Mobile Money: Knowing the Risks

Seminar for Senior Bank Supervisors from Emerging Economies
October 21-25, 2019, Washington DC

WORLD BANK GROUP
Finance, Competitiveness & Innovation

Gynedi Srinivas
Senior Financial Sector Specialist
Payment Systems Development Group

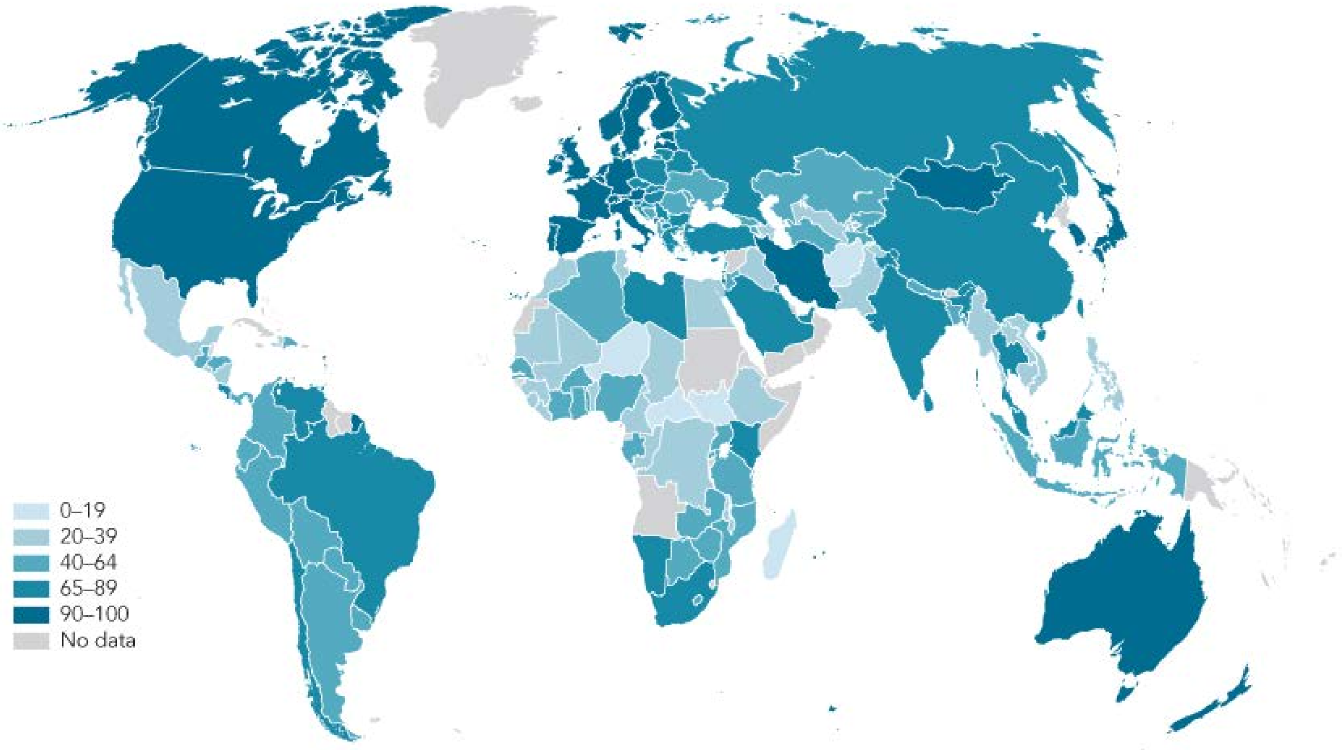
Agenda

- Financial inclusion and Digital financial services
- Defining e-money
- E-money models – Banks and non-banks; use cases
- Key risks - legal and regulatory; financial integrity; safeguarding of funds; operational resiliency;
- Access to national payments infrastructure – facilitating interoperability of e-money schemes;
- Usage of agents: non-exclusivity arrangements;
- Enabler for financial inclusion; transaction accounts;

Financial inclusion is on the rise globally

- The third edition of the Global Findex database shows that 1.2 billion adults have got an account since 2011, including 515 million since 2014.
- Between 2014 and 2017, account ownership rose globally from 62% to 69%. In developing economies, it went from 55% to 63%.

Today, 69 percent of adults around the world have an account
Adults with an account (%), 2017

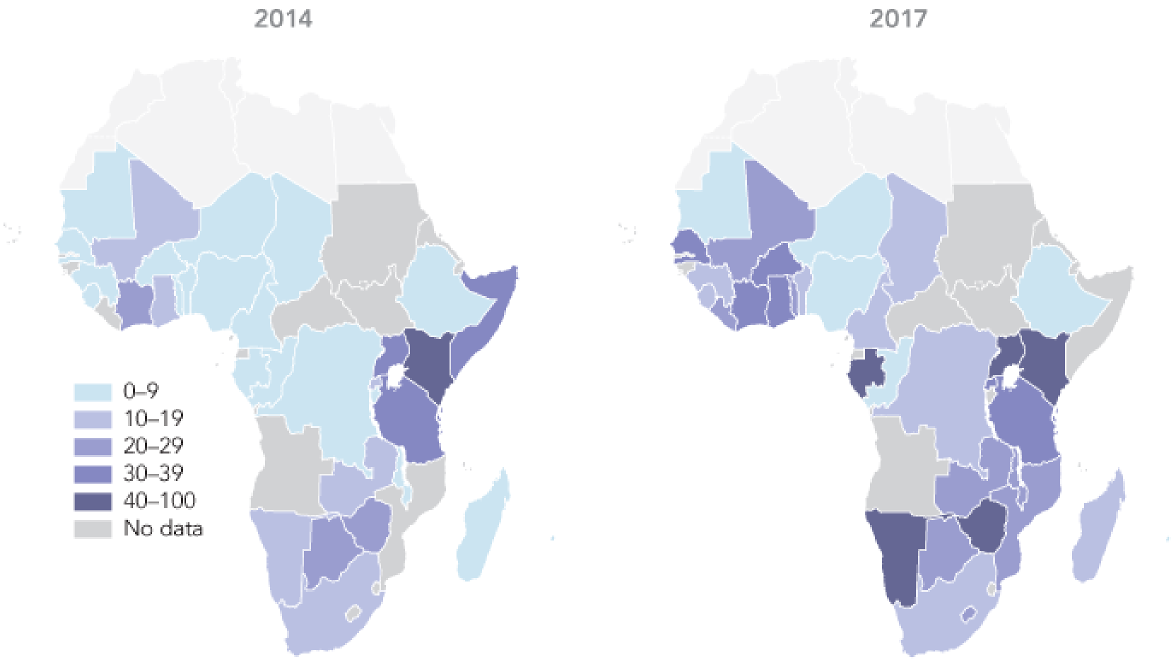


Source: Global Findex database.

Digital technology is driving access to and use of financial services

- In Sub-Saharan Africa, mobile money account ownership rose from 12% to 21%.
- Mobile money spread from East Africa to West Africa and beyond, and plays an important part in some fragile and conflict affected economies.

Mobile money accounts have spread more widely in Sub-Saharan Africa since 2014
Adults with a mobile money account (%)

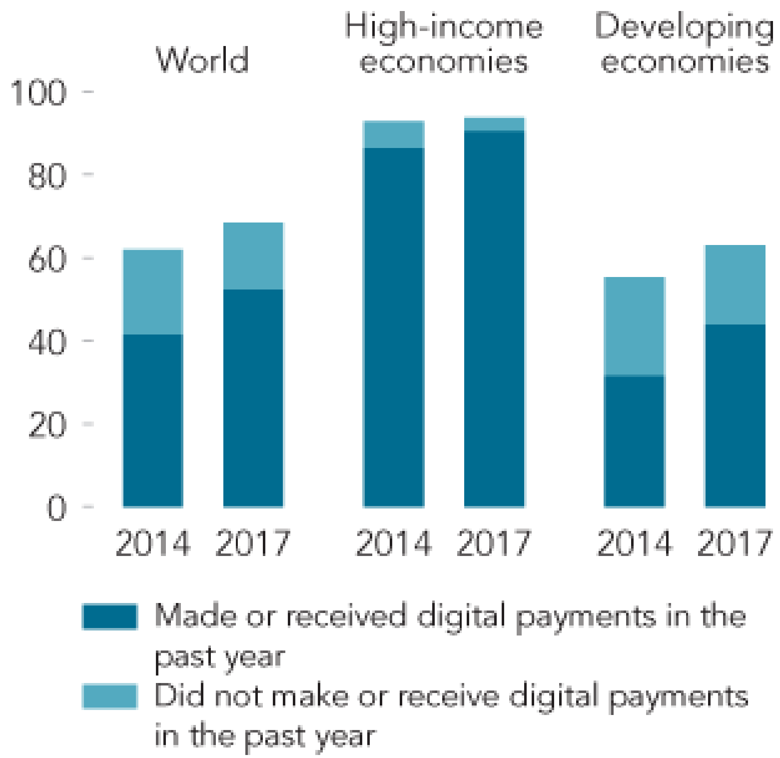


Source: Global Findex database.
Note: Data are displayed only for economies in Sub-Saharan Africa.

Use of Digital Payments is Increasing in Developing Economies

- Globally, 52 percent of adults or 76 percent of account owners, reported having made or received at least one digital payment using their account in the past year.
    - This share increased by 11 percentage points between 2014 and 2017.
- In developing economies, the share of adults using digital payments rose by 12 percentage points, to 44 percent.
- In some economies, this share increased by more than 20 percentage points, such as in Bangladesh (27 pp) China (23 pp), and Thailand (29 pp).

More people who have an account are using it for digital payments
Adults with an account (%)

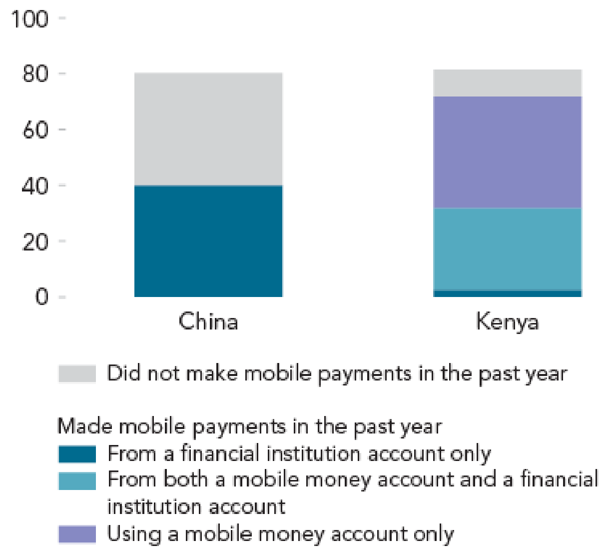


Source: Global Findex database.

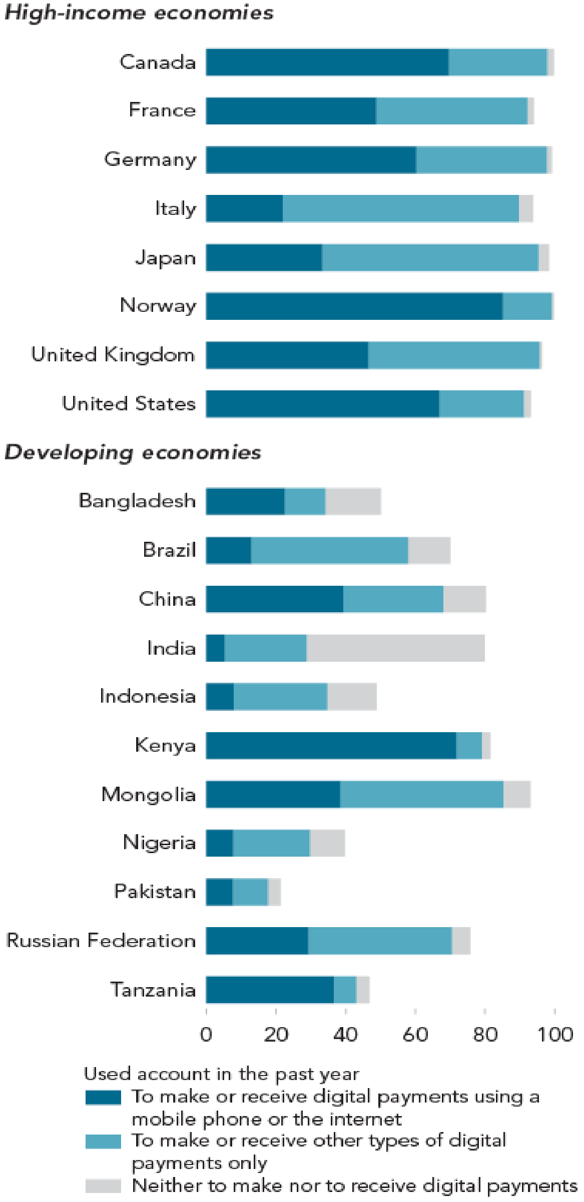
Using a Mobile Phone or the Internet to Make Payments

- Mobile phones and the internet increasingly offer an alternative to make a direct payments from an account – either a mobile money account or, through an app or a website, from a financial institution account.
  - In high-income economies 55 percent of account owners have done so and 19 percent in developing economies

Account owners in China tend to make mobile payments through apps, those in Kenya through mobile money accounts
Adults with an account (%), 2017

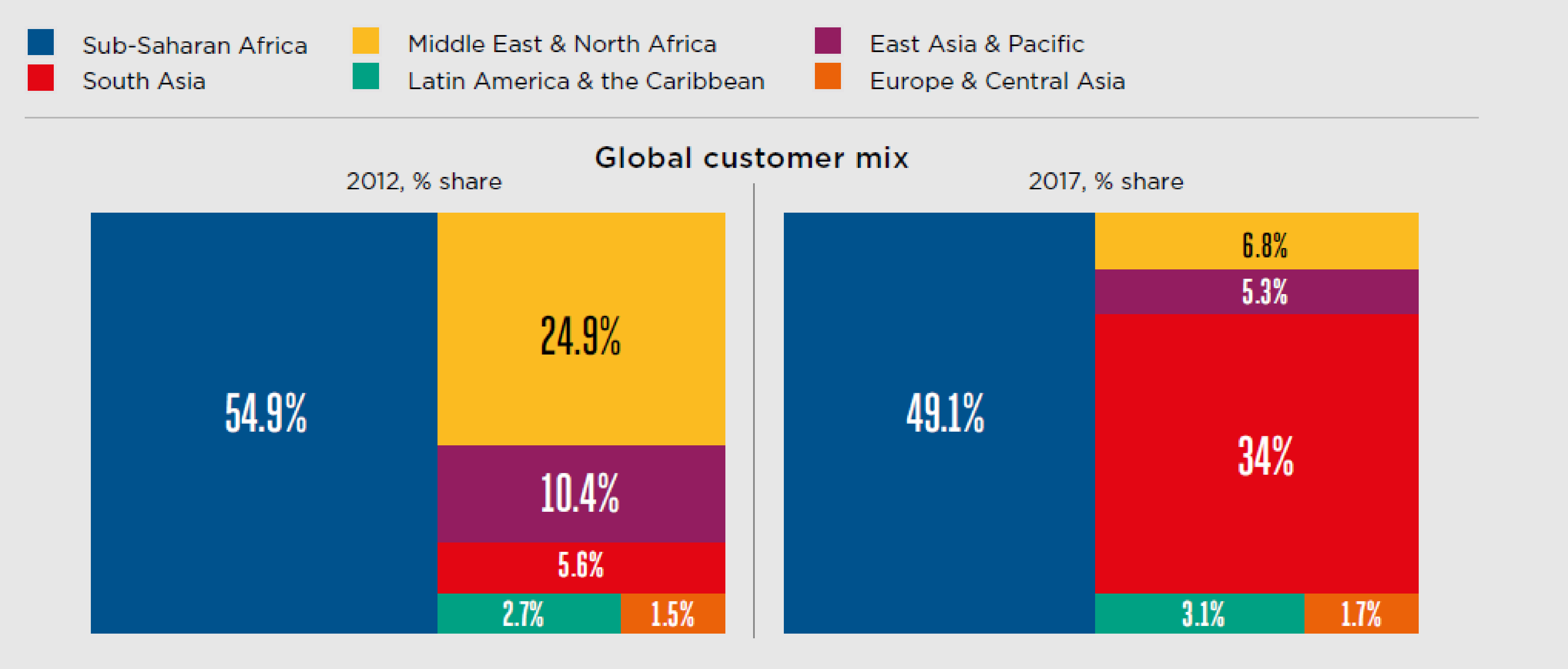


Half of adults in high-income economies use a mobile phone or the internet to make transactions from their account
Adults with an account (%), 2017



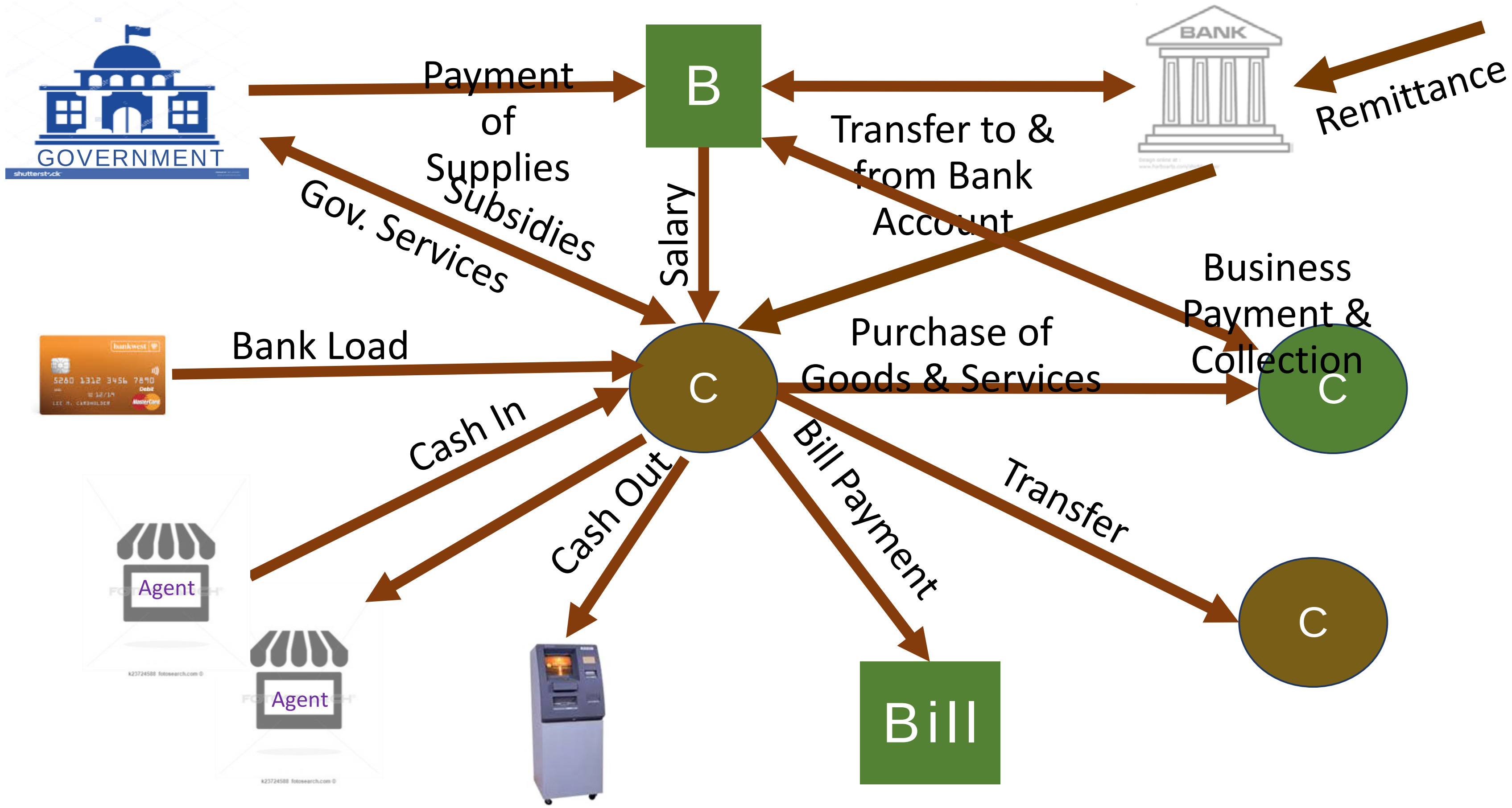
Source: Global Findex database.

Global spread of registered mobile money customers from December 2012-December 2017



Source: GSMA 2017 State of the Industry Report on Mobile Money

Growth could be attributed to a large number of use cases



Definition of e-money

- **Electronic money:** means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN (EU E-money Directive 2009);

- **Electronic money:** is prepaid value stored electronically, which represents a liability of the e-money issuer (a bank, an e-money institution or any other entity authorised or allowed to issue e-money in the local jurisdiction) and which is denominated in a currency backed by an authority. https://www.bis.org/cpmi/publ/d137.pdf (CPMI, Digital Currencies, 2015)

- Electronic money (e-money) is a digital alternative to cash. It allows users to make cashless payments with money stored on a card or a phone, or over the internet.

- **Mobile money** is a form of e-money and is made available through mobile devices

Definition of e-money

- **Closed loop:** Issued by an entity for facilitating the purchase of goods and services from that entity only and usually do not permit cash withdrawal. As these instruments cannot be used for payments or settlement for third party services, the issuance and operation of such instruments is not subjected to regulation and oversight.

- **Semi-closed loop:** Issued by an entity and used for purchase of goods and services, including financial services, remittance facilities, etc., at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment gateway) to accept them as payment instruments. Cash withdrawal, may or may not be permitted.

- **Open loop:** Widely accepted; for all purposes listed above, cash withdrawal also permitted.

Issuance of e-money

- Issuers of e-money can be both banks and non-bank payment service providers.
- Banks as issuers of e-money: Approval given by Banking Regulator or Central Bank; No additional license is usually required;
- Non-bank issuers of e-money: Licensing/authorisation requirements prescribed; not construed as a deposit taking activity.

Issuance of e-money - different models

Bank led

Pros
- Providers of financial services
- Aware of AML/CFT, risks, …
- Can extend financial services like deposit and credit to e-money accounts of customers.
- Well established procedures for customer grievance redressal
- Protection of customer deposits

Challenges
- Inadequate reach and presence in unbanked and underserved areas

Philippines

South Africa

Collaboration between Banks and MNOs.
Bank authorised by regulator with service provision and branding by the MNO
Uganda: Airtel Money

Non-bank led

Pros
- Leveraging on innovative technology
- Wider reach with stronger distribution channels
- Normally have stronger marketing campaigns

Challenges
- Need protection of consumer deposits (e-money).
- Need to separate between company's funds and consumers' deposits.
- AML/CFT issues

Kenya

Philippines

Key risks

- **Key risks**
  - Legal and regulatory regime;
  - Financial integrity;
  - Safeguarding of funds;
  - Operational resiliency;

Key risks – legal and regulatory regime

- A sound legal basis needed to:
  - help establish an effective oversight framework to monitor and mitigate potential risks; and
  - balance development versus stability objectives.

- The legal and supervisory framework to cover both financial and nonfinancial aspects: legislation on electronic funds transfers, consumer protection, data protection, deposit insurance, anti-money laundering, exchange control, and financial transactions reporting.

- Legal and regulatory framework necessary for e-money services to be licensed/authorised
  - Unlicensed service providers may provide a potential for abuse, particularly amongst those who are poor and vulnerable.

- Evidence of adequate capital/own funds; applicant’s legal status of association.

- Description of the applicant’s governance arrangements (including risk management, and auditing arrangements and measures); organizational structure.

- The identity of directors and managers, and indications of their suitability for the job.

- The intended use of agents, branches and outsourcing arrangements, participation in the national payment system.

Key risks – legal and regulatory regime

- Licensing regimes have sought to promote competition and innovation in some jurisdictions
    - Initial capital requirements for nonbanks that are proportionate to their risk.
    - For example, the initial capital requirement for European Union (EU) e-money institutions was lowered from 1 million euros to 350,000 euros to provide a lighter supervisory regime under Directive 2009/110/EC.
- Legal and regulatory framework to strengthen safeguards for consumers including grievance redressal mechanisms; clear terms and conditions of service;
- Legal framework to provide a level-playing field that promotes competition and innovation.

Key risks – financial integrity

- E-money – a good tool for reducing reliance on the use of anonymous cash, especially in countries that are predominantly cash-based; and for promoting financial inclusion.

- E-money payments are generally more traceable than cash and can be made subject to transaction monitoring and restrictions.

- However, e-money payments do increase complexity:
  - ➢ money laundering and financing of terrorism risks;
  - ➢ e-money services are often distributed by a much wider range of service providers, including nonbank service providers and their agents than the more traditional payment methods provided by banking institutions.

- Need to adopt FATF standards to address AML/CFT risks and CDD requirements.

  - ➢ FATF standards provide room for flexibility, enabling countries to craft effective and appropriate controls without compromising financial inclusion.

Key risks – financial integrity

- AML/CFT risks may stem, among others, from:
  i. lack of face-to-face relationships, customer identification and verification;
  ii. checks on funding sources;
  iii. difficulty in compiling or aggregating transactions across different agents;
  iv. geographical reach;
  v. access to cash through prepaid cards;
  vi. involvement of non-traditional players (such as telecommunication companies) and their agents which may not be regulated for AML/CFT purposes, or regulated at a lower level than banking institutions, and
  vii. absence of obligation for the providers and agents to detect and report suspicious activity.

- Effective and proportionate application of the AML/CFT framework would help mitigate the risks associated with e-money.

- Given e-money's potential - a balance should be struck between addressing the AML/CFT risks and promoting innovation.

- The FATF Recommendations support the development and implementation of a risk-based approach to AML/CFT.

Key risks – financial integrity

- AML/CFT risks to be addressed through an effective and proportionate regulatory framework;

- Service providers (e-money issuers) and agents involved in money transmission should be subjected to AML/CFT regulation and supervision.

- Regulators to adopt appropriate risk mitigating measures such as:
  i. customer due diligence;
  ii. record keeping;
  iii. transaction monitoring and suspicious activity reporting;
  iv. placing limits to loading, value and geographical reach; and
  v. restricting the sources of funding.

- Adopting a tiered KYC/CDD regime to further financial inclusion while at the same time addressing AML/CFT concerns.

Key risks – safeguarding of funds

- E-money are stored value funds and are different from bank deposits.
- Customer funds held by nonbanks may be at risk if unprotected.
- Many low to moderate income households are vulnerable to financial losses if risks controls for e-money schemes are weak;
- Such shortcomings may pose risks to protecting customer funds if there is the failure of a nonbank payment service provider.

Key risks – fund safeguarding

Risk mitigation

- Requirement for an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the nonbank payment service provider itself, provides some level of protection in the event of bankruptcy of the issuer.
  - Example - fund safeguarding provisions in the EU PSD 2 and E-Money Directives.

- Deposit insurance normally covers potential losses from bank insolvency;
  - such deposit insurance schemes would normally cover e-money services provided as part of banking services;

- Deposit insurance schemes may not apply for nonbank entities;
  - licensing of the postal operator as a bank in order to provide deposit insurance for customer funds - Switzerland;

Key risks – fund safeguarding

- "Pass through" deposit insurance has been introduced in the United States

  - ➢ Extends the protection of bank deposits in existing deposit insurance laws to funds in stored value facilities held with insured depository institution;
    1. a separate account has been opened in the name of the holder of the access mechanism, the FDIC will recognize the holder as the owner of the deposit;

  - ➢ In an agency or custodial capacity, a pooled account might be opened for all holders; coverage is available, when 3 conditions are satisfied:
    1. Custodial relationship disclosure: The account records of the insured depository institution must disclose the existence of the agency or custodial relationship.
    2. Identity and funds disclosure: The records of the insured depository institution or records maintained by the custodian or other party must disclose the identities of the actual owners and the amount owned by each such owner.
    3. Actual ownership: The funds in the account actually must be owned (under the agreements among the parties or applicable law) by the purported owners and not by the custodian (or other party).

  - ➢ If these 3 requirements are not satisfied, the FDIC will treat the custodian (the named account holder) as the owner of the deposits.
    1. the deposit account will be treated as one account and only covered up to the limit of 250,000 U.S. dollars.

Key risks – fund safeguarding

Other safeguarding measures:

- Usage restrictions: Customer funds to be used only for discharging liabilities and fees; prohibiting use for other purposes such as extending credit (which makes such schemes similar to a bank) or covering operating expenses of the nonbank entity.

- Protection requirements: Insulating customer funds against the claims of other creditors of the nonbank in the event of its insolvency.

- Float management: A segregated trust account is held by a third party with a licensed and prudentially regulated bank. Maintaining multiple accounts at different banks to diversify risks. Holding of other forms of safe assets such as government securities.

Key risks – operational resiliency

Operational risks can undermine public confidence

- Identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls.
- Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity.
- Business continuity management should aim for timely recovery of operations;
- Cyber risk, which is a potential source of systemic risk that has wide economic impact; should have adequate cyber protection measures and firewalls;
- IT and communication security policies, CIA principles – Confidentiality, Integrity and Availability; encryption, audit system, BCP documentation
- Security of transactions and customer data
- Use of standards throughout the payments processing chain

Access to national payments infrastructure – facilitating interoperability

Interoperability is the goal – either through a mandate or through moral suasion;

- Access to national payments system infrastructure
  - Objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access;
  - Between e-money schemes;
  - Between e-money schemes and other payment systems;

- Benefits of network effects
  - Increase in access points;
  - Greater acceptability of e-money by merchants;
  - Linking to remittances;
  - Greater P2P; P2G; P2B; G2P; B2B; B2G; B2P;
  - Standardization facilitates interoperability; use of APIs;
  - More transactions and usage;

Agent network

Agent networks to facilitate greater reach for e-money schemes and customer convenience

- Regulatory framework for Agents – businesses/natural persons; risk-based approach based on permissible list of activities; client servicing;
- Principal-Agent relationship to be clearly defined; Principal liable for all activities of Agents;
- Liquidity management by Agents;
- Concept of "Super agent" and "sub-agent";
- Specific clauses to ban exclusivity;
- Interoperability of Agents;
- Training of Agents

In conclusion: an enabler for financial inclusion - transaction accounts

- E-money accounts can be classified as transaction accounts - a transaction account is an essential financial service in its own right and can also serve as a gateway to other financial services.

- Transaction accounts are defined as accounts (including e-money/prepaid accounts) held with banks or other authorised and/or regulated payment service providers (PSPs), which can be used to make and receive payments and to store value.

- The transaction account and payment product offerings should effectively meet a broad range of transaction needs of the target population, at little or no cost.

- The usefulness of transaction accounts should be augmented with a broad network of access points that also achieves wide geographical coverage, and by offering a variety of interoperable access channels.

- The legal and regulatory framework should underpin financial inclusion efforts by effectively addressing all relevant risks and by protecting consumers, while at the same time fostering innovation and competition.

- Robust, safe, efficient and widely reachable financial and ICT infrastructures are effective for the provision of transaction accounts services, and also support the provision of broader financial services.

Payment aspects of financial inclusion , CPMI, April 2016 https://www.bis.org/cpmi/publ/d144.pdf

Key challenges

Challenges

- facilitate the emergence of new, innovative and secure e-money services;
- provide new companies with access to the e-money market;
- encourage effective competition between all market participants;
- promote interoperability;
- promote financial inclusion;
- provide safe, efficient, low or no cost services to customers with customer protection measures.

Key success element: effective collaboration amongst all stakeholders: regulator; telecom authority; payment service providers – banks and non-banks; and customers.

Thank you

www.worldbank.org/paymentsystems