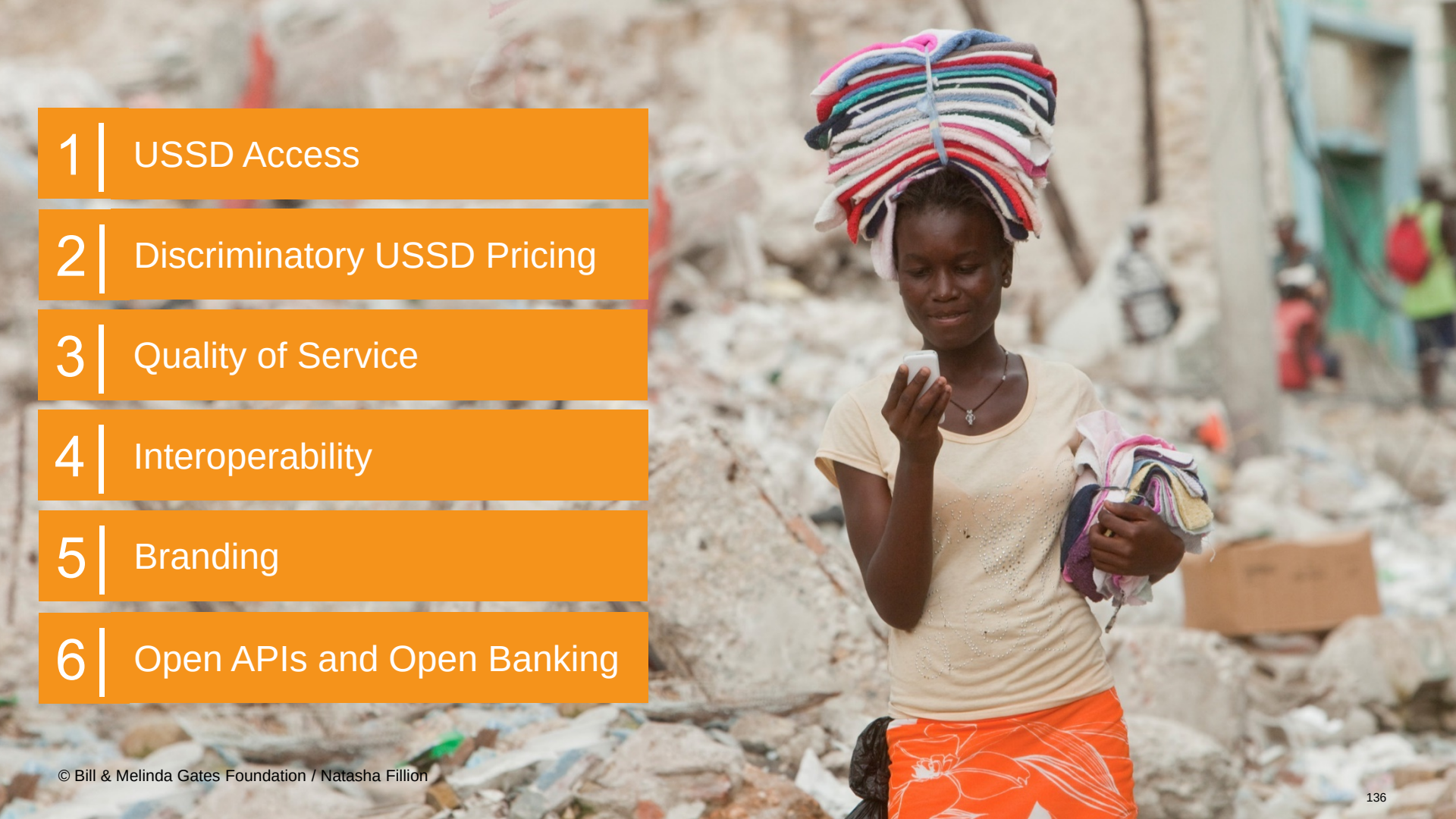
In **India**, the Telecommunications Regulatory Authority established a ceiling of INR 1.50 (USD 0.02) per USSD session in 2013 and then reduced the ceiling to INR 0.50 (USD 0.007) in 2016 to encourage uptake.

In addition, India has created a National Unified USSD Platform (NUUP) to enable USSD access for all banks.

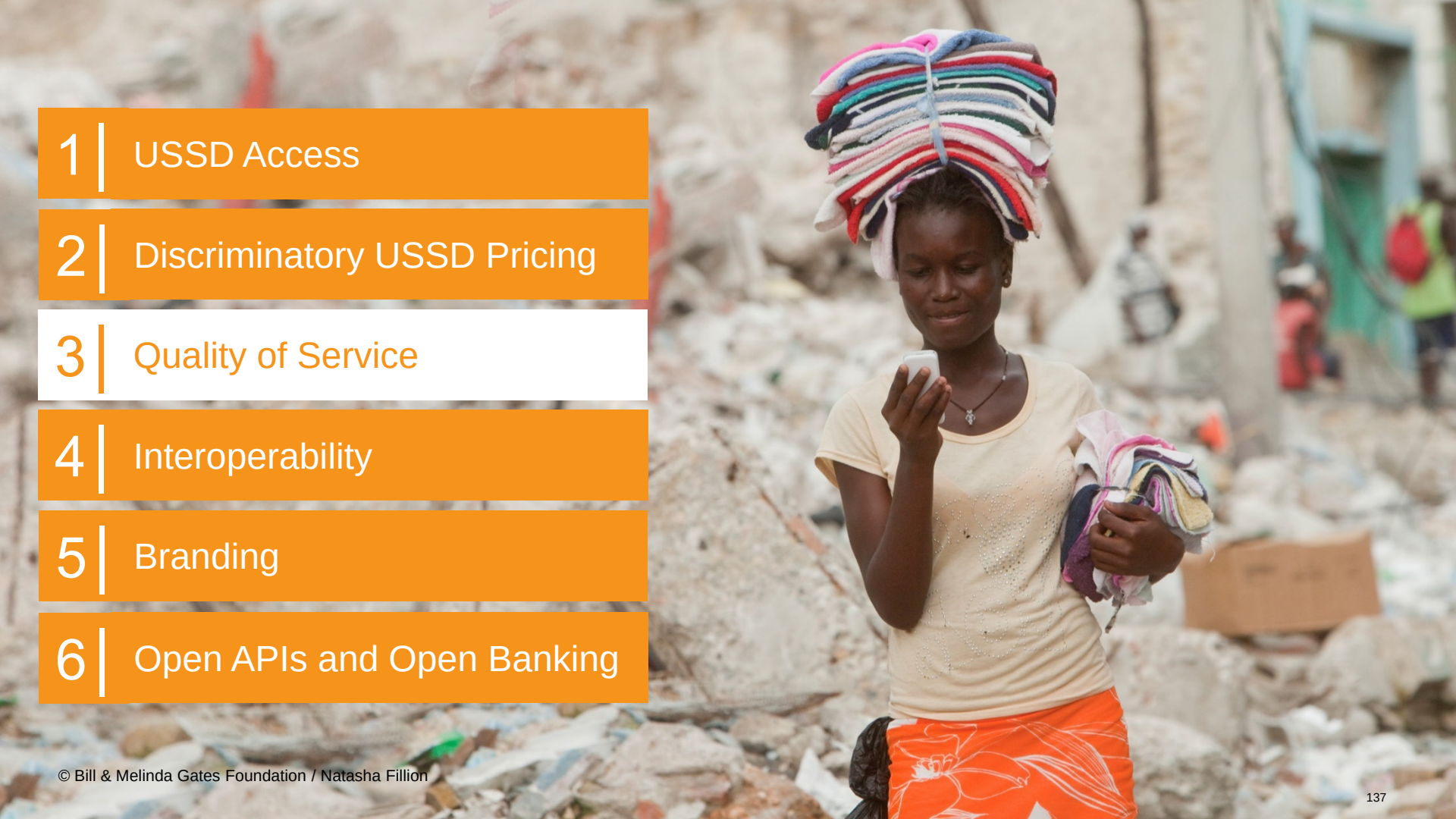
Source: TRAI (2016); Financial Express (2016)

Considerations

- As a first measure, financial regulators could require MNOs to price USSD services exactly the same for related and unrelated EMIs.
- Telco regulators also could review complaints regarding USSD pricing and share EMI-related complaints with the financial regulator.
- Setting USSD floors and/or ceilings requires a detailed inquiry into industry costs and could impede market development. Given the inherent costs and risks, regulators may wish to consider setting prices only if market-based efforts are unsuccessful.
- Financial and telco regulators could sign an MoU governing e-money cooperation (see here for a template). They could then jointly review complaints regarding USSD pricing and consider potential responses, as appropriate.



1. USSD Access
2. Discriminatory USSD Pricing
3. Quality of Service
4. Interoperability
5. Branding
6. Open APIs and Open Banking



1. USSD Access
2. Discriminatory USSD Pricing
3. Quality of Service
4. Interoperability
5. Branding
6. Open APIs and Open Banking

Issue

Failure to complete USSD interactions (sessions) results in user frustration as well as uncertainty as to whether transactions have completed

Examples of USSD session failure issues affecting user transactions include:

- Session timeouts
- Dropped sessions
- Insufficient number of stages per USSD session

There are, however, different reasons why a session may not complete, only some of which are related to the MNO's delivery of a USSD session (MNO QoS)

For example:

- Customer may abandon a transaction (user issue)
- Customer may move into a network dead zone during session and lose connectivity (network service issue)
- EMI may not respond (provider issue)
- Network may fail during the session (network issue)

Therefore, **regulators should be cautious when considering establishing USSD session QoS requirements**, as (i) not all USSD session failures are network-related; and (ii) some failures are due to multiple indistinguishable causes, some network-related and others customer- and/or EMI-related.

3 | QUALITY OF SERVICE – VOICE VS. USSD

Issue

USSD QoS issues are different from voice QoS issues, so voice QoS performance measures cannot be directly applied to USSD.

Some QoS issues are directly comparable while others are not, so USSD performance measures must be carefully designed to be both **measurable** and **attributable**.

Some voice call and USSD session failure modes are different

- Failure to hand over from one base station to another: For voice, this is determinable from network statistics. USSD sessions cannot be handed over, so moving between cells is seen as a loss of contact.
- Session timeouts: Voice calls cannot timeout. USSD session timeouts can be determined, but there are multiple potential causes.

Common voice call and USSD failure modes

- Inability to establish a call or USSD session: This is a common failure, but is not determinable from network statistics as the network ‘never finds out’ about the attempt.
- Mid-call and mid-USSD session failure: Loss of communication due to network failure.

3 | QUALITY OF SERVICE – ACTIVE DISCRIMINATION

Risk

Provision of lower-quality service to competitors by an MNO (or cartel) with dominant or significant market power can negatively impact competition.

Telco regulators should have (i) **the means** to test for service manipulation; and (ii) **the power** to sanction MNOs and require MNOs to restore full contracted service.

Examples of active USSD quality of service (QoS) degradation include:

- Session length reduction
- Bandwidth throttling to USSD gateway
- Claimed unavailability by the USSD gateway
- Limitation of number of concurrent sessions in USSD gateway

Manipulations can be found through testing:

- Most manipulations can be independently tested for from USSD test devices that transact over USSD, without actually internally auditing the USSD arrangements in the MNO.

3 QUALITY OF SERVICE
COUNTRY EXAMPLES

Colombia

In **2016**, the Communications Regulatory Commission issued draft regulations proposing the following USSD QoS requirements:

- 99% of USSD sessions successfully completed.
- 99% of USSD requests received at the destination terminal within less than 5 seconds.

The final issued regulations did not include USSD QoS requirements.

NOTE: Enforcement of such requirements would face challenges with respect to attributability (see next slide).

India

Some banks complained that limits on the number of stages per USSD session were insufficient for mobile banking purposes.

- In response, in **Nov. 2016**, the Telecommunications Regulatory Authority increased the minimum number of stages per USSD session from five to eight.

Strictly speaking, this is not a QoS issue, but rather a mismatch of the maximum provided stages and the required stages. Resolvable by process optimization and/or increase of stages.

Analysis of regulatory approach

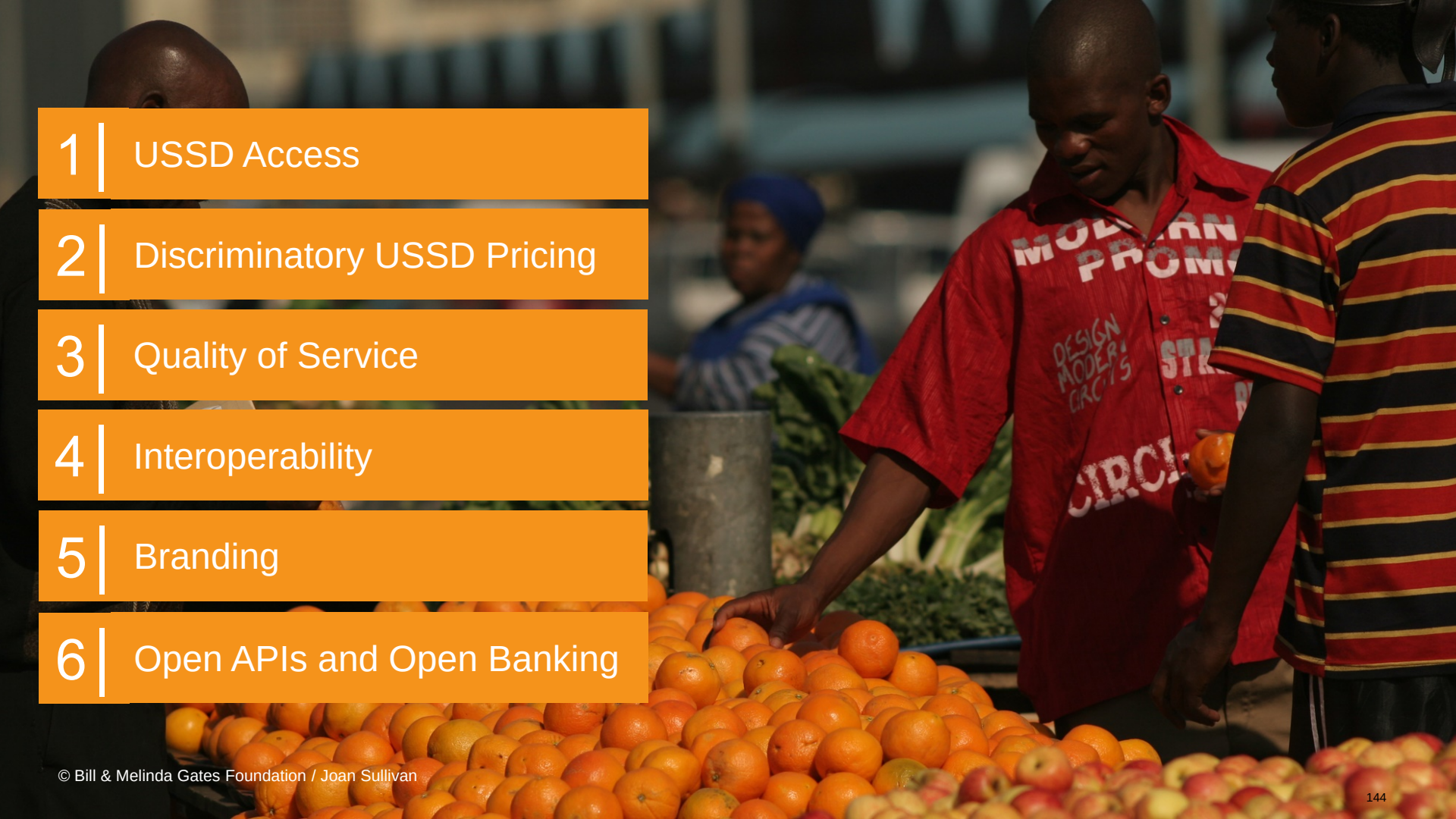
Quality of Service Standards when established to address USSD quality of service (QoS) must be **measurable** and **attributable**

Measuring Quality of Service (QoS)

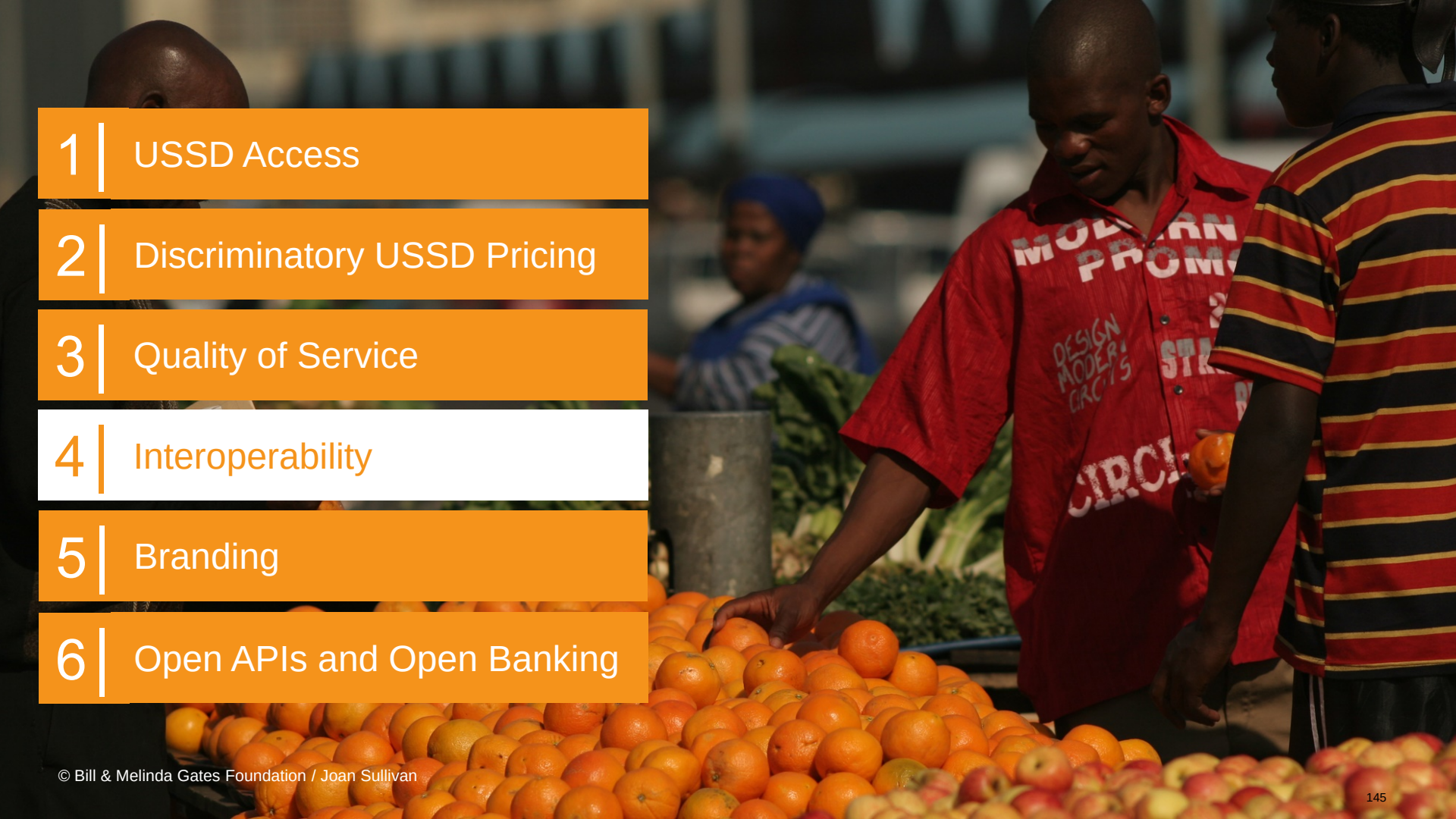
- In practice, it is difficult to enforce QoS standards such as Colombia's draft requirements.
- When a USSD session with an EMI fails, there are many possible reasons, some of which are related to the MNO's QoS and others due to elements such as:
  - Users being too slow or abandoning sessions
  - USSD aggregators having performance and reliability issues
  - EMIs themselves being slow to respond or not responding at all
- Unless the reason for failure can with certainty be attributed to the MNO, fairly measuring and enforcing MNO performance with respect to QoS Metrics is not possible.

Considerations

- There is currently no publicly available failure cause analysis of USSD to use as a basis for setting QoS standards for MNOs and USSD aggregators.
- There are many elements where failure could lead to a failed USSD session, including the handset, the mobile network, USSD aggregators, data communication lines between the MNO and the EMI, the USSD menu server, and the EMI's own systems. Each element in this chain would need its own QoS standard.
- Failure cause analysis should only be undertaken if it is coupled with a determination of (i) whether the cause is measurable/discernable; and (ii) if so, whether it is attributable to a specific party.
- Failure causes that are attributable to specific parties could be included in QoS requirements, with the party identified and the performance metric specified.
- A QoS standard for USSD-delivered services could be jointly developed by telecommunications and financial regulators. These regulators could sign an MoU governing e-money cooperation (see here for a template). They could jointly review complaints regarding USSD QoS and consider potential responses, as appropriate.



1. USSD Access
2. Discriminatory USSD Pricing
3. Quality of Service
4. Interoperability
5. Branding
6. Open APIs and Open Banking



1. USSD Access
2. Discriminatory USSD Pricing
3. Quality of Service
4. Interoperability
5. Branding
6. Open APIs and Open Banking

Issue

In the absence of a specific mandate to interoperate, many e-money markets lack payment scheme interoperability.

Dominant e-money providers often resist efforts to promote interoperability (typically to maintain a competitive advantage, but sometimes for other reasons such as prioritization of resource allocation).

Interoperability can be beneficial, but issues such as (i) timing, (ii) technical and commercial models, and (iii) role of authorities are very important and country-specific.

Interoperability is not a panacea. Many markets achieved high levels of e-money uptake without interoperability (e.g., Ghana, Kenya, Rwanda, Uganda), while many interoperable markets have low e-money uptake (e.g., Indonesia, Nigeria, Pakistan, Sri Lanka).

Arguments for mandating interoperability

Ease of use

Interoperability can make it easier for customers to use e-money and other DFS.

Competition

In mature markets with a dominant provider, lack of interoperability can serve as a barrier to effective competition.

Cost

By increasing competition and streamlining cross-net transfers, interoperability could eventually lead to lower customer costs.

Arguments for not mandating interoperability

Investment

Mandating interoperability in the early stages of market development could disincentivize investment by first movers that perceive this as a threat to their ability to recoup initial investments.

Opportunity cost

Implementing interoperability requires significant time and resources, which could affect other initiatives aimed at promoting market development.

Commercial viability

Mandating the technical and/or commercial model for interoperability could result in a solution that is not commercially viable.

Option #1: Require interoperability to be technologically feasible at low cost

Tanzania

The TCRA required MNOs' systems to have the capacity to be interoperable and to adhere to international standards. With encouragement from the BoT, TZ's three major e-money providers voluntarily interoperated (first Airtel and Tigo in Feb 2015, with Vodacom joining a year later). Payment scheme interoperability quickly led to an increase in cross-net transfers.

Kenya

The NPS Regulations require PSPs to use systems "*capable of becoming interoperable with other payment systems in the country and internationally*." In May 2017, the country's e-money providers agreed to interoperate within three months. Eventually, interoperability went live in April 2018.

Option #2: Mandate interoperability but be flexible regarding business model and timing

Rwanda

- After initially setting strict timelines (by 2013) for interoperability, in 2014 the National Bank of Rwanda (NBR) issued an Interoperability Policy in which it recognized that "*different payment systems are at different stages of market development*" and therefore "*there are differences in the speed and priority with which interoperability may be achieved*."
- Since then, the NBR has engaged with e-money providers to promote interoperability. Two of the three major providers (Airtel and Tigo) piloted interoperability in 2015, but the largest (MTN) did not join.
- In August 2018, it was reported that the three major e-money providers were seeking regulatory approval to launch interoperable services.

Option #3: Mandate the timing, technical model, and commercial model for interoperability

Nigeria

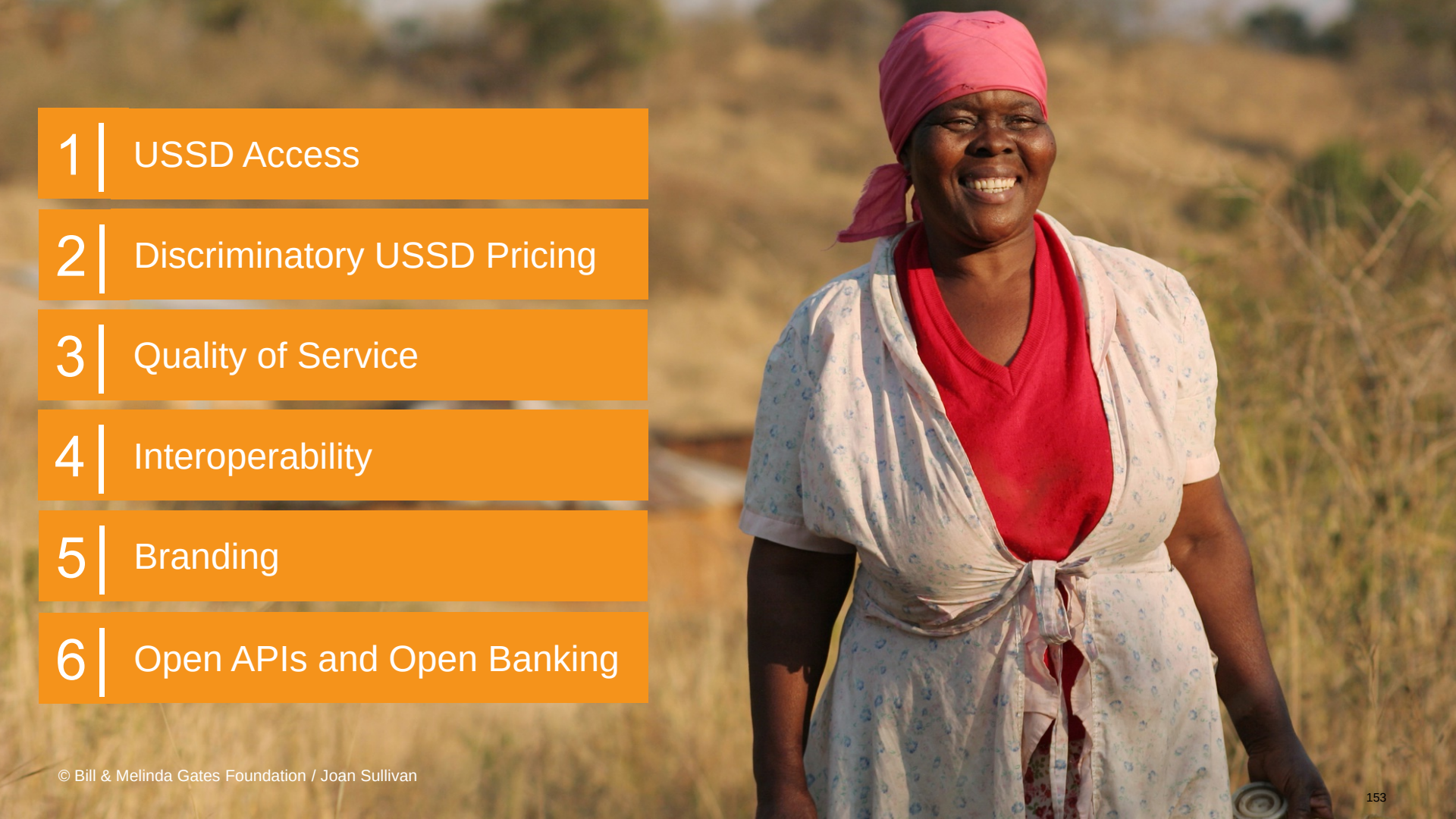
- Per Circular BPS/DIR/GEN/CIR/01/014, EMIs were required to connect to the national central switch for real-time credit-push instant payment by end Feb 2013.
- However, in a 2016 test, ¾ of interoperability transactions were unsuccessful.
- Reasons for not enabling interoperability included (i) cost, (ii) fear of inability to recoup investments, (iii) loss of competitive advantage, and (iv) perceived lack of industry readiness.

Ghana

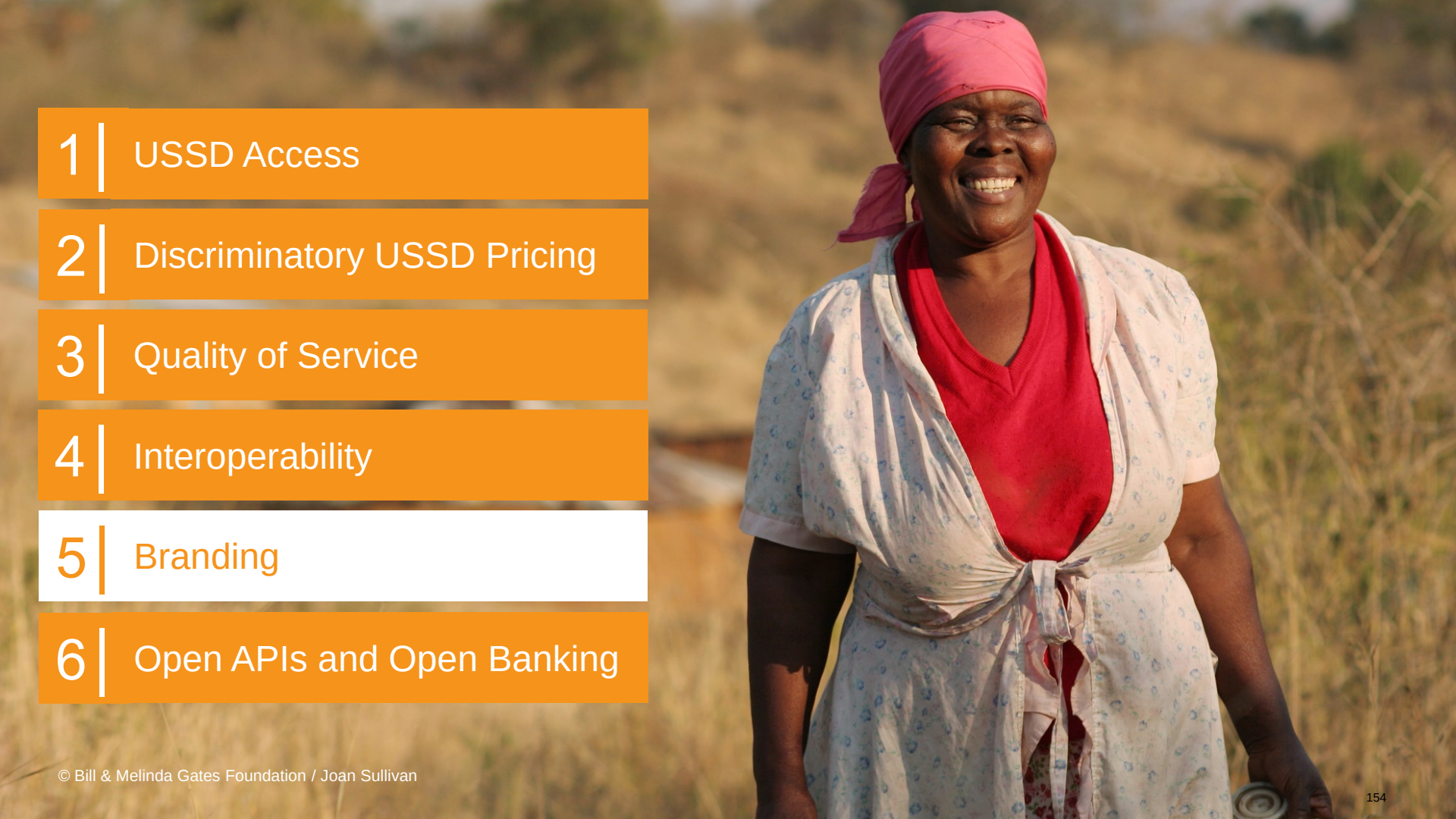
- In 2008, the Bank of Ghana issued Guidelines on Branchless Banking that required banks and MNOs to (i) collaborate on a fully interoperable branchless banking ecosystem and (ii) process all transactions through the national central switch.
- After several years of tepid growth and investment, the Bank of Ghana, citing "*unintended negative consequences*," issued revised E-Money Guidelines eliminating the interoperability requirements and enabling MNOs to establish EMI subsidiaries.

Considerations

- In many cases, a **market-driven approach to interoperability** will ensure that the timing, technical model, and commercial model for interoperability make sense for EMIs.
- Efforts by regulators to dictate the **technical and commercial models** for interoperability may result in an approach that is not commercially viable and lacks provider buy-in.
- With respect to **timing,** regulators may wish to **strike a balance** that encourages investment in the early stages of market development, while monitoring the market for signs that lack of interoperability is hampering competition and/or market development.
- If regulators determine that lack of interoperability is a key barrier to competition and/or market development, they could first engage with EMIs to develop a **mutually agreeable plan** for implementation of interoperability.
- If market-led solutions in a well-developed market are **unsuccessful due to resistance from a dominant player**, regulators could consider a more interventionist approach that is carefully designed to avoid disincentivizing investment and innovation.



1. USSD Access
2. Discriminatory USSD Pricing
3. Quality of Service
4. Interoperability
5. Branding
6. Open APIs and Open Banking



1 | USSD Access

2 | Discriminatory USSD Pricing

3 | Quality of Service

4 | Interoperability

5 | Branding

6 | Open APIs and Open Banking

Issue

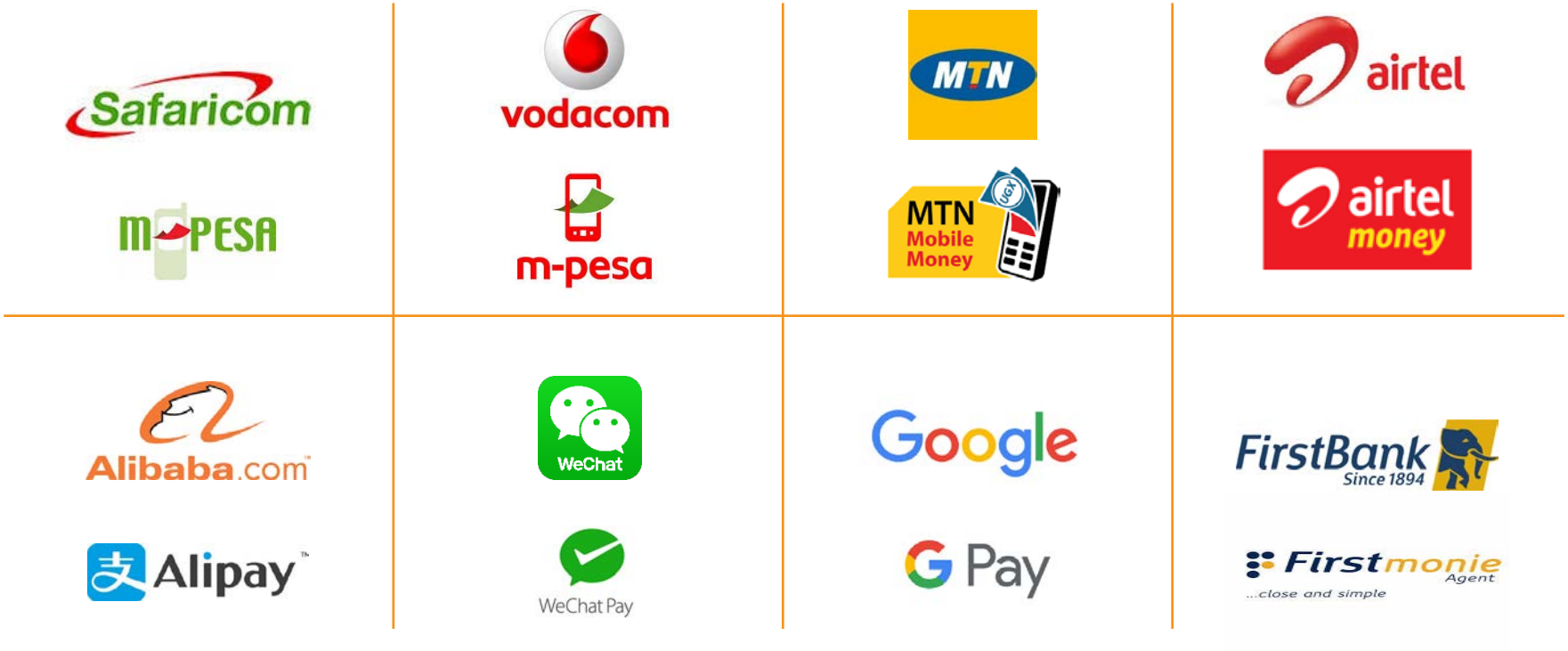
Should EMIs operated by MNOs, banks, or “superplatforms” (e.g., Google, Facebook, WeChat) – whether directly or via a subsidiary – be permitted to use their branding for the EMI service?

Arguments for permitting use of branding

- Incentivizes investment by the parent company
- Parent company may offer better customer service to protect overall brand reputation
- Customers may feel more confident adopting service if they trust the parent company

Arguments for prohibiting use of branding

- Could create confusion regarding legal status of e-money service and associated protections (e.g., applicability of deposit insurance)
- Enabling companies to leverage their brand in a parallel market could offer a competitive advantage that some might deem unfair



Disclaimer: All logos are the property of the respective organizations and are provided for illustrative purposes only.

Ethiopia

Banking Business Proclamation

Part Two, Art. 3.2: *No person shall use the word 'bank' or its derivatives as part of the name of any financial business unless it has secured a license from the National Bank.*

Regulation of Mobile and Agent Banking Services

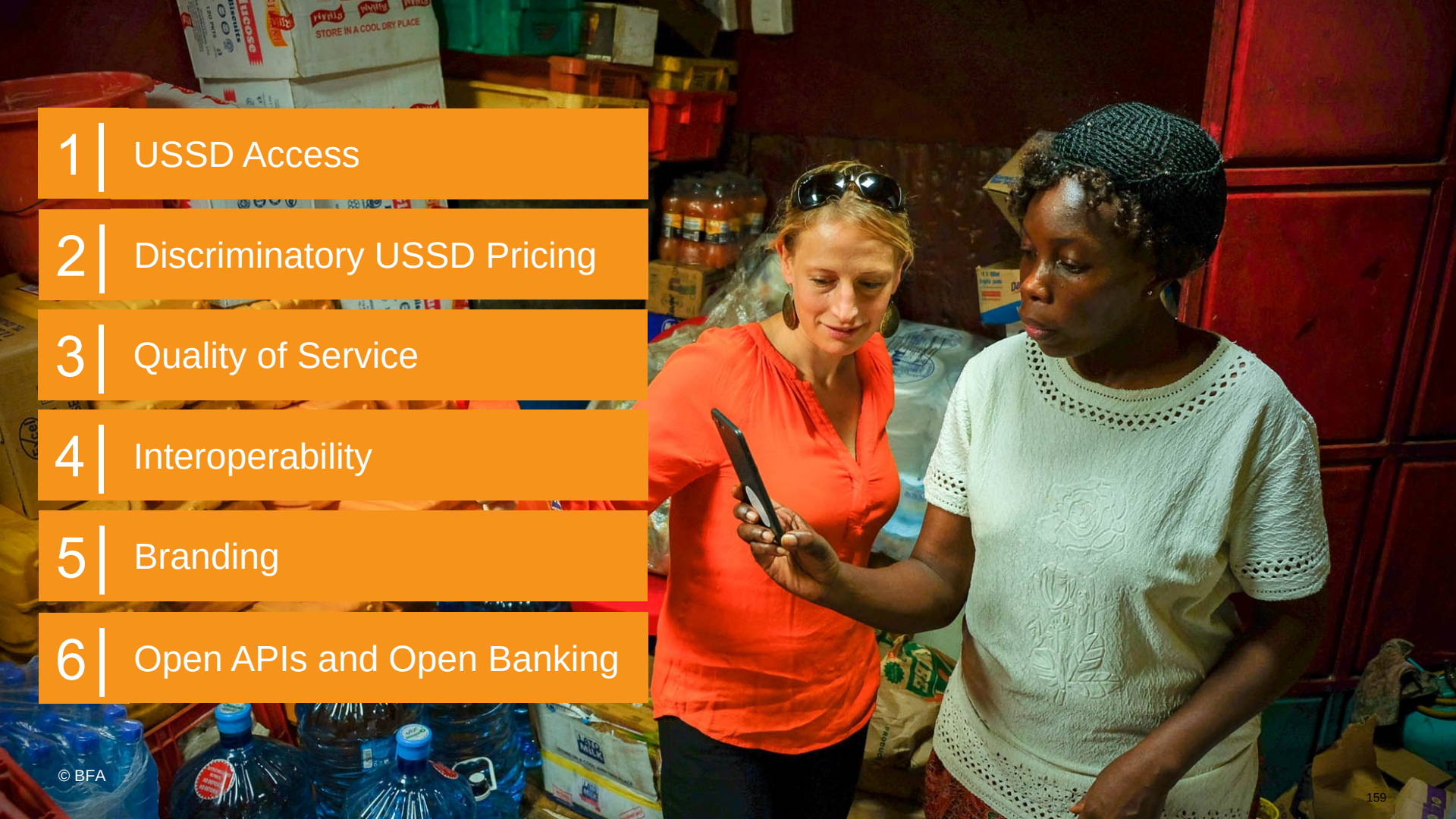
9.2.5: *In branding agent network, financial institution shall avoid use of words like bank, microfinance, financial intermediary, microfinance bank or any other word that might suggest that the agent by itself is a financial institution.*

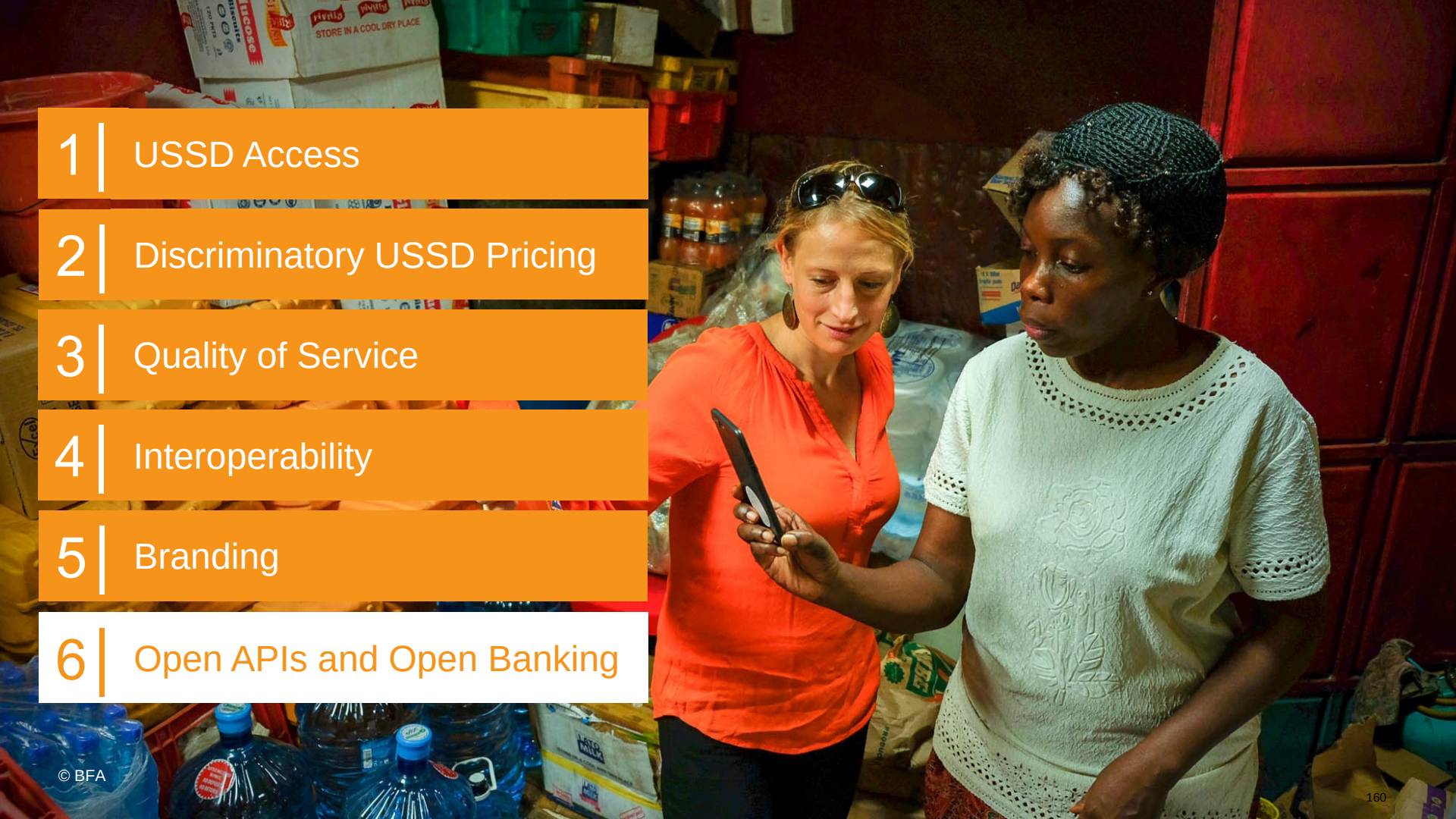
Issue

Should EMIs operated by MNOs, banks, or “superplatforms” (e.g., Google, Facebook, WeChat) – whether directly or via a subsidiary – be permitted to use their branding for the EMI service?

Considerations

- Allowing established MNOs, banks, superplatforms, and others to use similar branding for their e-money service could promote uptake and incentivize investment.
- Where applicable, properly disclosing to customers that e-money and similar services lack comparable protection to bank products (e.g., deposit protection) could help ensure that customers are not misled by similar branding.
- Clearly labeling agent locations could help to ensure that customers are aware that they are not interacting directly with parent company staff.


1 USSD Access
2 Discriminatory USSD Pricing
3 Quality of Service
4 Interoperability
5 Branding
6 Open APIs and Open Banking



1 | USSD Access

2 | Discriminatory USSD Pricing

3 | Quality of Service

4 | Interoperability

5 | Branding

6 | Open APIs and Open Banking

Issue

Open APIs and open banking offer the potential to stimulate competition and innovation and accelerate financial inclusion.

Application Programming Interfaces (APIs) are interfaces that enable machines to communicate with one another:

- **Private APIs** are interfaces between a closed network of computers.
- **Public APIs** enable providers to allow access to carefully selected outside parties.
- **Open APIs** are public APIs with automated, streamlined onboarding processes to enable outside parties to quickly (i) access and integrate with a provider's interface; and then (ii) test and launch connected services.

Open APIs can make it much easier for Fintech firms and others to connect to EMIs and other DFS providers, thereby catalyzing innovation in the DFS space.

Source: BFA (2016)

How open APIs can foster innovation

By dramatically reducing the time and cost for outside developers to integrate with DFS providers, open APIs can foster innovation, extend customer outreach, and increase revenue.

- With traditional public APIs, developers are selected through a lengthy manual process that requires significant face-to-face interaction and bespoke paperwork.
- With open APIs, developers can register online, test their product using an online “sandbox”, and request authorization through an automated, streamlined process, reducing approval times from months to days.
- Shifting from traditional public APIs to open APIs can attract small, innovative Fintechs and rapidly grow the market for a DFS provider’s core products.

Example: In Nov 2018, MTN Uganda launched its MoMo API to facilitate development and integration of applications using MTN Mobile Money for collections, merchant payments, disbursements, and remittances.

Issue

Open APIs and open banking offer the potential to stimulate competition and innovation and accelerate financial inclusion.

Open Banking gives individual customers the power to allow third parties to access their financial data. Potential benefits include:

- **Competition:** Requiring banks and other payment account providers to let customers share data can facilitate competition for customers' business.
- **Innovation:** Open Banking can enable Fintech firms to harness the power of data analytics to develop innovative financial products, either directly or in partnership with other licensed financial service providers.
- **Inclusion:** With a fuller picture of customers' financial lives, providers can better assess customer needs and identify potential opportunities for improved financial health and inclusion.

Source: PwC (2018)

6 OPEN APIS AND OPEN BANKING

OPEN BANKING COUNTRY EXAMPLES

European Union

In January 2016, the EU published the Revised Payment Services Directive (PSD2). As of January 2018, PSD2 requires all providers of payment accounts to provide third parties with access to customer accounts (with proper consent) via open APIs to share account information and initiate payments.

Source: PwC (2018)

United Kingdom

In February 2016, the UK developed initial Open Banking standards aimed at standardizing how banking data should be shared under PSD2 and facilitating the creation of an Open Banking ecosystem. In January 2018, the 9 largest UK providers of current accounts were required to provide standardized open API access under this system.

Source: PwC (2018)

Other Countries

A number of other Open Banking-related initiatives are being developed around the world, such as the Berlin Group API standardization initiative (Germany and other W. European countries), Australia's Consumer Data Right, Mexico's FinTech Law, and the US National Automated Clearinghouse Association's API standardization program.

Source: PwC (2018)

Considerations

- Open APIs and open banking offer great potential for fostering innovation and promoting the development of digital financial services for low-income customers around the world.
- At the same time, open banking initiatives are in the early stages of development, so a consensus around good practices does not yet exist.
- Financial authorities in developing countries could monitor the experiences of early adopters of open banking initiatives and evaluate the readiness of their financial sector (and their supervisory capacity) to launch similar initiatives.
- Concurrently, policymakers could work to create an enabling environment for Fintech innovation to prepare for a world of open APIs and open banking.

INTEGRITY & SECURITY

1 | AML/CFT Requirements

2 | AML/CFT Training for Agents

3 | Cybersecurity

1 | AML/CFT Requirements

2 | AML/CFT Training for Agents

3 | Cybersecurity

MONEY LAUNDERING / TERRORIST FINANCING RISK

Risk

Compared to cash, use of e-money increases certain money laundering (ML) and terrorist financing (TF) risks while reducing others.

Four key money laundering risks

- **Anonymity:** Customer's identity is unknown
- **Elusiveness:** Ability to disguise amount, origin, and destination.
- **Rapidity:** Speed at which funds are transferred.
- **Oversight:** Extent and quality of oversight.

Compared to cash, e-money poses greater risks with respect to rapidity but lower risks with respect to anonymity, elusiveness, and oversight (see next slide).

Source: World Bank (2008)

ML/TF RISK: E-MONEY VS. CASH

- Indicates ML/TF Risk is Highly Prevalent
- Indicates ML/TF Risk is Somewhat Prevalent
- Indicates ML/TF Risk is Low

Risk factor	Mobile money			Cash	
	Before	Controls	After		
Anonymity: Customer's identity is unknown	●	• Transactions linked to a unique mobile number • Transactions recorded (sender's mobile number, amount, receiver's mobile number, date) • Transactions traced • CDD and customer profile building	●	●	• It's anonymous • There is neither a unique identifier for the user nor a way to trace the payment
Elusiveness: Ability to disguise amount, origin, and destination	●	• Mobile money transactions are clearly traceable in the mobile money provider's system as part of standard business practice • Mobile number of the sender and receiver, the time, and the amount of the transaction are all known to the mobile money provider • Limits on maximum balance and on amount, frequency and number of transactions • Real-time monitoring	●	●	• Elusive

Source: GSMA (2015)

ML/TF RISK: E-MONEY VS. CASH

- Indicates ML/TF Risk is Highly Prevalent
- Indicates ML/TF Risk is Somewhat Prevalent
- Indicates ML/TF Risk is Low

Risk factor	Mobile money			Cash	
	Before	Controls	After		
Rapidity	🔴	• Real-time monitoring • Restrictions on transaction frequency • Restrictions on transaction amount and total account turnover in a given period	🟡	🟢	• Slower than mobile
Lack of oversight or poor oversight	🟡	• Mobile money providers are properly regulated and supervised • MNOs put in place strict internal controls with regular internal and external auditing	🟢	🔴	• None: cash transactions lack oversight

Source: GSMA (2015)

MONEY LAUNDERING / TERRORIST FINANCING RISK

Risk

E-money raises specific ML/TF typologies that need to be properly mitigated

Key e-money actors that may be involved in ML/TF

- Customers
- Agents
- Merchants
- Employees

The following slides describe the primary ML/TF typologies for customers, agents, merchants and employees, along with measures that could be taken to mitigate these risks.

MONEY LAUNDERING / TERRORIST FINANCING RISK

KEY E-MONEY ML/TF TYPOLOGIES: CUSTOMERS

Typology	Mitigation measures
Fraudulent registration	System controls, development of national ID
Multiple registrations	Central ID verification database, development of national ID, limit of number of accounts per person, SIM registration
Transfer of service after registration	ID requirement for certain transactions, geographic monitoring, PIN authentication.
Loading with PoC	Risk-based transaction and balance limits, transaction monitoring systems, PIN authentication, ability to locate mobile device via MSISDN and IMSI.

Typology	Mitigation measures
Transfer of PoC to co-conspirators	Risk-based transaction and balance limits, transaction monitoring systems to detect anomalous activity.
Use of PoC to purchase from sellers	
Pooling PoC in single account	
Withdrawal of PoC	
Transfer to/from terrorists	Use of international and domestic watchlists.

Source: GSMA (2015). PoC = Proceeds of Crime.

MONEY LAUNDERING / TERRORIST FINANCING RISK

KEY E-MONEY ML/TF TYPOLOGIES: AGENTS & MERCHANTS

Typology	Mitigation measures
Agent allows PoC to be cashed in or out from account	Proper criteria for agent selection, ongoing agent due diligence (automated transaction monitoring, in-person mystery shopping), sharing of agent blacklists.
Agent fails to fulfill due diligence obligations	
Agent allows customers to exceed cash-in or cash-out limits	Proper automated system controls that may not be overridden by agents.

Typology	Mitigation measures
Complicit merchant received PoC	Sound criteria for merchant onboarding, proper ongoing due diligence (automated transaction monitoring, in-person mystery shopping).
Fraudulent merchant misappropriates funds	

Source: GSMA (2015). PoC = Proceeds of Crime.

MONEY LAUNDERING / TERRORIST FINANCING RISK

KEY E-MONEY ML/TF TYPOLOGIES: EMPLOYEES

Typology	Mitigation measures
Fraudulent registration of false accounts to facilitate ML/TF	• Proper initial and ongoing staff due diligence • Cross-referencing staff / customer / agent / merchant account details to ID possible • Segregation of duties • Access controls • Audit trails • Transaction monitoring • Effective staff discipline policy • Verification of customer account information • Regular reconciliation of outstanding e-money liabilities and funds kept for repayment
Theft of funds using internal access through, e.g., false transactions, creation of unbacked e-money, theft from dormant accounts	

Typology	Mitigation measures
Allowing PoC to be cashed in or out from account	• Proper initial and ongoing staff due diligence • Effective transaction monitoring systems that can ID suspicious activity (e.g., smurfing, inconsistent behavior, transfer to/from high-risk areas, transfer to/from previously dormant accounts, staff activity on customer/merchant/agent accounts)
Allowing customers to exceed cash-in/out limits	• Proper initial and ongoing staff due diligence • Audit trails that record all internal approvals to override limits or assign customers to higher-tier account

Source: GSMA (2015). PoC = Proceeds of Crime.

TRANSACTION AND BALANCE LIMITS FOR ELECTRONIC MONEY & SIMILAR DFS IN SELECT COUNTRIES (USD)

Risk-based account tiers

Country		Single transaction limit (P2P)	Daily limit	Monthly limit	Annual limit	Maximum account balance
Fiji		None specified, although providers may wish to establish limits for accounts opened with only a 'referee letter' to fulfil the identification requirements. Mobile money provider Digicel has established the following limits:				
		$566	$5,666			
Ghana	*OTC (no ID)**	$48	$119	$597		
	*OTC (with ID)***	$119	$477	$4,774		
	Minimum KYC		$72	$716		$239
	Medium KYC		$477	$4,774		$2,387
	Enhanced KYC		$1,194	$11,936		$4,774
Liberia	*OTC*	$100				
	Level 1		$250	$2,000		$1,000
	Level 2		$1,000	$8,000		$4,000
	Level 3		$2,000	$20,000		$10,000

* OTC clients who lack acceptable ID must be introduced by someone with acceptable ID.

** "Acceptable ID" requirements for OTC clients are equivalent to KYC requirements for Medium KYC accounts. Minimum KYC accounts can be opened with any photo ID, while Medium KYC accounts may only be opened with a national ID, voter ID, national health insurance ID, driver's licence, or passport.

Source: GSMA (2015)

TRANSACTION AND BALANCE LIMITS FOR ELECTRONIC MONEY & SIMILAR DFS IN SELECT COUNTRIES (USD)

Risk-based account tiers

Country	Single transaction limit (P2P)	Daily limit	Monthly limit	Annual limit	Maximum account balance
Russia *No KYC*	N/A (P2P prohibited)	$95 (withdrawals only)	$755		$285
Simplified KYC	$285		$3,775		$1,135
Full KYC	$11,350				$11,350
Philippines			$2,430		
Sri Lanka	No pre-set limits; the regulation requires providers to submit proposed limits for Central Bank approval. The following limits were approved for mobile money provider Dialog:				
Dialog Basic Account	$40				$80
Dialog Power Account	$40 for P2P, $200 for utility payment				$200

Source: GSMA (2015)

MONEY LAUNDERING / TERRORIST FINANCING RISK

SIMPLIFIED DUE DILIGENCE REQUIREMENTS FOR LOW-VALUE DFS ACCOUNTS

Country and account	Simplified due diligence requirements for low-value DFS accounts	Full customer due diligence requirements for regular accounts
Colombia (e-deposits)	Full name, national ID number and issuance date (verified through access to biometric ID database).	Full name, ID number, address, telephone, occupation, employer information.
Honduras (e-wallets)	Full name (as shown on ID card), address, phone number(s) (verified within 30 days through National Register of Persons).	21 requirements, including full name, place/date of birth, type of ID, nationality, sex, address, phone number, occupation, income, assets, marital status, and more.
Afghanistan (e-money)	Any government-issued document, privately-issued document, or other device or practice that identifies an individual.	Full name, father's name, gender, government-issued ID, address, date of birth, nationality, occupation, income/source of income, phone number, and photo.

Source: FATF (2017); GAFILAT (2016); Afghanistan e-money and AML/CFT regulations.

MONEY LAUNDERING / TERRORIST FINANCING RISK
ELECTRONIC KYC (E-KYC) & SIM KYC FOR DFS ACCOUNTS

Country	How e-KYC works
India	Customer provides fingerprint and Aadhaar (unique ID) number and authorization to conduct e-KYC. Provider sends information to Unique Identification Authority of India's server; if it matches, account can be opened instantly.*
Colombia	Banks have access to Registrar of Banks' biometric ID database and can use this database to conduct e-KYC.
Pakistan	All SIMs are biometrically verified and linked to customer identity in National Database and Registration Authority (NADRA). Biometrically verified SIMs can then be used to remotely open entry-level branchless banking accounts in a few seconds.
Kenya	Banks are able to leverage KYC details obtained during SIM and e-money account registration to open entry-level mobile banking accounts remotely. Information obtained from the MNO/EMI is verified against information in the national ID database.

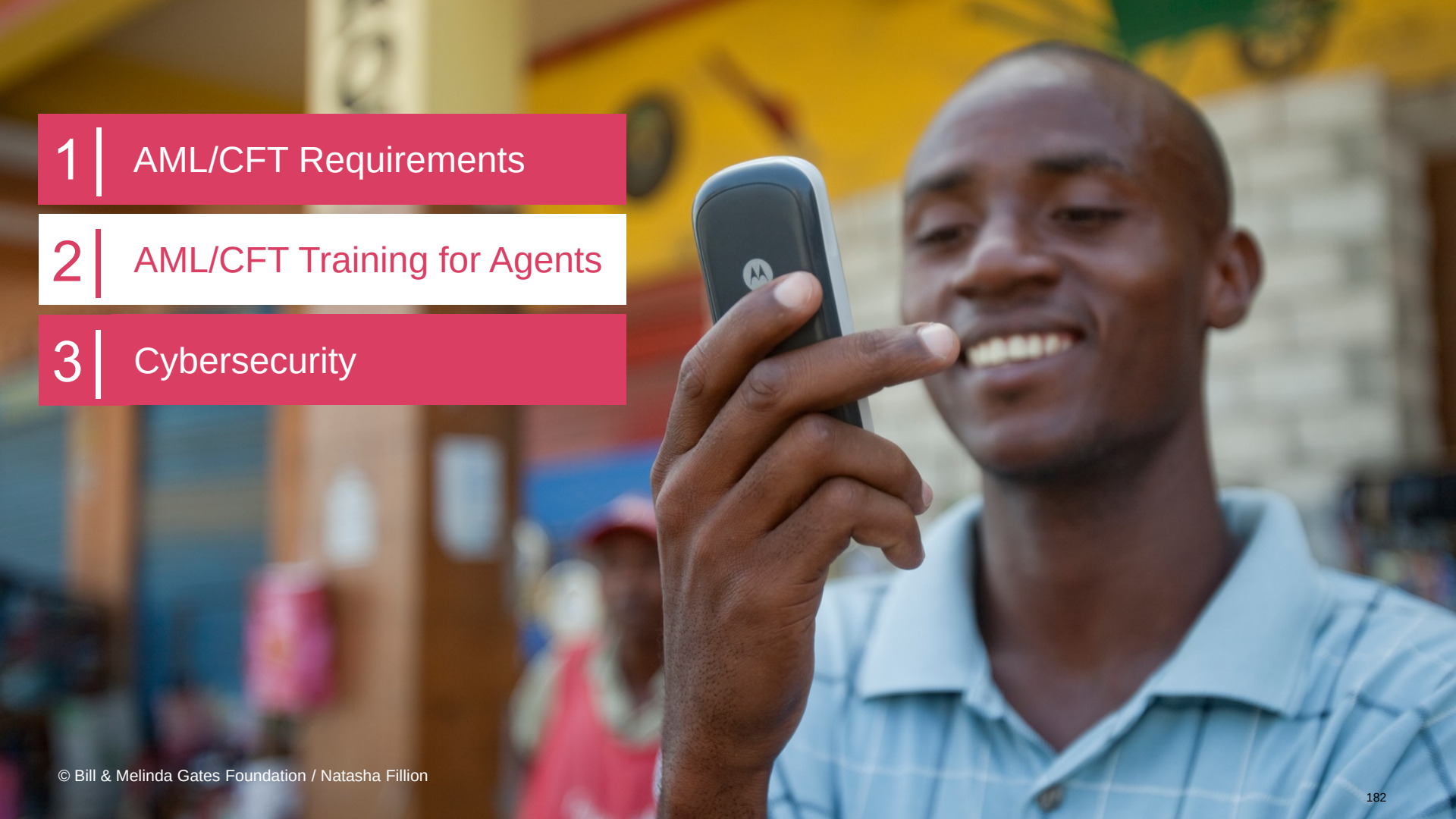
Source: FATF (2017)

* As of Jan 2019, the permissibility of using Aadhaar for e-KYC was uncertain following a decision by India's Supreme Court stating that requiring Aadhaar to open a bank account was disproportionate.

MONEY LAUNDERING / TERRORIST FINANCING RISK

Considerations

- **Risk-based account tiers and digital ID:** Establishing different DFS account tiers with proportionate, risk-based Know Your Customer (KYC) requirements and transaction/ balance limits and supporting the development of digital ID systems that enable remote customer verification (e-KYC) can help facilitate financial inclusion while effectively mitigating ML/TF risk.
- **Transaction monitoring:** ML/TF risk can be reduced by requiring EMIs to use transaction monitoring software with behavior profiling, geographic validation, and other features aimed at identifying suspicious behavior.
- **Supervision:** Steps that regulators could take to strengthen AML/CFT supervision include (i) conducting national and sectoral AML/CFT risk assessments; (ii) building supervisory capacity; and (iii) adopting RegTech tools to improve data collection, processing, and analysis in the AML/CFT supervisory context.



2 | AML/CFT TRAINING FOR AGENTS

While critical to the success of e-money, the use of agents creates certain AML/CFT risks, including the following:

Poorly trained agents may be unaware of AML/CFT good practices and may fail to detect and report suspicious activity.

Poorly vetted agents may collude with others to facilitate transfer of proceeds of crime.

2 | AML/CFT TRAINING FOR AGENTS
COUNTRY EXAMPLES

- The Financial Action Task Force (FATF) considers agents an extension of the regulated entity, so customer due diligence (CDD) is treated as if conducted by the principal EMI.
- The **Central Bank of the Philippines** initially required all new e-money agents to attend a one-day AML/CFT training, which was not widely available outside of Manila. As this was considered a significant barrier to agent registration, the Central Bank now allows e-money issuers to train their agents directly.
- The **Central Bank of Nigeria** requires EMIs to train their agents on AML/CFT requirements. EMIs must share agent AML/CFT policies with the central bank, which also reserves the right to directly inspect agents.

Considerations

- Some of the way that regulators can help to ensure that EMIs properly train their agents with respect to AML/CFT include the following:
  - Holding the EMI responsible for the actions of its agents on its behalf, including with respect to AML/CFT compliance;
  - Requiring EMIs to share AML/CFT policies related to agency business with the regulator before engaging agents; and
  - Reserving the right to directly inspect agents and to examine records or data held by agents.

1 | AML/CFT Requirements

2 | AML/CFT Training for Agents

3 | Cybersecurity

1 | AML/CFT Requirements

2 | AML/CFT Training for Agents

3 | Cybersecurity

Issue

Like all electronic payment providers, EMIs and other DFS providers face cybersecurity threats that must be properly mitigated.

- **Cybersecurity** and **operational security** are closely related.
- **Insider risk** is a major challenge for both cybersecurity and operational security.

Key cybersecurity risks include:

- **Business-related risks:** Risks to the integrity and ongoing operation of the e-money service.
- **Customer-related risks:** Risks to customer funds and their ability to access their account.

Cybersecurity vs. Operational Security

- **Cybersecurity** – management of computer networks and systems to reduce the risk of materialization of threats that exploit vulnerabilities in such networks and systems. Cybersecurity aims to ensure that network and system integrity, availability, and confidentiality are maintained and not compromised.
- **Operational Security** – management of operational processes and personnel to reduce the risks of fraud and failure impacting the business and its customers.
- Cybersecurity and operational security are **closely related and often interlinked** (e.g., authentication of an employee when signing in to a system and establishing access controls for that employee).
- Both security types should be managed together as part of a comprehensive risk process.

Insider Risk

- **Insider risk** posed by staff (employees and contractors) is a large risk that is common to both cybersecurity and operational security.
- Insider risk can manifest as compromise of computer software, network security, granting of unauthorized access, unauthorized transfer of value (theft), leakage of confidential information, theft of encryption keys, and other breaches of trust.
- Many large losses by EMIs have been due to fraud and negligence by staff.
- Good practices includes segregation of duties, dual authorization of transactions, and role risk management.
- Role risk management comprises (i) identifying positions that require higher trust due to risk involved in the assigned duties; and (ii) assuring that the employee in the role meets the organization's standard of trust.

Business-related risks

As e-money transactions are processed in real time, it is essential that the e-money system is always accessible through its electronic channels

From a business perspective, cybersecurity should be aimed at maintaining system integrity and continued operation. Key business-related risks include:

- Core system failure
- Communications network and channel failures
- Denial of service attacks
- Large-scale information theft
- Theft of funds from e-money float

Customer-related risks

Key customer-related risks include:

- Compromised authentication
- Fraud on customer account
- Theft of customer funds
- Inability to access account due to electronic channel unavailability

While most customer-related risks involve relatively small sums from the EMI's perspective, such losses are very material for individual customers and may damage the EMI's reputation.

NOTE: Many of the biggest customer-related risks are human-related, such as PIN disclosure, loss of mobile handset, and SIM swap.

3 CYBERSECURITY
COUNTRY EXAMPLES

- The **Central Bank of the Philippines'** Enhanced Guidelines on Information Security Management require EMIs and other licensed financial institutions to establish a robust and resilient information security risk management framework that addresses cybersecurity and operational security..

- The **Central Bank of Nigeria** has issued a Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. This document provides guidance regarding cybersecurity governance, oversight, risk management, operational resilience, monitoring, and reporting.
- In addition, the Guidelines on Mobile Money Services include provisions on cybersecurity and operational security.

GSMA

- In April 2018, the GSMA (the global association for MNOs) launched the GSMA Mobile Money Certification, a program through which mobile money providers can be assessed against a number of good practice criteria, including cybersecurity.
- With respect to cybersecurity, the GSMA Mobile Money Certification Toolkit includes 68 security-related indicators on topics such as:
    - Security policies
    - Data protection
    - Identification and authentication
    - Information process
    - Audit trails
    - Testing of systems and processes

© GSMA

As of May 2019, 9 mobile money providers had been certified.

Business-related risks

- From a systems perspective, EMIs face similar risks to banks and other DFS providers. Regulators could identify good Information Security Management practices used by banks and others, assess their applicability to EMIs, and require EMIs to implement as appropriate.
- Regulators could require EMIs to adopt a proportionate risk management approach that involves (i) conducting vulnerability assessments of their core systems, operational processes, and all electronic channels; and (ii) where high risks are identified, implementing appropriate countermeasures.
- To reduce fraud and collusion risk, regulators could require EMIs to segregate roles in all processes requiring trust (e.g., preparation vs authorization, two-step authorization). Proper appointment processes can help ensure that staff meet organizational standards of trust commensurate with their role(s).
- Due to the online real-time nature of EMIs' business, redundant and resilient communication infrastructure is essential. Regulators could require EMIs to perform analyses of the redundancy and failure modes of the network on an ongoing basis and address identified vulnerabilities.

Customer-related risks

- To address mobile channel vulnerabilities that affect customers – whether using simple phones, feature phones, or smartphones – regulators could require EMIs to (i) identify such vulnerabilities; (ii) conduct a vulnerability analysis and risk assessment; and (iii) develop and implement countermeasures to proportionally address identified risks.
- Regulators could require EMIs to regularly conduct penetration testing and deploy penetration detection software to ensure that electronic channels are well-protected and not exposing vulnerabilities.
- Regulators could require EMIs to ensure that customers are well-informed regarding human-related risks and how to avoid common vulnerabilities such as SIM swap, PIN disclosure, and phishing.
- Regulators could require EMIs to (i) ensure proper segregation of duties for staff involved in customer-related processes to avoid fraudulent collusion between staff (and between staff and customers); and (ii) ensure that staff meet the organization's standards of trust.

AGENT REGULATION & SUPERVISION

1 | Agent Regulation

2 | Agent Supervision

1 | Agent Regulation

2 | Agent Supervision

Issue

While allowing EMIs and other DFS providers to offer services through agents can incentivize them to target low-income and remote customers, regulators are seeking to strike a balance that will enable providers to offer low-cost services through agents without negatively affecting service delivery or consumer protection.

Key regulatory considerations include:

- **Exclusivity:** Should agent exclusivity be permitted?
- **Identity:** Who can serve as an agent?
- **Permitted Services:** Which services may be outsourced to agents?
- **Authorization:** What notification/authorization requirements exist for appointing agents?
- **Geographical limits:** What geographical restrictions exist? For example, must agents be located within a certain distance of the nearest branch? Are agents prohibited from operating in urban areas?
- **Tiers:** Are different agent tiers (e.g., master agents and retail agents) permitted?

Source: CGAP (2011); EPAR (2018)

Arguments for Permitting Agent Exclusivity

- **Exclusivity may encourage investment:** First-movers spend significant resources identifying, training, and monitoring agents. To incentivize agent network development, they should be permitted to recoup these expenses without allowing competitors to free-ride on their investment in agent identification and training.
- **Exclusivity may not impact competition:** Exclusive agents often are not the only potential agents, so effective competition often is still possible.

Arguments for Prohibiting Agent Exclusivity

- **Exclusivity may favor first-movers:** In countries where first-movers have significant market power, exclusivity agreements may make it difficult for later entrants to compete on a level playing field.
- **Exclusivity may be particularly harmful in rural areas:** In some areas (particularly rural areas), there may be few entities that are able to meet the requirements to serve effectively as an agent.

1 AGENT REGULATION – EXCLUSIVITY
COUNTRY EXAMPLES

- Some countries explicitly prohibit agent exclusivity (see following examples), while other markets (e.g., Namibia) allow it in the absence of evidence of abuse of market power.
- In several countries (including **Kenya** and **Uganda**), telco-led e-money providers with significant market power initially established and enforced exclusivity agreements with agents. These agreements made it difficult for later entrants to compete on a level playing field.

Following are examples of approaches taken in different jurisdictions with respect to agent exclusivity:

Telecommunications Regulation: In Uganda, the Commercial Court declared that agent exclusivity agreements violated the *Communications Act* and were null and void.

Competition Law: Prior to a Competition Authority ruling in July 2014, 96% of Kenyan agents were exclusive. This dropped to 87% by Dec 2014.

E-Money Regulation: Many countries' e-money regulations prohibit agent exclusivity (e.g., **Nigeria**, **Ghana**, **Tanzania**). Following the above decisions, both Kenya and Uganda issued e-money regulations prohibiting agent exclusivity requirements.

Considerations

- As market structures and incentives vary, the merits and risks of agent exclusivity policies will need to be evaluated in the particular country context.
- While every country is different and should be evaluated independently, in most cases the risk to effective competition from **permitting** agent exclusivity is likely to outweigh the risk that **prohibiting** agent exclusivity would discourage investment in agent infrastructure.
- In countries where agent exclusivity is prohibited, regulators may need to monitor the market for signs of possible agent coercion, such as high rates of “voluntary” agent exclusivity, particularly with respect to agents of a market leader or other large EMI.

1 | AGENT REGULATION – IDENTITY

Arguments for Stricter Requirements

Consumer protection: Certain types of providers (e.g., for-profit shops, individuals rather than legal entities, unregistered businesses) should be prohibited from serving as agents due to the risk to consumers.

Permissible activities: Certain providers (e.g., faith-based organizations, not-for-profit entities, entities licensed by another regulatory agency) should not be engaging in agent business.

Arguments for Greater Flexibility

Principal responsibility: Regulators can protect consumers by (i) requiring that the principal (DFS provider) conduct due diligence on potential agents; and (ii) holding the principal responsible for the actions (or omissions) of its agents.

Cost: Heavy restrictions can affect the viability of agent networks, particularly in rural and remote areas

1 | AGENT REGULATION – IDENTITY
COUNTRY EXAMPLES

Stricter requirements → **Greater flexibility**

Indonesia

While banks and MFIs are permitted to use both individual agents and legal entities for branchless banking purposes, only banks are permitted to use individual agents when issuing e-money.

Source: KPMG (2016); Bank Indonesia (2018).

India

Initially, only nonprofits, post offices, and cooperatives were permitted to serve as bank agents. Over time, this restrictions was gradually loosened. Today, a wide variety of actors may serve as agents, including individual shop owners and companies with many retail outlets.

Source: CGAP (2010); Master Circular (2014)

Kenya

Individuals may be retained as agents provided that they possess proper business licenses, are permitted to provide agent services, and are financially sound.

Source: NPS Regulations (2014).

Considerations

- In countries with high levels of business informality, requiring DFS providers to use legal entities may limit uptake, particularly in rural, remote, and other underserved areas.
- To mitigate the risk of allowing DFS providers to appoint a broad range of individuals and legal entities as agents, regulators could (i) require providers to conduct due diligence on prospective agents; (ii) hold providers responsible for the actions (and omissions) of their agents; and (iii) ensure effective supervision of DFS providers.

Arguments for Stricter Limits

Consumer Protection: Only simple services such as cash-in and cash-out should be outsourced to agents. More complex services, such as loan disbursement/repayment or customer enrollment, should be provided directly by DFS provider staff.

Arguments for Greater Flexibility

Principal Responsibility: Even if DFS providers are permitted to outsource the delivery of various financial services to agents, they are still held responsible for the actions (or omissions) of their agents.

Financial Inclusion: Enabling DFS providers to open accounts remotely and provide a wide variety of services through agents can lower costs, improve the financial viability of agents, and foster financial inclusion.

1 | AGENT REGULATION – PERMITTED SERVICES
COUNTRY EXAMPLES

Stricter limits → Greater flexibility

Sri Lanka

The Guidelines clearly list cash-in and cash-out as permitted functions for agents (referred to as “merchants”) but do not clarify whether additional services may be offered by agents. In practice, agents are not conducting account registration for new customers.

Source: Central Bank of Sri Lanka, Mobile Payment Guidelines No. 2

Solomon Islands

Agents may perform a wide variety of activities, including customer enrollment, cash-in and cash-out, fund transfer, bill payment, loan repayment, and other activities approved by the Central Bank of the Solomon Islands.

Source: Central Bank of the Solomon Islands, Practice Guidance Note 1: Use of Cash Agents

Considerations

- Allowing DFS providers maximum flexibility regarding which services to outsource to agents typically increases the potential impact of agents on financial inclusion, particularly with respect to rural and underserved areas.
- To ensure that DFS providers have given careful consideration to risk mitigation, regulators may wish to require that providers submit detailed plans for how they intend to manage the risks inherent in the provision of each service that they propose to deliver through agents.
- Proportionate agent supervision could help to ensure that DFS providers are following proper due diligence procedures and effectively mitigating agent risk.

1 | AGENT REGULATION – AUTHORIZATION

Arguments for Greater Oversight

Consumer protection: Regulators need to ensure that agents will not defraud or otherwise harm customers.

Prudential oversight: Outsourcing service provision to agents is risky and could affect the financial viability of an institution.

Arguments for Greater Flexibility

Principal responsibility: Regulators can protect consumers by (i) requiring that the provider conduct due diligence on potential agents; (ii) holding the provider responsible for the actions (or omissions) of its agents; and (iii) requiring providers to periodically submit information regarding agency agreements.

Risk-based regulation: Regulatory review of individual agents is costly and time-consuming. In most cases, agent risk – both to individual providers and to the financial sector – does not require prudential oversight.

1 AGENT REGULATION – AUTHORIZATION
COUNTRY EXAMPLES

Greater oversight → Greater flexibility

Nepal

- EMIs must obtain approval from the Nepal Rastra Bank for all agents.
- Detailed information must be submitted, including personal and contact details, authority limits, liability provisions, and copies of agreements.

Source: NRB, Payment and Settlement Bylaw.

Georgia

- 30 calendar days prior to commencing agent services, DFS providers intending to provide payment services through agents must submit the following information to the National Bank of Georgia: (i) list of payment services to be provided through agents; and (ii) agent framework contract.

Source: Rule of Registration and Regulation of Payment Service Providers

Considerations

- To ensure that DFS providers have a well-thought-out agent due diligence plan, regulators may wish to require that providers submit detailed plans for how they intend to appoint and manage their agents.
- To maximize efficient use of limited supervisory resources, regulators may wish to require DFS providers to periodically share updated lists of agents rather than reviewing and approving appointment of individual agents.
- Proportionate agent supervision could help to ensure that DFS providers are following proper due diligence procedures and effectively mitigating agent risk.

1 | AGENT REGULATION – GEOGRAPHICAL LIMITS

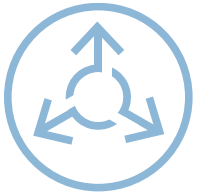
Arguments for Stricter Limits

Financial Inclusion: To ensure that DFS providers target unbanked and underserved customers, specific geographic targets (e.g., rural quotas, restrictions on service provision in areas with higher financial inclusion) are required.

Effective oversight: Agents must be located within a certain distance of a DFS provider's branch to ensure effective agent oversight and cash management.

Arguments for Greater Flexibility

Commercial Viability: DFS providers are best able to determine where to invest and how to oversee their agents. Imposing too many restrictions can hamper the DFS business model and inadvertently harm financial inclusion efforts.



Flexibility: Providers require sufficient flexibility to adapt to business conditions and circumstances (e.g., geographic conditions, competition, service uptake).

1 | AGENT REGULATION – GEOGRAPHICAL LIMITS
COUNTRY EXAMPLES

Stricter limits → **Greater flexibility**

Indonesia

- To ensure that branchless banking will focus on remote areas, banks are prohibited from using agents in provincial, regency, or municipality capitals.

Source: KPMG (2016).

India

- At least 25% of physical access points for Payments Banks must be in rural areas.
- Payments Banks must establish a controlling office for a cluster of agent access points.

Source: RBI, Guidelines for Licensing of "Payments Banks".

Kyrgyz Republic

- No specific geographical restrictions

Source: NBKR, Position on Electronic Money in the Kyrgyz Republic

Considerations

- While access to formal financial services typically is lower in rural areas, many countries have large unbanked (or underserved) urban populations as well.
- To maximize the likelihood that DFS providers are able to grow and scale their services, regulators may wish to provide significant flexibility, particularly in the early stages of sector development.
- Proportionate agent supervision could help regulators to monitor DFS development and ensure that DFS providers are (i) reaching the unbanked and underserved; and (ii) effectively managing and overseeing agents.

Arguments for Stricter Limits

Effective oversight: Requiring DFS providers to maintain a contractual relationship with each individual agent may incentivize better agent oversight.

Arguments for Greater Flexibility

Impact on financial inclusion: Allowing DFS providers to sign one contract that provides access to hundreds or thousands of agents can expedite agent network development and foster uptake and financial inclusion.

Efficiency: Allowing DFS providers to outsource agent network management to a specialist organization may be more efficient, enabling faster rollout and/or lower costs.

1 AGENT REGULATION – TIERS
COUNTRY EXAMPLES

Stricter limits → Greater flexibility

Armenia and Mongolia

- In many countries, the permissibility of agent tiers is not specified in DFS regulation.
- In countries with a civil-law legal tradition, this lack of clarity may lead to an interpretation that agent tiers are prohibited.

Mali and Chad

- 84% and 44% of successful mobile money agents operate without access to a bank in Chad and Mali, respectively. In both countries, master agents provide the necessary link between banks and retail agents to address retail agents' liquidity management needs.
- In addition to liquidity management, master agents provide training support and address retail agents' questions.

Source: GSMA (2015).

Considerations

- Agent tiers play an important role in countries with limited traditional banking infrastructure, particularly in rural and remote areas.
- Regulators may wish to permit agent tiers, subject to the requirement that any DFS provider engaging in a tiered agent relationship remains ultimately responsible for the actions of its agents and any sub-agents.
- In countries where the permissibility of agent tiers is unclear, regulators could provide necessary clarity through relevant regulatory documents.


1 Agent Regulation
2 Agent Supervision
© BFA


1 Agent Regulation
2 Agent Supervision
© BFA

Issue

As e-money grows, so does the need to assess the risk presented by use of agents to deliver e-money services.

Examples of agent-related risks include the following:

Consumer	Operational	ML/TF
Fraud	IT system failure	ML/TF by agent
Unauthorized fees	Service outage	ML/TF by customer
Lack of receipts	Contingency planning	
Lack of disclosure/transparency	Internal controls	
Inadequate dispute resolution mechanisms		
Insufficient liquidity		

Agent risk is affected by several factors (see next slide)

Source: CGAP (2015)

FACTORS IMPACTING AGENT RISK

Provider experience with agent oversight

Provider resources (consider capitalization and ability to scale)

Types of services provided by agents (e.g., account opening, payments, transfers, loans)

Agent collateral (e.g., whether agent operates on pre-funded basis)

Location of agents (e.g., risks re: robbery, network connectivity, ML/TF)

Technology used by agent (e.g., paper vs. electronic records, ability to electronically or biometrically verify customer identity)

Source: CGAP (2015)

MATERIALITY TEST FOR AGENT SUPERVISION

COUNTRY EXAMPLES

Test #1 (Brazil & Mexico):

In general, should agent supervision be a priority?

If so, which topics should be emphasized?

Considerations include the following:

- What percentage of providers' transactions are conducted by agents?
- What percentage (and what type) of customer complaints are related to agents, as compared to other delivery channels and as a % of total complaints?
- What risks are raised by the products delivered by agents?
- How frequent and serious are media reports of problems with agents?

Source: CGAP (2015)

MATERIALITY TEST FOR AGENT SUPERVISION
COUNTRY EXAMPLES

Test #2 (Brazil, Colombia, Peru):

Which individual providers should be closely scrutinized regarding their agent business?

Considerations include:

- Number and geographic coverage of agents
- Number of customer accounts used at agents
- Volume/value/types of transactions conducted at agents
- Types of services available at agents
- Relative importance of agents to the provider (e.g., % of total revenue, transaction volume/value, total accounts)
- Complexity of agent network management arrangements

Source: CGAP (2015)

RISK-BASED AGENT SUPERVISION
COUNTRY EXAMPLES

- Most supervisors do not assess risk of individual agents. Instead, they consider:
  - Provider's internal controls and risk mitigation tools; and
  - Market-level consumer, operational, and ML/TF risks related to use of agents (less common).
- Most supervisors see agent risk as lower priority, so onsite agent supervision is uncommon.

- Several countries collect aggregate monthly and/or quarterly information on # of agents, volume/value/type of transactions, customer complaints, and/or fraud/theft/data breaches.
- **Pakistan** is an exception; it collects similar data on a monthly basis at the level of individual bank agents.

Source: CGAP (2015)

Considerations

- Regulators may first wish to consider **whether to prioritize agent supervision** by evaluating criteria such as the volume of agent transactions, volume of complaints through agent channels, and risks raised by services provided through agents.
- Regulators may also wish to consider the **relative importance of agents to individual DFS providers** to identify which providers should be most carefully scrutinized.
- To facilitate these assessments, regulators could require providers to **submit monthly or quarterly information** on agents, transactions, customer complaints, and fraud/theft/data breaches.
- In most countries, agent-related supervision focuses on the provider's **internal controls and risk mitigation tools** rather than on-site inspection of individual agents.
- Adoption of RegTech tools by regulators offers the potential to improve the efficiency and efficacy of data collection, processing, and analysis/visualization for agent supervision.

CONSUMER PROTECTION

1. Disclosure and Transparency
2. Fraud
3. Complaint and Dispute Resolution
4. Data Protection
5. Pricing Regulation
6. Discrimination & Disparate Access

1 Disclosure and Transparency

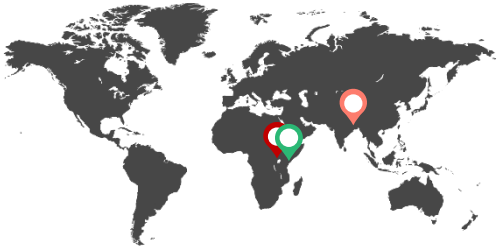
2 Fraud

3 Complaint and Dispute Resolution

4 Data Protection

5 Pricing Regulation

6 Discrimination & Disparate Access



Issue

In some countries, customers are not aware of the fees, charges, and other terms and conditions related to use of e-money services.

Many e-money providers do not provide adequate disclosure.

Country examples of poor disclosure/transparency practices

In **Uganda** and **Bangladesh**, mystery shopping revealed that fee charts often were not displayed at agent shops.

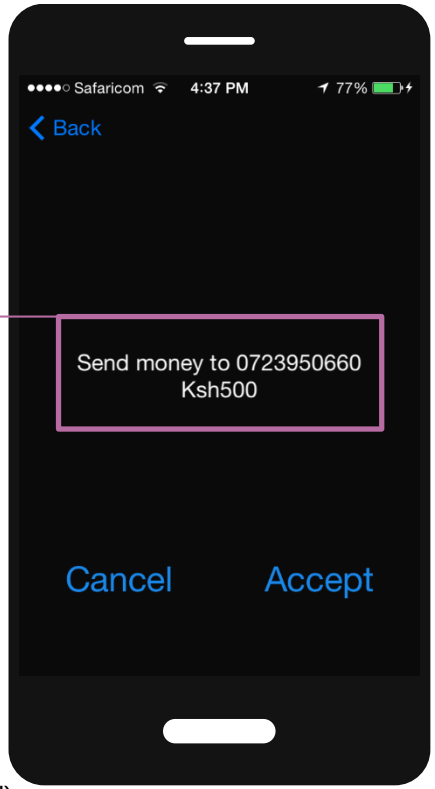
In **Uganda**, lack of transparency of fees for e-money services has led some customers to believe that all fees charged for transactions at agents were fraudulent.

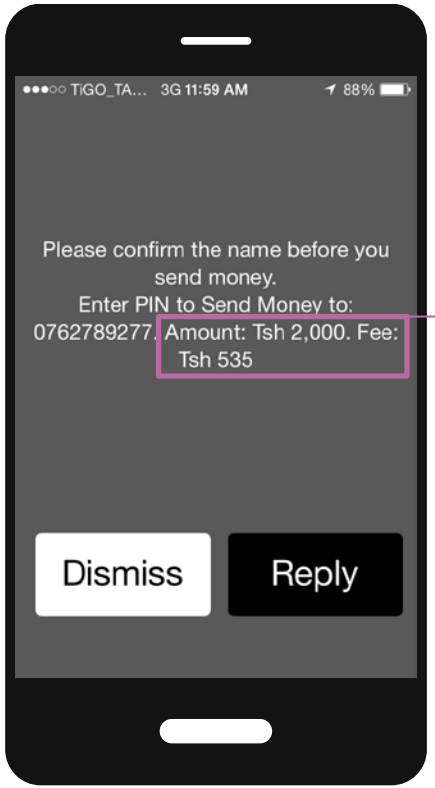
In **Kenya** as recently as 2016, fees for transactions such as P2P transfers and bill payments were not disclosed in advance (see next slides).

Source: CGAP (2015)

DISCLOSURE OF E-MONEY FEES IN KENYA VS. TANZANIA

Kenya:
No disclosure of transaction fee





Tanzania:
Transaction fee clearly disclosed

Source: Mazer (2016) (unpublished)

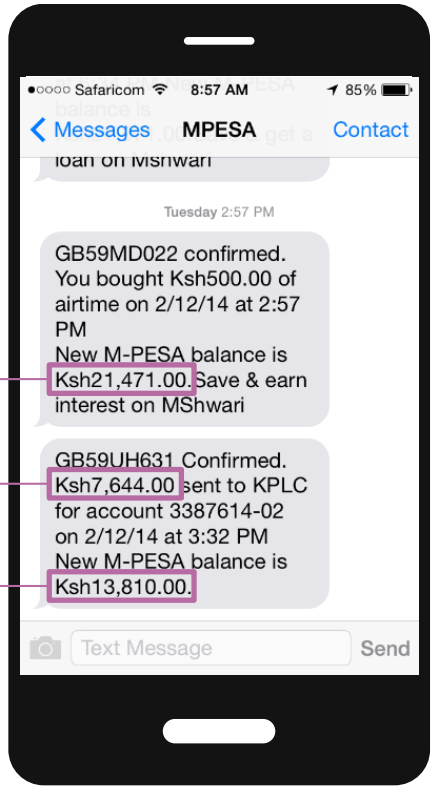
BILL PAY: THE COST OF NOT KNOWING FEES

Starting Balance**: 21,471**

Bill Pay Amt.: **7,644**
Expected New Balance: **13,827**

Actual New Balance: **13,810**

Implicit Transaction Cost: **17**



What do consumers know about bill pay fees? (n=500)

- 40% used Pay Bill feature before
- 35% thought fee of last transaction was zero
- Average USD 8.60 per year in fees for users in this sample

Source: Mazer (2016) (unpublished)

1 DISCLOSURE AND TRANSPARENCY
COUNTRY EXAMPLES

European Union

The Revised Payment Services Directive (PSD2) requires PSPs to make information on fees and charges available "*in an easily accessible manner*" prior to conducting any transaction. In addition, the Payment Accounts Directive requires payment service providers to provide customers with a standardized fee information document prior to opening a payment account.

United States

As of October 2017, providers of prepaid accounts must disclose fees and charges using standard disclosure forms. For accounts opened electronically, disclosures should also be provided electronically in a manner reasonably expected to be accessible and "*viewable across all screen sizes*."

Kenya

In October 2016, CAK ordered banks and e-money providers to ensure that all fees related to mobile transactions were disclosed via the mobile channel in advance of each transaction by end of 2016. Several larger providers received an extension until June 2017. In practice, however, some providers were still noncompliant on some of their channels as of February 2018.

Considerations

- Regulators could issue **detailed guidance on disclosure requirements** – including provisions for electronic disclosure – aimed at ensuring effective disclosure of fees, charges, and other terms and conditions for mobile phone-based and other digital products, regardless of type and size of phone or other digital device.
- Where appropriate, regulators could design **standardized forms and formats** for electronic disclosure of fees, charges, and other terms and conditions for products delivered digitally.
- Regulators could require **electronic disclosure of fees** for payment transactions prior to transaction fulfillment.
- If an EMI elects not to pay the USSD charge for its customers' transactions, regulators could require the EMI to **notify customers upon registration for e-money services** that the customers' MNO may deduct a USSD access fee from their airtime.

1 | Disclosure and Transparency

2 | Fraud

3 | Complaint and Dispute Resolution

4 | Data Protection

5 | Pricing Regulation

6 | Discrimination & Disparate Access

1 Disclosure and Transparency

2 Fraud

3 Complaint and Dispute Resolution

4 Data Protection

5 Pricing Regulation

6 Discrimination & Disparate Access

Issue

As e-money adoption increases, so does fraud risk due to:

Rapidity: The ability to quickly transfer funds without appearing in-person is attractive both to legitimate users and fraudsters.

Inexperience: Many customers and agents have little experience with formal financial services, making them more vulnerable to fraud.

Outsourcing: Effective agent oversight is challenging, particularly in remote areas.

Identification: Countries lacking ubiquitous national ID schemes may struggle to identify fraudsters.

Rapid Growth: In countries with rapid adoption, providers' internal controls may fail to keep pace.

Agents are particularly susceptible to e-money fraud, with 22%-53% of agents in high-adoption markets reporting that they had been defrauded.

Source: Helix Institute (2016)

2 FRAUD MITIGATION MEASURES ADOPTED BY PROVIDERS

Type of fraud	Response
Fake currency	UV light and other detection tools
Fake P2P transfer message followed by request to reverse “erroneous” transaction	Customer and agent education by e-money providers
Facilitation fees for prize “winners”	Customer education by e-money providers
Agent overcharging customers	Customer education, mystery shopping, effective recourse mechanisms
PIN appropriation (targeting agents)	Agent education by e-money providers
SIM replacement	Additional verification requirements (e.g., secret words, date of birth, parents’ names) Quarantine period for using e-money account after SIM swap

Source: MicroSave (2014); CGAP (2017).

Country examples of good fraud mitigation regulation

European Union

Revised Payment Services Directive limits liability for all unauthorized payment transactions to maximum of EUR 50 (except where payer acts fraudulently or fails to notify PSP of loss, theft, or misuse of payment instrument).

United States

Truth in Lending Act and *Electronic Funds Transfer Act* limit customer liability for fraudulent charges for credit card and debit card accounts, respectively. Prepaid accounts lack the same level of legal protection, so liability depends upon the rules of the issuer.

Considerations

- Regulators could develop **guidance tailored** to the types of fraud common in the e-money sector and the financial sophistication of the typical e-money customer (including agents). In addition, regulators could require EMIs to **train agents and sensitize customers** to common fraud typologies and how to avoid them.
- Regulators could require EMIs to institute proper **policies and processes for fraud mitigation**, such as segregation of duties, physical and logical access controls, proper data storage infrastructure, and conduct of periodic audits and internal risk assessments.
- Regulators could require EMIs to **refund customers for losses** due to fraud unless they can prove that the loss was due to the customer's fraudulent or otherwise culpable behavior.

1 Disclosure and Transparency

2 Fraud

3 Complaint and Dispute Resolution

4 Data Protection

5 Pricing Regulation

6 Discrimination & Disparate Access

1 Disclosure and Transparency

2 Fraud

3 Complaint and Dispute Resolution

4 Data Protection

5 Pricing Regulation

6 Discrimination & Disparate Access

Issue

E-money customers face challenges with complaint and dispute resolution, including the following:

Inexperience: Many e-money customers are new to formal financial services and may lack the knowledge and resources to know how to effectively obtain recourse.

Distance: E-money customers may reside far from providers' customer service centers. As a result:

- In-person complaint resolution may be costly;
- Customers often seek assistance from agents, many of whom are not trained to perform this role (and who are sometimes the reason for the complaint); and
- Customers who elect to report complaints by phone may face long hold times and dropped calls due to network issues.

Product Complexity: For some products – such as bank accounts opened using an e-money account – customers may not know which provider is responsible for complaint and dispute resolution.

Key requirements for effective internal recourse mechanisms at financial institutions

- Providers have internal complaints mechanism with specialized staff and appropriate oversight;
- Complaints mechanism uses properly documented policies and processes;
- Customers informed of right to complain and how to do so;
- Customers able to submit complaints using readily available mechanisms (e.g., in-person, phone, using informal language);
- Customers receive tracking number and are kept informed of complaint status;
- Providers ensure timely investigation and resolution;
- Customers informed of right to external recourse and how to exercise this right;
- Providers track complaints to identify key problem areas;
- Providers subject internal complaints mechanism to periodic audit; and
- Providers regularly report complaints data to financial authority.

Source: CGAP (2013)

Considerations

- Regulators could require EMIs to establish and implement effective **internal recourse mechanisms** that meet the requirements listed on the previous slide.
- Regulators could ensure that:
  - **Multiple complaint channels** are available;
  - Complaint channels address the **needs of various clients** (e.g., language, literacy, proximity to service centers); and
  - Complaint channels are **tailored** to the types of financial services offered and how they are delivered (e.g., web-based vs. USSD/SMS-based).
- Regulators could establish **timeframes** for addressing complaints, along with guidance on mechanisms for **external resolution** (e.g., Financial Ombud, central bank mediation, arbitration) if internal efforts fail.

1 | Disclosure and Transparency

2 | Fraud

3 | Complaint and Dispute Resolution

4 | Data Protection

5 | Pricing Regulation

6 | Discrimination & Disparate Access

1 Disclosure and Transparency

2 Fraud

3 Complaint and Dispute Resolution

4 Data Protection

5 Pricing Regulation

6 Discrimination & Disparate Access

Issue

In the absence of proper security and access controls, personal customer data could be used for fraudulent purposes.

In the absence of regulatory requirements or good institutional practices, providers may neglect to consult customers before their data are collected, processed, or shared with other parties.

Even if they are consulted, customers may lack a clear understanding of how data are used and shared with other parties.

There are numerous examples of national and regional comprehensive data protection regulation, including:

European Union
General Data Protection Regulation

ECOWAS
Supplementary Act A/SA.1/01/10 on Personal Data Protection

African Union
Convention on Cyber Security and Personal Data Protection

SADC
Model Law on Data Protection

Ghana
Data Protection Act

Typical provisions of such laws include:

Legitimate processing criteria: To process customer data, providers must obtain their consent or rely upon another legitimate processing criterion.

Purpose and relevance: Personal data must be collected for specified, explicit, and legitimate purposes, and the data collected must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.

Security: Personal data must be protected against unauthorized alteration, destruction, or access.

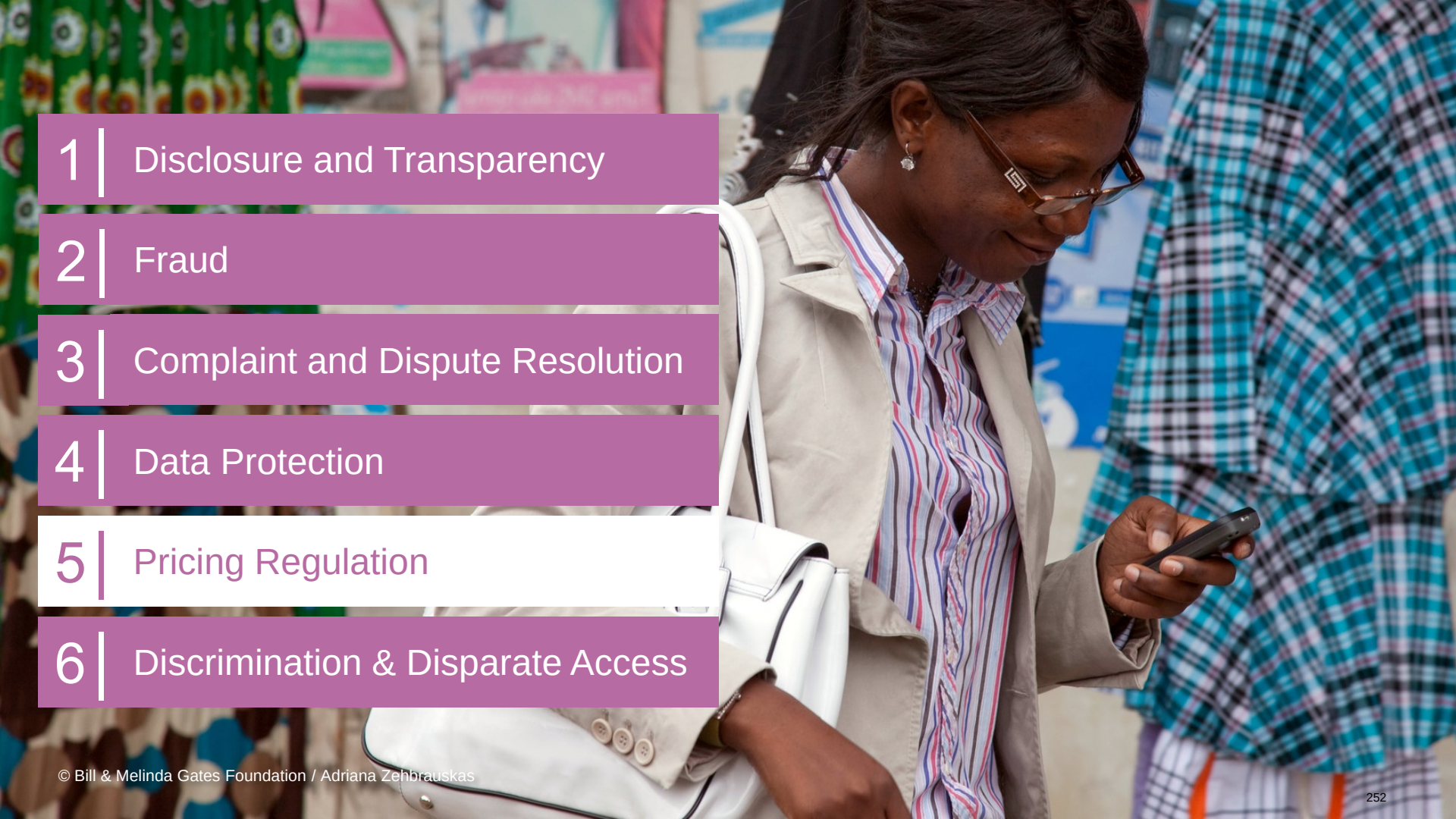
Direct Marketing: At minimum, consumers have the right to object to and opt out of data processing (some jurisdictions require consumers to explicitly consent ("opt-in").

Considerations

In countries that lack a comprehensive data protection regime, regulators could **develop guidance** for EMIs and other DFS providers on how to implement effective data protection policies and processes, addressing issues such as:

1. Data collection and processing;
2. Customer consent;
3. Sale/sharing of customer data;
4. Direct marketing;
5. Customer rights to review data and correct errors;
6. Data security;
7. Disclosure of privacy policies; and
8. Non-discrimination.

1. Disclosure and Transparency
2. Fraud
3. Complaint and Dispute Resolution
4. Data Protection
5. Pricing Regulation
6. Discrimination & Disparate Access



1. Disclosure and Transparency
2. Fraud
3. Complaint and Dispute Resolution
4. Data Protection
5. Pricing Regulation
6. Discrimination & Disparate Access

Issue

In an effort to protect customers, some financial authorities are considering or are already regulating fees and charges for e-money transactions (e.g., cash-in, cash-out, P2P transfer, bill pay).

Arguments for regulating fees and charges

- **Monopolistic behavior:** Given the power of network effects in the e-money and telecommunications sectors, monopolistic or cartelistic behavior may harm customers through high prices.

Arguments against regulating fees and charges

- **Investment incentives:** EMIs need to know that they can recoup CapEx and OpEx costs to justify significant investments in e-money services.
- **Incentives and transparency:** Setting fees and charges below market rates can discourage investment, disincentivize service provision to lower-income customers, and reduce transparency (if additional charges are hidden elsewhere).

Nigeria

Central Bank of Nigeria sets fee ceilings (and sometimes floors) for the following:

- **Cash-in** at agent or via bank account (direct debit)
- **P2P** (intrascheme or interscheme, agent-assisted or self-initiated)
- **Bill Payment**
- **Cash-Out** (no charge permitted)
- **Bulk Payments**

Source: CBN, Guide to Charges (2017).

Indonesia

The Financial Services Authority has limited the permissible fees that banks may charge for branchless banking:

- **Fees may not be charged for:** Monthly account maintenance, bookkeeping transactions, cash-in, incoming transfers, or account closure.
- **Fee limits:** Any fees charged must be lower than the charges for similar transactions using a regular savings account

Source: OJK, Branchless Banking Rules (2014)

Considerations

- The vast majority of e-money markets do not set ceilings or floors for e-money transactions.
- Even in highly-developed payment card markets (e.g., US, EU), deciding whether to cap interchange fees and other charges remains controversial.
- Most e-money markets are at a much earlier stage of development. Establishing ceilings and floors on e-money transactions risks disincentivizing investment by EMIs and adoption by agents and merchants.
- Promoting DFS innovation and competition could help lower costs without disincentivizing investment and uptake by key stakeholders.

1 | Disclosure and Transparency

2 | Fraud

3 | Complaint and Dispute Resolution

4 | Data Protection

5 | Pricing Regulation

6 | Discrimination & Disparate Access

1 | Disclosure and Transparency

2 | Fraud

3 | Complaint and Dispute Resolution

4 | Data Protection

5 | Pricing Regulation

6 | Discrimination & Disparate Access

Issue

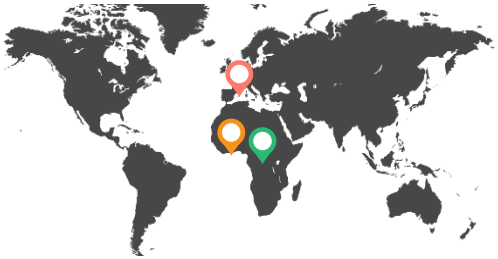
While new technologies offer the potential to dramatically expand access to financial services, adoption of digital financial services also raises risks related to discrimination and disparate access.

Discrimination

- Reliance upon algorithms to assess creditworthiness raises the possibility that discriminatory criteria may be considered (see next slide).

Disparate Access

- There is a gender gap in DFS usage, but this gap is narrower than the gender gap in usage of traditional formal financial accounts (see following slides).



Algorithmic Discrimination

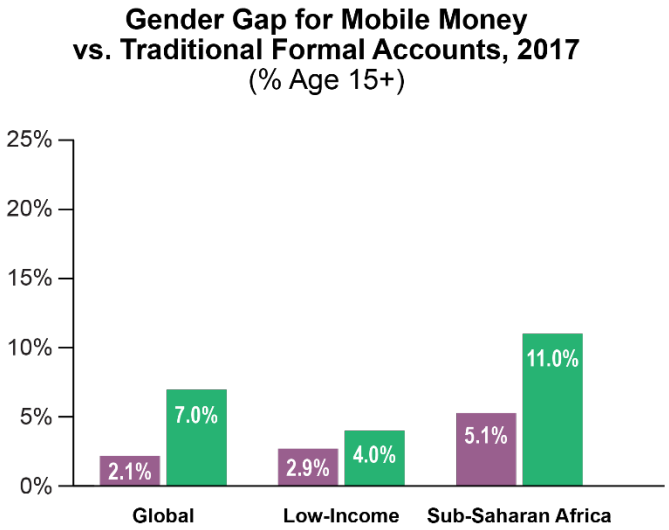
- To develop creditworthiness assessments in the absence of formal credit histories, algorithms are analyzing a wide variety of other criteria, such as social reputation, use of airtime and mobile money services, and other considerations.
- In the absence of clear regulatory limitations and proper internal oversight, algorithms could consider factors that are either *de jure* discriminatory (e.g., age, race, gender) or *de facto* discriminatory (e.g., shopping preferences, social circle, education/literacy).
- Most jurisdictions with comprehensive data protection regimes offer individuals certain protections with respect to decisions based solely upon automated processing of personal data. Some jurisdictions prohibit purely automated decision-making for decisions with "legal effects" or "other significant effects" (e.g., **African Union**, ECOWAS), while others permit automated decision-making but give individuals the right to ensure that decisions that significantly affect them are not based solely upon automated processing of personal data (e.g., **EU**, **Ghana**).

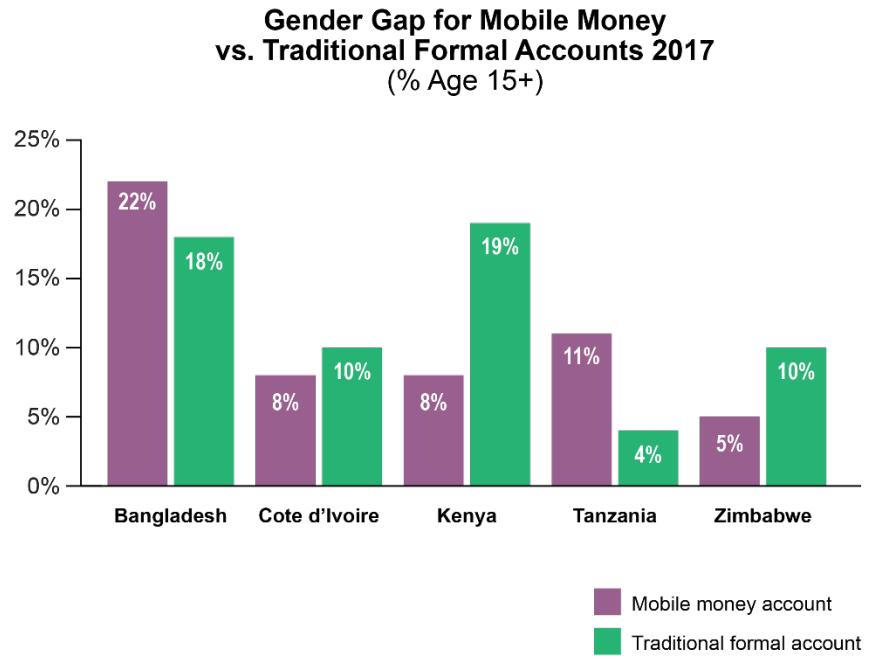
DISPARATE ACCESS

Gender and DFS

- Globally, e-money and other DFS are contributing to financial inclusion. The percentage of the population with a mobile money account doubled from 2014 to 2017, both for women and men.
- In low-income countries globally and in **sub-Saharan Africa** – where 18% and 21% of adults used a mobile money account in the past year, respectively – mobile money is a key financial inclusion tool for both women and men.
- While there is a gender gap in mobile money usage, it is narrower than the gender gap in usage of traditional formal financial services (see next slide).

Source: World Bank (2018)





Source: World Bank (2018)

Considerations
Discrimination

- Striking a balance that encourages innovation in credit assessment while avoiding *de jure* and *de facto* discrimination is a key regulatory challenge.
- Regulators could clarify the types of factors that legally may and may not be considered by providers who use algorithms and alternative data sources to assess creditworthiness.
- Where disparate impact is identified (see next point), regulators could review algorithms to understand key factors affecting credit assessments and assess whether algorithmic inputs are inadvertently generating discriminatory outcomes.
- Any credit provider with significant loan volume – whether otherwise licensed and regulated by the financial authority or not – could be subject to market conduct supervision.

Considerations
Disparate Impact

- Regulators could require DFS providers to collect gender-disaggregated data.
- Regulators could encourage DFS providers to understand the reasons for the DFS gender gap (and, where relevant, gaps for other identifiable groups such as religious, racial, or ethnic groups) and work to eliminate it.

