UN Principles for

# Responsible Digital Payments

Building trust, mitigating risks & driving inclusive economies

UPDATED EDITION, OCTOBER 2021

BETTER THAN CASH ALLIANCE

**In 2016, the Responsible Digital Payments Guidelines (RDPGs) was the first publication to chart a fairer and swifter route to financial equality.**

It did so by articulating how digital payments might better serve their users and become truly responsible. It explained how all stakeholders might follow and implement these principles.

The intervening five years have seen seismic shifts in the digital payments landscape. Every single one of these has been amplified by the COVID-19 pandemic.[1]

The digital economy is now accelerating our attainment of the Sustainable Development Goals, guided by UN Secretary General's Digital Cooperation Agenda. Governments increasingly rely upon it for government-to-person payments (G2P) - especially to the underserved and vulnerable. The fintech industry itself is innovating at speed. Artificial intelligence (AI), machine learning and big data platforms are remaking the industry at a terrific pace. These innovations bring change and risk. Worldwide, more than 80 governments have launched digital transfer programs. Those benefitting from a prior investment in digitization outperform the rest.

Growth is incredible. Yet challenges remain. Most underserved users either distrust (or are unfamiliar with) digital payments. Women are disproportionately excluded when their participation remains the single most important catalyst to financial equity.

Members are moving at lightning speed. Times are changing quickly. An enormous opportunity presents itself. To reflect these facts, the Responsible Digital Payments Guidelines have been comprehensively reworked and updated. Key additions include:

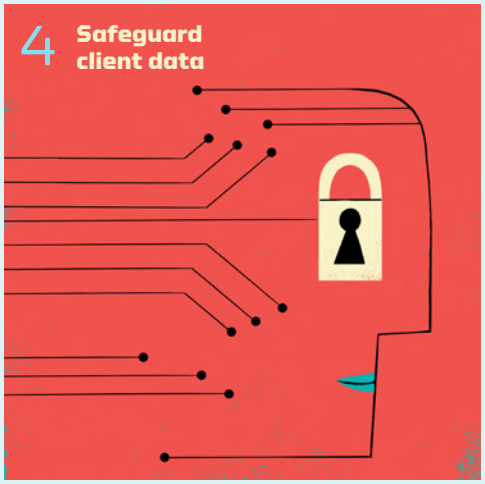
- **Women are recognized and prioritized**
- **New technologies are dissected and assessed**
- **A stronger user lens examines all aspects of digital payments**
- **Insights and experiences are pooled and shared**

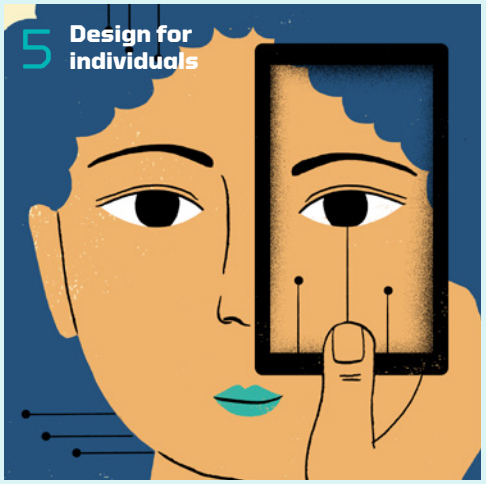
The Principles advocate for responsible practices in the digitization of payments. They are not intended to provide a technical analysis of what each Principle, such as transparency, means in practice.

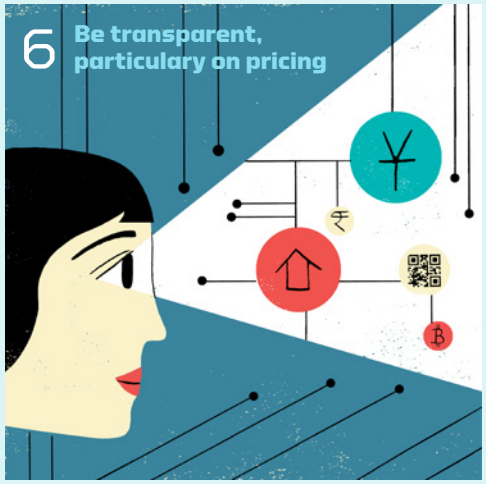
# The **PRINCIPLES**

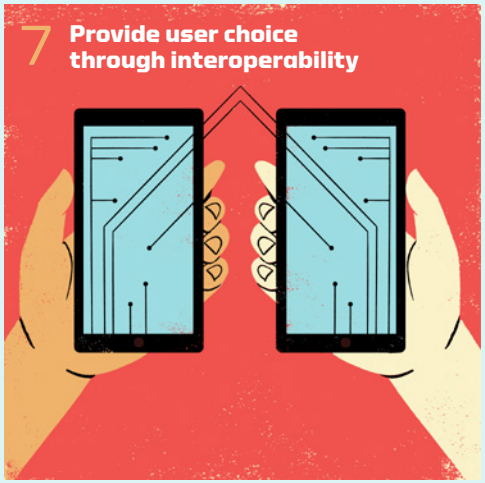
These revised principles advocate for who needs to be responsible, what it means to be responsible, and how to be responsible

Look for **EMERGING TRENDS**



*Illustrations by Hanna Barczyk*

PRINCIPLE

# 1 Treat users fairly

**An increase in use of digital payments can drive economic growth**, which, in turn, can help to attain the Sustainable Development Goals[2] by transferring value to those who need it most. Such transactions are increasingly important to people's lives, yet many users are still being treated unfairly.

Treating people with fairness is the bedrock upon which responsibility is built. Consequently, fairness remains a capstone principle.

**It is essential to note that the definition of fairness evolves in symbiosis with payment innovations. Recently, artificial intelligence (AI) has proved a powerful tool to forge better services for users. Still, left unchecked, artificial intelligence can exacerbate systemic biases and deepen discrimination against the marginalized.**

In a future where digital payments will be omnipresent, it is vital to ensure that fairness is systemically embedded.

In tandem, standards are shifting from a passive mantra of "do no harm" to an active duty to create experiential value for users.[3] Consideration is now being given to long-term positive outcomes for all users. Our members are more aware of the emerging risks and how they impact fair treatment – and are understanding better the causal links. This reveals a need to move away from merely shielding clients from risk toward boosting their agency.

As more governments, companies, and international organizations adopt digital payments, fairness and trust become central to success. For each and every user, digital payments should be demonstrably better than cash.

The requirement for fairer systems is logically irrefutable. For now, digital payments are expanding at speed, but it is salutary to consider their future. The next billion users of digital payments will comprise those who are underserved and excluded today. These users routinely face higher barriers to adoption and suffer more keenly if funds go astray, and many of these users view digital payments as inferior to cash. In part, this is attributable to expediency. Consumer protection requirements often result in provision of the bare minimum – the notion of "do no harm." Yet, consequently, inequality persists in the treatment of affluent and underserved users, and these measures are therefore insufficient. To attract sceptical users and bridge the trust deficit, systems must be inherently fair. Fairness, to this end, may be defined as occurring when all users feel supported in achieving their financial goals.

The business case for building a fair system is vested in four issues.

### 1. A payment is often the user's first experience with digital finance. It needs to work every time. Anything less and users revert to cash.

People have used cash for thousands of years. Although not without limitation, cash is familiar and tangible, and users have adapted to its constraints. Digital payments remain a relatively recent innovation and users often start this journey with scepticism. In Central Asia and Latin America, more than 32 percent of adults cited "poor trust" as a reason for being unbanked, a dynamic likely amplified in digital finance.

Even in the developed financial sector of the United States, 25 percent of users are "digitally averse," citing security concerns and low trust in digital wallets as key reasons.[4] It takes just one bad experience – a mistaken payment, an incident of fraud, a misunderstood feature – for many users to lose faith and revert to cash. It is critical to adapt for equity and consistently deliver an outstanding user experience that meets enhanced trust standards set by stakeholders collaborating to empower the next billion users.

### 2. Technologies such as artificial intelligence pose risks of bias and exclusion.

Emerging technologies such as artificial intelligence rely heavily on "rules" generated based on past human interactions and judgements.

Although latent with promise, careless implementation has led to a systemic adoption of historical inequity. Imbalances and biases against minority users or those whose actions are not captured in previous data are iterated. In a global survey of financial firms, more than 58 percent of respondents believed that mass artificial intelligence adoption would increase the risk of biases and discrimination.[5]

To prevent exclusion, concerted efforts must be made to review and adapt technologies – particularly the inputs and assumptions that shape them – to be more inclusive and reflective of users' diversity.

### 3. Digital fraud keeps pace with technological innovation.

The incidence and sophistication of fraud deters users. Nearly one in three digital payments users in India has been a recent victim of digital fraud and it remains the biggest concern for more than half of users.[6] Ransom payments increased by 33 percent in the first quarter (Q1) of 2020,[7] with attackers taking advantage of the increased socioeconomic disruption early on in the COVID-19 crisis.

This threat also extends to businesses, whose systems are susceptible to hacking and breakdowns. Nearly 60 percent of organizations experienced some form of fraud in 2020, having grown 50 percent over a 3-year period. As such, it is imperative to design highly secure digital payments to thrive in this high-risk digital environment.

### 4. There is a growing movement for businesses to invest in user-centricity and fairness.

Across industries, many businesses are recognizing that thinking beyond short-term profits is crucial to their sustainability. Around the world, governments and consumers alike are demanding greater attention to fairness from the financial services industry. Regulators must evolve to protect user interests. When businesses do not consciously step up to the plate, they risk bearing higher compliance costs and in the long run fail to earn the loyalty of the next billion users.

**The next BILLION users of digital payments will comprise those who are underserved and excluded today. These users routinely face higher barriers to adoption and suffer more keenly if funds go astray, and many of these users view digital payments as inferior to cash.**

# What constitutes fair treatment of users?

To treat users fairly is to go beyond the status quo. In interactions, this requires a move from shielding customers from losses towards building trust-based relationships. In assessing equity, it requires a shift from blind tech adoption to ethical innovation, as well as a shift of focus from wealthy or tech-savvy consumers to low-income users.

## A. Trust-based relationship

Go beyond "do no harm" to create positive relationships with users and support them when things go wrong

### Create positive relationships that exceed the transactional

- Embed sector- and institution-wide codes of ethics into all engagements. Use a customer outcomes framework or principles-based approach[8] and reduce the need to prescribe standards for each fair treatment issue.
- Continually seek user input, or feedback, into product design, so that users feel heard and that their voice has an impact.

### Prevent risks to users and compensate them fairly

- Ensure operational reliability and prevent risks that might impact a user's trust by including safety features, and create contingency plans to prevent system failures. Users should not be responsible for the inherent risks in a product's experimentation phase.
- Shoulder the burden when challenges do occur across the value chain. Ensure adequate compensation and remove liability from users, especially for reported mistaken payments, theft, fraud, or other losses that are no/limited fault of the user. Communicate assurances clearly to inspire user confidence.

## B. Realignment of interests

Align user interests with those of agents, providers, and payers

### Confer control to users

- Allow users the ability to switch providers and promote interoperability, not only for business and personal use but also G2P and humanitarian transfers. This will boost competition, leading to better offerings and lower prices for users.[9]
- Communicate terms and conditions in a way that users understand, promoting informed user choice.

**Vietnam Consumer Protection Directive**[10]

A 2019 directive affirming the enduring importance of consumer protection. Embeds responsibility in government authorities at all levels.

Issued six groups of solutions to be implemented, including improved complaints mechanisms, legal regimes, and public awareness.

**VISA artificial intelligence-enabled fraud detection**[11]

An artificial intelligence-enabled Advanced Authorization platform rates every transaction across the network on the likelihood of it being fraudulent, enabling swift detection.

**Ghana's Payments Systems and Services Act 2019**[12]

The Payments Act includes a section on principles of consumer protection. This demands that providers: transparently disclose the fundamental benefits, risks, and terms of their offering to users; provide sufficient information to users on their rights and responsibilities; and ensure responsible conduct from all staff and agents toward users.

- Develop agents' business models and training to align better with the needs of users.
- Tie agent compensation and fees to customer service. Promote rating systems for users to share feedback and prevent predatory or deceptive practices via "mystery shopper" checks.
- Help agents build their active listening skills so that they understand the impact of even small transaction failures and know to treat users with dignity and respect. This may include gender-sensitive training and responsive issue escalation matrices.
- Review provider and payer business models, keeping user interests in mind.
- Declare any unfair terms as void[13] (e.g., terms that prioritize a provider's convenience alone, reduce competition, or limit users' access to justice). Carefully select partners that align with these commitments.
- Establish fees and schedules to fit users' capacity and the volatility in their lives. Encourage good behavior and provide reasonable coverage for the costs of the specific service being offered.[14] Do not charge users for disclosing required information (#rdpg3). Acknowledge and quantify the savings payers achieve through use of digital payments and underwrite transaction costs accordingly.
- Assess potential conflicts of interest to prevent unreasonable incentives that could detract from user outcomes.

**Canadian government artificial intelligence on ethics**[15]

Released a Directive on Automated Decision-Making that pushes governments to commit to utilizing artificial intelligence while maintaining "transparency, legality, accountability and procedural fairness."

Implemented an algorithm impact assessment to score levels of risk to provide agencies with practical steps to remediate discrepancies in artificial intelligence implementation. Those results are tied back to Canadian policies on how to move forward with the project.

**US government credit data regulation**[16]

Per regulation, data on a credit applicant's race, ethnicity, and closely correlated factors such as ZIP codes cannot be used to make a credit decision.

**Ehsaas Emergency Cash (EEC) program Pakistan**[17]

Simplified the know-your-customer (KYC) procedure for users by collecting simple data fields and issuing accounts after basic verification.

Incentivized 500,000 branchless banking agents to work with the program by reducing taxes on commission earned from beneficiaries, thereby increasing doorstep banking services to elderly, persons with disability, and women.

**MTN Cameroon platform for humanitarian organizations**[18]

Created a customized cash and voucher assistance product for users in humanitarian settings without identification documents to spend at specific merchants.

## C. Unbiased tech usage

Continually monitor the ethical implications of technology on users

### Assess algorithmic biases of technological tools and set up measures for future upkeep

- Audit algorithms and their impact by introducing expert privacy representatives. They will identify biases and assess fairness to improve transparency for users.[19]
- Regularly measure and report on discrimination, especially for at-risk users. It is important to consider algorithms within the context of the design of the product as a whole and not in isolation.
- Update algorithms and other decision tools to reduce unfair outcomes.
- Collaborate with community groups to ensure accurate and powerful user feedback.
- Design algorithms "from" and "for" users with adequate representation in decision-making (e.g., include women and other underrepresented voices in design to check for biases).
- Address the sources of bias. These reside in the collection of data sets, in data processing, (actively detecting outliers and handling sensitive information properly), and in data analysis – be mindful of confirmation bias and avoid misleading trends.

### Develop a deeper knowledge of user behavior

- Contribute to building a better, more robust knowledge base of how users behave and use digital payments. Accumulating data on underrepresented segments of users in data sets can help reduce occurrences of bias. Members can use data on first-time users to build intelligence for the common good and better tailor offerings for diverse user segments.

## D. Inclusion for all

Humanize the user experience and create user satisfaction

### Provide experiential journeys for all users with different needs and capabilities

- Respect users' time and resources regardless of who they are or the value of their transaction. Commit to equal opportunity and nondiscrimination on gender, sexuality, religion, and ethnicity. Enshrine these values in a code of ethics or principles.
- Install processes to understand user needs and design alternatives across this journey to accommodate diversity, especially for first-time and previously excluded users. This may encompass larger print for those with vision impairment or sufficient cash-in-cash-out (CICO) points to ease the transition from cash for first-time users.
- Ensure information is not merely shared but understood by all users, giving them confidence and helping them to meet their goals.
- Ensure user experience with digital payments is delightful.
- Design products that are more than just functional and aim to generate user satisfaction, such that the value proposition of digital payments exceeds cash in its ease, speed, safety, control, and transparency.
- Collect disaggregated data to track progress at the firm and sector levels. Revisit and update services based on changing circumstances, behaviors, preferences, and aspirations.

**Nearly 60% of organizations experienced some form of fraud in 2020**

CASE STUDY

# Ingreso Solidario

## Colombia's G2P cash transfer program in response to COVID-19[20]

**The Financial Regulation Unit (FRU), in collaboration with the National Planning Department (DNP),** launched a G2P financial service provider (FSP) program to provide timely and adequate relief to households both severely impacted by COVID-19 and excluded from G2P payment schemes. Despite operational challenges, the program successfully transferred US$42 monthly to 3 million households (60 percent headed by women), many of whom were hard to reach. Sixty-two percent of recipients made digital transactions with the funds and 42 percent deposited additional cash into their digital wallets. This success is largely a result of close collaboration between the private and public sectors, investment in a national social registry, a wide network of on-ground agents, and tailored solutions.

### Notable features

#### Inclusion for all

- Three user segments were recognized that required different approaches: bank transfers for the banked, digital onboarding and mobile transfers for the unbanked, and cash transfers for those not willing to use any financial product.
- For easy onboarding of the unbanked, text messages were sent directly to their mobile phones, indicating where and how to open a digital wallet account.

#### Trust-based relationships

- Fraud potential was high, given outdated mobile numbers in the existing social registry. The FRU signed an agreement with the credit bureau to overcome this by designing a unique HASH number[21] for those in the database.
- School registries were used and a survey implemented to validate identities of those not in the registry.

#### Realignment of interests

- The FRU aligned private interests with the government's goal to serve at-risk users by positioning FSPs as co-creators of solutions rather than as entities to be controlled, and welcomed participation in decision-making via a "situation room."
- Interoperability was boosted by setting up a fast payment clearing house, enabling collaboration between banks and fintech players.
- Ingreso collaborated and coordinated with the regulator to ensure payments were made smoothly.

## Implementation journey

### 1. Strong foundation for smooth implementation

- Created a national social registry consolidating data from the existing national ID system and multiple other public, private, and credit bureau sources, which allowed for effective mapping of at-risk households across the country.
- Enhanced internet and mobile connectivity by subsidizing access for at-risk users and incentivized telecom providers to adopt an app by providing free data.
- Instituted regulatory frameworks through simplified KYC (remote opening enabled, requirement for paper formats and electronic signature eliminated[22]), which eased onboarding, and permitted non-banks to develop their own payments platforms, which increased competition and gave users a wider choice.

### 2. Situation room to leverage private players to the fullest potential

- Brought 22 FSPs on board as co-creators and set up participative decision-making to build trust, discuss user barriers, and mitigate risks together, while also enabling competition and comparative advantage.
- Collaborated with banking association of Colombia to ensure a smooth flow of information and best practices with FSPs.
- Emphasized need for a user-centric approach in designing platforms via: forbidding automatic debits from beneficiaries (e.g., for overdue loans before they had access to subsidy); agreement with banks to not charge high ATM fees to beneficiaries and to authorize free electronic transfers between accounts; and FSPs asked to enhance call centers for support in onboarding and recourse.

### 3. Extensive identification of beneficiaries

- Prioritized users not covered by prior government cash transfer schemes and therefore most at risk. Partnered with local municipalities and the postal service, harnessing a wide network of on-ground agents who conducted onsite visits to identify households not in the social registry.
- Classified households by their access to formal finance and mobile phones to determine the optimal channel for cash transfer.

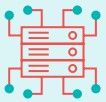
### 4. Tailored product and outreach based on beneficiary needs

- Conducted outreach through multiple channels – SMS, social media, mass media, postal mail, physical visits – to reach all identified beneficiaries.
- Developed on-site KYC facilities in rural areas to ease onboarding, while providing digital financial education to new users.
- Urged FSPs to make apps available for both feature phones and smartphones to ensure access for low-income segments.

## KEY LEARNINGS

**Use multiple modes of outreach and create customized product designs for users.** The program emphasized user preferences by employing multiple outreach channels to onboard users, and multiple FSPs were encouraged to design their payment platforms accounting for diverse user needs and preferences.

**Collaboration between local governments and FSPs provides twin benefits of wide reach and tailored solutions.** The FRU onboarded key stakeholders in a timely manner and created a platform to exchange best practices and information. It successfully used the reach of local municipalities and the adeptness of private FSPs to create tailored solutions.



**Enhance mobile and internet access and create a competitive payments environment.** Internet and mobile subsidies were key in ensuring user access to digital platforms. Regulations increased competition among FSPs while promoting user choice.

## KEY CHALLENGES

**Reaching users without access to mobiles and IDs.** Identifying and understanding requirements of beneficiaries outside the national ID system and SIM registry was a costly and inefficient process that required door-to-door visits from on-ground agents and coordination with multiple parties.

**Providing users with the ultimate choice on mode of transfer.** The program did not enable users to choose which FSP they wished to hold an account with, nor did it allow for ATM interoperability. These important steps for user choice have now been prioritized for phase two of the program and extended to other G2P payment schemes.

**Prioritizing at-risk users during a time and resource crunch.** Reaching and serving at-risk, hard-to-reach communities while balancing business model sustainability for private FSPs represented an inherent challenge and required flexibility.

© Shutterstock

Treat users fairly

# Recommendations

Governments, companies, and international development organizations (IDOs) have an **opportunity to leverage partnership agreements** with digital payment providers to include commitment to Principles 1-9 and ensure fair treatment of the next billion users.

All members can **define fair treatment** in their strategies to help guide their partnerships to deliver outstanding digital payments experiences for users.

All members can **champion the collection of user data** in disaggregated forms to reveal segment-wide trends around transactions and user challenges.

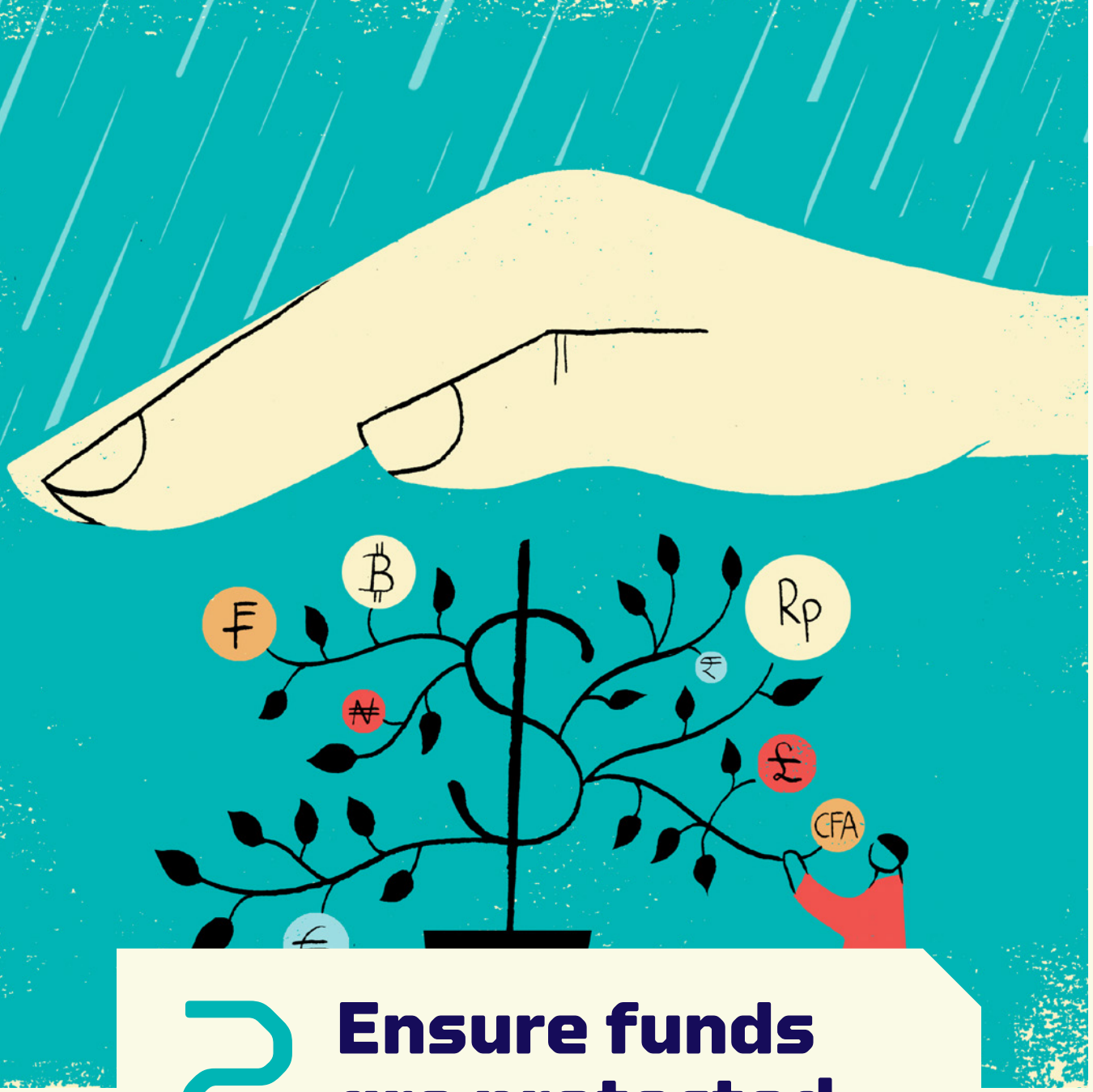
All members can collaborate with civil society-advocacy groups or think tanks that **scrutinize and spread awareness** of gaps in digital payments and algorithmic technologies.

Governments and IDOs can **invest in user-centric tools** such as local language-enabled voice messages resulting in greater access to and usage of digital payments platforms among excluded groups.

Treat users fairly

# Recommendations

| For **GOVERNMENTS** | For **COMPANIES** | For **INTERNATIONAL ORGs** |
|---|---|---|
| **Governments are uniquely positioned to lead national, regional, and global collaboration to regulate the responsible use of artificial intelligence in digital payments considering power asymmetries and protecting vulnerable populations.** | **Companies can consider how to leverage their supply chains and processes to drive user-centricity and be the first line of recourse for digital merchants and users.** | **IDOs can build greater trust in digital payments through clear and accountable principles for fraud, theft, and mistaken payments. This includes liability for providers on activities of agents and employees, and relaxations on the types of ID required to register.** |
| **Governments can espouse fair usage by reviewing the impact of algorithms and scrutinizing the inputs and assumptions in key areas such as customer profiling and recommendation engines to identify discriminatory biases.** | **Companies can collaborate to distill key insights to improve the digital payments experiences of their supply chains, holding partners accountable to high standards.** | |
| **Governments can ensure artificial intelligence ethics discourse is local and specific by relying on empirical research, widespread consultation, and pilots.** | | |




PRINCIPLE

# 2 Ensure funds are protected and accessible

**The blisteringly rapid growth of digital payments has exerted pressure** on all aspects of service delivery: 1.2 billion more users have been added since 2017 and the curve is steepening. Under this deluge, systemic fissures are widening. As noted, digital payments should work every time. Anything less breeds distrust among new or potential adaptors.

**A prerequisite of digital payments is that they match or surpass the qualities of cash. All users rightly expect their funds to be safe and readily available, but this is not always the case. The causal factors behind this are multiplex.**

As payment volumes increase, so too do those of fraud. Risks of fraud are unevenly distributed, with those most vulnerable exposed to a greater degree. Indeed, more sophisticated systems appear to deter fraud more effectively.

From a user's perspective, funds can seem to disappear via mistaken transactions and poorly communicated fees. Even when funds are safe, system downtimes and last-mile challenges can make them inaccessible in times of need.

For marginalized users, these challenges have devastating consequences. Delayed payments can lead to home foreclosures. Interrupted bank transfers can damage relationships between senders and recipients. Such effects exceed inconvenience. They take funds out of reach for users who have very little room for error in their financial lives. Ultimately, confidence in digital payments decays.

**5+ BILLION**
**people globally**
**use digital payments**

Historically, such risks have been addressed by regulators and service providers. But significantly moving the needle requires leadership from all sectors, including governments, companies using digital payment service providers (PSPs), and IDOs. These crucial actors can leverage their relationships with users and providers to safeguard user funds.

**Today, more than 5 billion people globally use digital payments.** Maintaining user confidence in the safety and accessibility of their funds is paramount. Initially, this means giving users proof that their funds are safe and then providing the tools necessary to access them at any time.

**Despite progress in consumer protection regulations, compliance and oversight is often weak. Providers have had mixed success, resulting from four key challenges.**

### 1. Systemic issues often inhibit access to funds.

As digital payment ecosystems grow in scale and complexity, their dependence on reliable infrastructure increases commensurately. These dependencies are not always addressed. A 2015 study found that a third of mobile money users across six countries experienced delayed or interrupted transactions because of network difficulties.[23] This is exacerbated by back-end systems that are often complicated or difficult to change. The resulting integration gaps are magnified at scale, as systems are placed under progressively greater burden.

When digital payments in India increased following the outbreak of COVID-19, time-out failures also increased from 3 percent to 12 percent.[24] As a result, users were unable access their funds when they needed them. Yet worse, some found their funds stuck in limbo where neither the payer nor the intended payee could access them. Faced with uncertainty, users may resort to risky

behaviors, such as sharing account details with agents and other third parties. Conversely, users may erroneously believe their transaction to be successful, leading them to default on important payments. Improvement in technology to handle higher volumes, such as during pandemics, and instilling public confidence in digital payments is crucial.

### 2. Reactive fraud management is inadequate.

As technology grows in complexity and speed, the window for detecting fraud is shrinking rapidly. Transactions take place across complex interconnected systems, increasing the number of access points available to cybercriminals and paving the way for fraud. Moreover, funds flow across systems more quickly, creating opportunities for a range of actors – including third party hackers, business partners, merchants, employees, and agents[25] – to execute fast-moving fraud before providers can be alerted. In the short term, tenuous fraud management means users are deprived of hard-earned funds. In the long term, heightened risk drives users away.

### 3. Users struggle to understand complex payment interfaces.

While regulators have addressed the issue of safeguarding funds at the bank level, users can still have trouble accessing their funds in practice. This challenge stems from products, partnerships, and systems that are well intentioned but inadequately designed to facilitate user access. Unintuitive menus and navigation tools, lack of local language support, cumbersome transaction or opaque recourse workflows make products hard to use. Further, users may cope with challenging interfaces by seeking help from an agent, or third parties, exposing themselves to greater risk of fraud. This leaves underinformed and digitally less-literate users at risk of losing funds through unauthorized transactions and fraud. It also leaves them underequipped to report these issues in a timely manner.

### 4. Last-mile challenges with agents.

As more people use digital payments, the need for agents as cash-out points and providers of assistance assumes increasing importance. By December 2019, there were more than 7.7 million registered agents – more than 2.5 times the count from 5 years earlier.[26] However, agent-assisted transactions carry unintended risks. Underinformed users can be exposed if their agents have insufficient know-how (e.g., of payment flows for complex products such as insurance), resources (e.g., insufficient float), or unscrupulous goals (e.g., charging unauthorized fees).[27] Fifty-seven percent of respondents to a 2015 survey of Kenyan mobile money users were unable to complete at least one transaction because of insufficient agent liquidity. This risk is even higher with digital social benefit transfers.

A further complication resides in the fact that incentive structures are often misaligned, encouraging banking agents to disregard users' best interests to maximize fees. These risks erode the quantum of funds that ultimately make their way into users' hands.

# What does it mean to keep users' funds safe and accessible?

Successfully putting users' funds within their reach means giving them transparency and control of being able to view, access, and use those funds on demand. It also means giving them the confidence that all necessary steps are being taken to safeguard their funds - both proactively, to prevent loss or compromise of their funds in the first place, and reactively, to ensure swift action is taken following a loss of funds.

## A. User control

Make funds visible and available to users when they need them

### Equip users with the resources they need to manage their funds and avoid risks that could compromise them

- Educate end-users on their rights and the tools they can use to exercise them. Core rights may include: the ability to view their current balance and transaction trails for free at any time via channels that work for them; transparent terms and conditions including pricing and fee structures to minimize risk of fund erosion; and guidance on behaviors that create security risks (e.g., not keeping PINs confidential) through public education campaigns, agent engagement, etc.
- Support the development of intuitive user interface/user experience so that digital payments are as clear or clearer than cash, especially for new users. Provide simple, digestible, and action-oriented menus and visual cues that steer users away from falling victim to fraud or mistaken transactions. Educate users on the different UI/UX for requesting vs. making payments[28] while also promoting preventive behaviors – "Never share your OTP/PIN."

### Ensure that users can use and cash-out funds on demand

- Invest in infrastructure and technology that achieve real-time, affordable payments.[29] Pay particular attention to back-end architecture and intuitive front-end interfaces that enable immediate settlements. Build toward broad-based interoperability to minimize integration gaps for transactions that cross multiple platforms, retailers, or billers.

**Nigeria's instant settlements service**[30]

Nigeria's Inter-Bank Settlement System (NIBSS) uses a central payment switch to enable seamless transfers between accounts held in commercial banks.

Fees were imposed on users transacting above specified amounts, which constrained cash-outs and ultimately limited uptake. To reduce fund erosion and encourage uptake, the limits were increased (to US$3,000 for individuals, US$18,000 for companies) and fees were scaled down.

To ensure user funds are backed with sufficient liquidity (particularly salaries and pensions), participating institutions are required to secure them in prudentially regulated deposit money banks.

**It also means giving them the confidence that all necessary steps are being taken to safeguard their funds – both proactively and reactively**

- Enforce norms for backing users' e-money funds with safe and liquid assets protected from insolvency in providers' institutions. For example, 100 percent matching funds for user balances held in prudentially regulated banks and prohibited from usage as security for debt or claims by third party creditors.[31]
- Ensure users can use or cash-out funds reliably and conveniently. This may include incentive and penalty systems across the value chain to ensure that agents are accountable for maintaining the requisite float and avoid unethical practices (e.g., multiple small transactions to drive up fees).

## B. Loss prevention

Build infrastructure to mitigate loss of user funds resulting from circumstances beyond their control

### Prevent operational reliability and security failures via systems testing and monitoring

- Develop policies and directives to license providers and monitor their compliance against standard national and regional protocols for funds safety and availability.[32] For example, in business continuity planning, backups and appropriate governance (e.g., the European Union's Payment Services Directive [PSD2]).[33]
- Ensure providers continuously stress test systems to identify and resolve inherent vulnerabilities (e.g., siloed organizations and governance mechanisms, weak malware defences), particularly for legacy technologies such as USSD and SMS.
- Keep in mind a risk-based perspective when instituting security requirements, recognizing that some requirements may pose barriers to users with limited tech access and capability (e.g., in many countries, transactions via USSD require five to six time-constrained steps, which can lead to repeated time-outs for less digitally literate users).

### Proactively track and protect against unauthorized transactions, including fraud and mistakes

- Advocate for appropriate security controls to mitigate transaction risks (e.g., biometric security,[34] two factor authentication,[35] limits on logins or transaction amounts,[36] creating "need-to-know" administrative privileges for interacting with client data).
- Realign agent incentives to minimize price gouging by agents seeking to maximize transaction volumes (e.g., reward continued active use vs. number of registrations).
- Train and support fraud reporting in the transaction data. Establish clear protocols and escalation matrices.[37]
- Cultivate data analytics capabilities to detect suspicious behaviors and transactions, being cognizant that real-time settlements significantly reduce the fraud detection window.

**Rappi and VISA's e-wallet for LatAm users**[38]

Rappi, a Colombian fintech, leverages VISA's globally recognized fraud management solution, CyberSource, to proactively mitigate fraud risk in its digital payments.

The system uses machine learning to identify fraudulent transactions in real time (e.g., learning from historical fraud patterns to recognize new instances of fraud near instantaneously).

The system also sought to pre-empt fraud through a rules-based algorithm that "tells" the system which transactions are permissible, proactively safeguarding users' funds against fraud.

## C. Compensation

Where losses occur, compensate users seamlessly

### Shift the burden of detection from the user

- Automate failure detection, kick-starting compensation processes without requiring user reporting. In particular, apply this to cases of fraud stemming from the actions of employees or reasonably preventable security failures.
- Offer settlement guarantees to enable timely compensation to users after loss of funds, or – in cases where the user is liable for a loss – require providers to give evidence.[39]
- Ensure providers disclose fraudulent transactions, system breaches, or shutdowns to users,[40] limiting the user's responsibilities and liability in such situations.[41]

### Equip users to be compensated in a streamlined manner

- Push out notifications to users confirming initiation and completion of any transactions via their account, enabling them to independently monitor for unauthorized transactions.
- Facilitate agreements between providers to distribute liability based on system compromise, ensuring relevant providers and sending/receiving institutions take full responsibility for the actions of their staff and agents.
- Incentivize and enforce strong recourse provision for user compensation requests, ensuring clear standards for timeliness (e.g., managed through ticketing/complaints tracking systems) and quality of redressal (e.g., by equipping agents with training, scripts, and active listening skills, and escalation matrices for more complex cases).

**India's Unified Payments Interface**[42]

Near-guarantee of instant settlements allows the Unified Payments Interface (UPI) platform to identify instances where transactions fail and proactively initiate reversals, as needed.

Instant SMS notifications are sent to the payer and payee upon successful completion of a transaction, giving them information to independently flag fraudulent or mistaken transactions.

The platform eliminates users' risk through a settlement guarantee fund worth approximately US$27 million. The fund is managed by National Payments Corporation of India (NPCI) and sustained through contributions from participating providers. This settlement ensures that victims of fraud are immediately compensated while their claims are explored.

CASE STUDY

# Mexico's Cobro Digital (CoDi)

## A mobile payments gateway enabling instant, secure settlements[43]

**In late 2019, the Central Bank of Mexico (Banxico) announced the Cobro Digital (CoDi) platform**, which mounts secure payment request functionality onto Mexico's existing Instant Electronic Payments System (SPEI) via a user-friendly mobile front end. The platform uses quick response (QR) and near-field communication (NFC) technology to rapidly connect users that trust one another and to facilitate secure, instant, and free digital transfers between them. These technologies are supported on the back end by SPEI, which rapidly executes a high number of short settlement cycles to enable secure movement of funds in near-real time, keeping funds within users' reach and building their confidence in the safety and reliability of digital payments. As of September 2020, CoDi had onboarded 39 participating banks with nearly 140 more expressing interest and more than 5.1 million validated accounts.

### Notable features

#### User control

- Used QR technology to allow payee and payer devices to identify each other, lowering the risk of mistaken transactions.
- Used NFC technology to allow trusted mobile devices in direct proximity to transact safely and reliably regardless of connectivity.
- Featured an intuitive interface that displays the user's account balance and recent transaction history.

#### Loss prevention

- Gave users the option to add secure access controls to the application using biometric or face scan technology.
- Supported the SPEI platform with an automated application programming interface (API) based e-reporting tool, which sources data from FSPs, and uses machine learning to flag suspicious transactions, reducing funds loss.

### Implementation journey

#### 1. Building a technical and regulatory foundation

- Deployed the SPEI to replace the country's legacy settlements system, enabling instantaneous 24/7 digital settlements. Participation in SPEI was opened to all regulated financial entities.

- Set norms requiring participating banks to credit payments within 1 minute. SPEI's norms required payment orders to be sent within 30 seconds of a request and payments to be credited after an additional 30 seconds, building user confidence in funds security.
- Used an open protocol system allowing participating banks to further innovate and automate to improve safety and efficiency.

### 2. Going beyond the foundation and conceptualizing the product

- Developed early prototypes for a user-friendly front end to SPEI, enhancing usability for peer-to-peer (P2P) and peer-to-business (P2B) use cases. This yielded the early concept for CoDi.
- Conducted a roadshow to share the concept with the formal financial ecosystem. This was focused on sharing product mock-ups, explaining how the system would work and sensitizing the business case for instant, zero-cost settlements.
- Developed an application together with fintech partners, settling on QR, NFC, and push notifications as technologies for optimizing a secure user experience.

### 3. Piloting with users and iteratively building the solution

- Conducted pilot studies in three cities around the country, introducing an early version of the CoDi platform to communities of representatively varied characteristics. Surveyed participants to gauge satisfaction levels (80 percent), while also revealing areas for improvement.
- To drive early acceptance, mandated all banks with more than 3,000 accounts registered in SPEI to transact via CoDi. Onboarded banks (including 33 of Mexico's 51 private sector banks) to build their readiness for rolling out the CoDi platform and initiate further in-house testing programs.

### 4. Building toward scale

- Used diverse communication channels (including SMS, social media, television) to reach a wider audience, showcasing the benefits of using CoDi over cash (e.g., greater security of funds, instant settlement) and risky behaviors to avoid when transacting digitally.
- Onboarded approximately 150 merchants across sectors to build greater acceptance and familiarity with cornerstone technologies (e.g., QR, NFC) and instill best practices for safe digital transacting.

## KEY LEARNINGS

**There is a trade-off between security and seamlessness.**
The CoDi platform is built on Mexico's existing settlement architecture, which has successfully used strict security controls to ward off cyberattacks. However, some of the platform design features, such as multiple verification steps for each transaction, can diminish ease of use.

**Instant settlements need a robust back end to work.**
SPEI required years of time and resource investment. Countries that have not made this investment may not be equipped to deploy similar solutions.

**A communication plan should be in place for providers.**
Banxico challenges assumed the product would sell itself to banks; however, the implications of a zero-fee model concerned banks, worried about its impact on their fee-driven business model. Addressing these concerns is important when building institutional relationships.

## KEY CHALLENGES

**While the application offers strong security measures at the back end, user-facing risks remain.** Users, particularly those transacting digitally for the first time, are often underinformed about risky behaviors (e.g., sharing their account credentials). Thus, they are easily targeted by phishing scams and other forms of fraud. This challenge highlights the importance of user-centric design, behavioral nudges and proactive transparency to empower and equip users, particularly during onboarding.

**Infrastructural challenges hamper performance and undermine confidence.** Less than 1 month after the launch of CoDi, bank transfers that had been advertised as instant were delayed by low network connectivity and system overloads. These delays were an early blow to the confidence of users already reluctant to transact digitally.

© Better Than Cash Alliance

**Ensure funds are protected and accessible**

# Recommendations

Governments, companies, and IDOs can **increase the scope of partnerships** with digital payments companies to maximize transparency of terms and conditions to users, such as local language translation and voicebot-enabled education to support the user's ability to access their funds.

Members can advocate with their regulatory guardians for three key principles that ensure access to funds:

- **advocate for real-time payment infrastructure** to minimize loss and interruption in service to end-users
- **advocate for safeguards** to ensure user funds are protected in the event of system failures
- **advocate for policy interventions and incentives** for financial service providers to ensure sufficient accessibility and liquidity for end-users to access their funds.

**Ensure funds are protected and accessible**

# Recommendations

## For **GOVERNMENTS**

**Governments can support public awareness and education campaigns on managing and protecting funds against phishing, spoofing, and social engineering, and steer users away from risky behaviors such as leaving their phones or account details with third parties.**

**Government can shape the policy discourse around consumer protection and collaborate in the implementation of:**

- **developing regulatory frameworks that guide the registration and licensing of providers and agents**
- **establishing consumer feedback-based benchmarks around funds and observing ethical practices**
- **developing and enforcing robust selection and training practices that reflect the more complex role of digital financial agents compared with traditional banking agents.**

## For **COMPANIES**

**Companies can support their supply chain to ensure user funds are always safe and accessible, and that recourse systems are timely and fit for purpose.**

## For **INTERNATIONAL ORGs**

**IDOs can provide technical assistance to product features and user interfaces that minimize mistaken transactions and equip users with reminders on how to avoid fraud and consciously focus on last-mile, small-value transactions.**

PRINCIPLE

# 3 Prioritize women

**To unleash the full potential of digital payment services,** industry must overhaul its approach to women. Governments and the private sector are increasingly aware of the transformative power of female enfranchisement on digital payment platforms. Recent female-focused welfare transfers during the COVID-19 crisis amply illustrate this. Success stories of women as merchants fail to be reflected in merchant infrastructure fund allocations.

**Yet, as the industry reaches out to women, significant scope for improvement remains. These opportunities ought to be maximized. The UN Principles for Responsible Digital Payments provides a freely sharable roadmap for change.**

Women represent a major constituency in the digital payments landscape. Too often, they suffer from systemic and organizational biases that exclude them. Artificial intelligence programs designed to highlight suspect transactions often hardwire existing gender disparities into services, and the services themselves are not optimized for women. Design needs to be gender-intentional, rather than gender-neutral, and legislators can help by building enabling regulatory environments that boost female service uptake.

To achieve the requisite sea change, women's voices need to be included at the decision-making stage. Products must reflect and improve women's lived realities. Data analysis needs to be fully gender-disaggregated to provide the ecosystem with the insights needed to drive improvement. The shifts in emphases required are both subtle and profound. They are also eminently achievable.

Prioritization of women is now crucial to the realization of financial equity. Consequently, the need to prioritize women is manifested in a new principle.

In point of fact, the case for extending digital payments to women is already manifest.[44,45] Women generate strong financial and social benefits. Leading reports highlight how digital payments transform the lives of women by helping them save formally and insulating themselves against financial shock. Yet, today, over 70 percent of female-owned businesses in developing countries remain unbanked.

For female entrepreneurs, access to digital payments means improved performance and creditworthiness. In turn, women exhibit enhanced product loyalty and corporate responsibility. Underpinning all else is the fact that digital payments are a gateway to broader digital inclusion, evidenced by the UN Human Right's Council's call to bridge the digital divide.

In a powerful ripple effect, affording women greater financial autonomy yields a demonstrable and catalysing effect upon their communities.[46,47] They pass on their financial knowledge to their children and are more likely than men to invest in health and nutrition.[48]

Women, therefore, constitute a vast, untapped market opportunity. Although they comprise nearly half of the world's population, they are hugely under-represented in the financial services sphere. Men account for 80 percent of loan volumes and 75 percent of global deposits.[49]

Despite compelling cases, there are serious and systemic barriers that make this roadmap ambitious. Nonetheless, it is encouraging to note that many ecosystem players are making efforts to bridge the disparity. In practice, countries are beginning to dismantle the systemic barriers that frustrate the potential that digital payments hold for women. These efforts should now be mainstreamed.

**47 MILLION more women and girls**
**are estimated to fall below the poverty line in 2021**

Three salient impediments to adoption exist.

### 1. Women lack connectivity, digital identity and have limited digital financial capability.

The confluence of these three issues deprives women of the toolkit they require for accessing digital payments. Globally, just under a third of women are financially literate,[50] and consequently tremendous opportunities exist to build their capabilities using voice-bots and other technologies that lower barriers to access and usage. Fewer women than men own a mobile phone,[51] and women are more likely to lack a formal ID.[52] Progress toward rectifying this should be accelerated, as it is known that people with formal ID are much more likely to hold accounts with financial institutions, own mobile phones, and to have acquired the levels of financial literacy necessary to use digital payments.

### 2. Social and regulatory barriers prevent women from transacting.

Social norms restrict women's ability to access mobile phones and the internet. In Pakistan, family disapproval is the main factor preventing almost 30 percent of women from using mobile internet.[53] Discriminatory gendered norms extend to national regulations, and correlate with lower levels of financial inclusion.

In Afghanistan and Benin, married women cannot obtain national ID in the same way as men and require a man's signature to open an account. Of women responding to a Global Findex survey, 20 percent cited restricted access to ID and the resultant barriers as key reasons for not having an account.[54]

### 3. Inadequate service design means that digital services do not fit women's lives.

Service design that is considered gender "neutral" is often merely gender "blind." Services are designed for men by default. This is driven by fewer instances of women in decision-making positions within those institutions that shape digital payments.

Poor design hurts women. Misaligned offerings and unsafe onboarding prevent women from demanding access to such services. To design better services for women, industry requires both a firmer commitment and a deeper understanding of their wants and needs, based on data.[55]

**Unilever Pakistan**

Unilever Pakistan partnered with mobile financial services provider, JazzCash, to enable members of their micro-retailer program, Guddi Baji, in rural Pakistan, to become roaming banking agents, to drive the financial inclusion of women in rural Pakistan.

The program is designed specifically to overcome obstacles to women's financial inclusion by addressing challenges around access to transportation, social taboos, and lack of financial literacy, by employing familiar, trusted community members to ease the onboarding and adoption process.

# How can women be prioritized?

These, then, are the most important design considerations[56] by which members can incorporate gender intentionality into their implementation of each RDPG.

## Treat users fairly

> **If I don't trust something, I will never put my details there, [if] I cannot handle mobile money then it is not safe.**
>
> Salina, Côte d'Ivoire[57]

- Identify and correct algorithmic biases in new technologies (e.g., artificial intelligence used for tailored customer service and product marketing) by adopting balanced approaches for dealing with outliers either by promoting self-regulation or through oversight committees.
- Include more women employees in digital payments institutions and women agents in banking networks. Treat them respectfully and empower them.
- Take an intersectional view, especially as part of social protection programs (e.g., disabled, LGBTQ+, women facing unique barriers to access, etc.).

## Be transparent with users

> **I read the first line, because it's probably the most important, and the shortest two lines. I skipped everything else.**
>
> Varsha, India[58]

- Ensure relevant communication on critical features – such as service terms, applicable fees, and account records – are designed for the base level of technical capability.
- Ensure that women, especially first-time users, can make informed decisions (e.g., simplified disclosures that account for lower financial and digital literacy, multiple avenues to share features such as print forms, mobile SMS, and social media).
- Ensure social norms are considered in sharing product information with women and account for any unintended consequences, such as delivering information without putting the user at risk through cultural insensitivity.

## Support user choice through interoperability

> **I don't use my phone [for electricity bill payment]. To transfer money, I use 'Paga' to get money on phone, then I withdraw it to transact in cash.**
>
> Adegoke, Nigeria[59]

- Promote interoperability in both government and private payment systems, especially those advantageous to women, who are less likely to have multiple phones or SIM cards to transact across diverse payment systems.[60]

## Serve as a steward for end-user data

> **I have no idea why they ask me for this data. What do they do with it?**
>
> Champa, India[61]

- Ensure gender dynamics are considered in data confidentiality and ownership. There may be instances where women may not wish to disclose the existence of an account or individual transactions to family.

- Be vigilant in stewarding women's data, recognizing that consequences of data misuse, especially loss of funds, are likely to bear greater risks for women (e.g., domestic violence in case of fund loss or identity theft).

## Ensure user funds are safe and within reach when needed

> **My sister withdraws and brings the money for me.... She tries to teach me, but I'm scared with all those buttons of messing up and losing money.**
>
> Woman, Colombia[62]

- Account for women's differing needs around frequency of fund withdrawals, preferences for proof of transactions, and lower financial capability to make funds more easily accessible.
- Secure funds in a manner that accounts for women's greater need for confidential transactions and helps build trust in digital payments.

## Design for user needs, preferences, and capabilities

> **I would prefer to receive financial advice from a woman. Someone who will be close to me. Right now, I just ask myself.**
>
> Fatima, Tanzania[63]

- Create products and experiences that account for gendered barriers (e.g., poor access to ID, lack of mobile device, and limited technical functionality) and needs, for instance, the inability to open accounts without the husband's approval.
- Use messaging content and channels that resonate with and are preferred by women (e.g., messaging anchored on aspirations for children's future, interactive voice response over text-based apps).
- Incorporate product features that cater to gendered literacy rates.

## Promote responsibility across the value chain

> **If you already paid online and change your mind - the refund will take too long! But with cash payment, you just don't pay if you don't want the item.**
>
> Sophia, Côte d'Ivoire[64]

- Ensure women's needs and aspirations are protected at all points in the value chain (e.g., providing gender-sensitive agent training or having more women in client-facing roles).
- Hold actors across the value chain accountable for ensuring that women's interests are adequately safeguarded, particularly to protect against higher risks of fraud, data misuse, or violence.

## Serve as a steward for end-user data

> **Calling a toll-free number to complain about violations will not work because it will always be busy.**
>
> Saliya, India[65]

- Design recourse systems that allow women to seek it more easily. There is a preference for more in-person recourse channels that are led by women employees and agents. Increase the availability of women operators on helplines and ensure operators are trained in gender sensitivity.
- Design recourse systems to accommodate constraints that more severely impact women including literacy and numeracy.

# Why prioritize women?

Embedding a gender lens across the RDPGs is a crucial first step. Yet, closing the gender gap will require transformational measures that prioritize women and redress their systemic exclusion. Consider the following five keystones.

## A. Gender-disaggregated data

Proactively track gender dynamics and apply insights

### Collect sex-disaggregated data to track women's experiences with financial services

- Ensure basic data collected are disaggregated by sex (e.g., account ownership, volume of transactions, frequency of usage, peak times of usage, complaints). Gather data points that also capture short- to-medium-term changes in women's access to digital services (e.g., the number of women downloading and/or registering for an app).
- Collect user-facing quantitative and qualitative data (e.g., loyalty, satisfaction) to understand whether women desire access to specific services.
- Collect provider-facing data (e.g., account usage, transaction volumes, attrition) to understand the performance of products and services across different segments of women.

### Use data insights to promote easier access and usage by women

- Analyse collected data on women along with feedback to iterate on products and improve relevance. Greater user and transaction data on women help to reduce biases in algorithms.

## B. Inclusive policies for women

Reimagine the policy environment to support women's use of digital payments

### Review discriminatory laws and policies to enable financial independence of women

- Reshape regulatory and legal frameworks to address identified challenges. Reduce women's dependence on men in accessing digital financial services (DFS) (e.g., eliminating discriminatory property laws and policies that require a male co-signer when opening an account).
- Identify opportunities to promote digital payments among women and build financial capabilities in other policy actions (e.g., higher cash transfers and benefits directly to women).

### Reduce documentation requirements to ease access, benefiting all marginalized groups

- Develop systems that accept alternative forms of identification that are more accessible, such as regional or local identification cards and digital IDs, as sufficient supporting documentation for opening accounts.

**Chile's commitment to sex-disaggregated data**[66]

Requested that commercial banks collect sex-disaggregated data and established a centralized unit to analyze data and publish emerging insights on an annual basis. Chile has been doing this for over two decades.

Started this effort by capturing data on volume, value, and frequency of transactions. Has since expanded to demographic and income data, all benchmarked with other countries.

Commercial players and Chile's only public bank leveraged these data to target women entrepreneurs through capital, education, and networking.

## C. Foundational investments in women

Make foundational investments that support women's ability to use digital payments

### Consciously increase the accessibility and affordability of digital payments

- Invest in infrastructure and supply chains for ID cards, mobile phones, network access, and other important enablers of digital financial inclusion.
- Undertake investments rooted in global best practices that specifically benefit and incentivize women's access and use, such as reducing transaction costs by promoting interoperability (given greater affordability challenges) and setting up more physical CICO points (given preference for in-person touchpoints).

### Invest in the skills women need to easily access and use DFS

- Advocate for and invest in education for girls and women, covering the basic elements of numeracy and literacy, how to engage with financial products, and how to employ digital tools.

## D. Women's seat at the table

Create space for women to inform and influence decision-making

- Ensure women have a voice in leadership positions to influence and inform the design, implementation, and iterations of digital payment products, policies, and programs.
- Include key stakeholder groups and voices of marginalized women to help ensure responses are locally appropriate.

**Kenya's Matrimonial Property Act 2013**[67]

The revised Property Act amended the original 1882 legislation, making married women's rights equal to those of their husbands (e.g., by reducing dependence for entering contracts for receipt of financial services).

Women are now empowered to own or co-own property, with property ownership recalculated based on contribution from each spouse.

© Shutterstock

## E. Women-centric offerings and communication

Design and market products for women

### Build organizational cultures that prioritize women

- Build gender-intentionality into the entire value chain by committing to use a gender lens, sensitizing staff to its importance in both the workplace and marketplace, and empowering local champions to anchor these initiatives.

### Tailor design of the offering to women's diverse realities in the target market

- Treat women like other priority segments by adjusting to their preferences for purpose and frequency of use (e.g., by aligning service hours to women's time constraints and schedules).
- Apply an intersectional lens to understand diversity among women (e.g., age, marital/parental status, income, geography, and disability).
- Design products with features that address the sociocultural and economic factors preventing women's access.
- Account for the unintended consequences of women-centric product design (e.g., directly interfacing with a woman can result in backlash by other household members). This can be managed through agent sensitivity training and engaging men in the communities. More broadly, design needs to be mindful of household dynamics.

### Market to women appropriately

- Leverage sales models attuned to structural barriers (e.g., using home-based consultations with women service agents to offset mobility constraints and low financial capability).

**Women's Micro Bank Limited Papua New Guinea**[68]

A 65 percent increase in women's customer base was credited to leadership support of "Women In Business PNG" and other women's groups supporting education efforts on the product.

**HUL Shakti India program**[69]

Ensures that bank accounts opened by women entrepreneurs (Shakti) are in their own names.

Simplifies onboarding with door-step document collection.

Plans to tailor incentives to women's needs and willingness to adapt to digital systems, with customized incentives to those more reluctant.

**Diamond Bank Nigeria agents**[70]

Savings accounts are created in under 5 minutes via a mobile app and require minimal documentation, reducing barriers.

Agents visit women's businesses to help open the account and initiate transactions, navigating low mobility challenges.

CASE STUDY

# Supported by Gap

## The Amader Kotha is a helpline for garment workers around digital wage payments

© Marcel Crozet / Better Work

**Amader Kotha was established in 2014 as a national helpline** to help Bangladeshi garment workers (85 percent women) report and resolve wage, safety, and other concerns. Since inception, it has served 1.5 million workers with a 99 percent success rate in resolving issues. In 2020, the government mandated digital wage payments in response to the COVID-19 lockdown and expanded the scope of this helpline to cover recourse on these factory wages as well. While still in its early stages, its success is the result of an intentional design approach to addressing women's needs, forging complex but powerful partnerships early on, and pioneering the use of sex-disaggregated data.

### Notable features

#### Gender-disaggregated data

- Tracked caller data by gender, a challenging task given men in the household often called on behalf of women. Helpline officers were trained to identify such occurrences and to persuade callers to allow women to report their concerns directly.
- Collected data on multiple gender-disaggregated metrics, including the percentage of women comfortable with digital payments and their preferred mode of recourse.

#### Women-centric offerings and communication

- Designed FAQs[71] for the helpline centered on the basics of cash withdrawal, given that women often have less experience in using digital payments and ATMs.
- Largely staffed the helpline with women officers to increase comfort among women callers.

#### Foundational investments

Beyond digital payments, Amader Kotha strives to enhance women's work experience via plans for:

- childcare support by partnering with brands to create functional daycare facilities inside factories
- health and hygiene support through supply of sanitary pads to factories and communities.

### Implementation journey

#### 1. Flexible partnership-building

- Initial plans to develop a new independent recourse mechanism in the wake of COVID-19 were driven in partnership between the Better Than Cash Alliance; a2i, the government's innovation unit; and BMGEA, the national garments export association, whose experience was critical in understanding the requirements of women garment workers.
- Following stakeholder buy-in challenges, there was a reorientation to instead partner with Amader Kotha, whose reach among garment workers and experience in operating a helpline was key in ensuring wide outreach and creating an efficient model.

### 2. Assessment of women's needs and preferences

- Harnessed decades-long experience of partners like Microfinance Opportunities (MFO), a2i, and the Alliance with garment workers in Bangladesh to understand the key constraints faced by women workers in digital environments. This knowledge was critical for drafting relevant FAQs used for training helpline officers.
- Referenced findings from focus groups with more than 500 women and surveys of 1,300 workers conducted by MFO to understand behavioral patterns (e.g., women workers preferred speaking with women helpline officers, women workers' low confidence with digital transactions led to lower frequency of use).

### 3. Outreach and design of recourse mechanism centering on women

- Conducted outreach through mobile phones by sending voice messages to existing database of past helpline callers.
- To prevent selection bias, phone outreach urged women to leverage their strong P2P networks and to share recourse mechanism details with colleagues.
- Planned outreach through television, radio, and public-announcement (PA) systems in factories did not materialize because of lack of resources after the withdrawal by BMGEA, and low turnout on factory floors as a result of the COVID-19 lockdown.

### 4. Plans to enhance women's digital and financial independence

- Assessed success holistically. Wage digitization efforts were successful in that women and men accessed their funds at the same rates. Data suggested that more women required help doing so and were unable to access funds independently.
- Developed new priorities to tackle these barriers to women's financial resilience and digital independence, including improving recourse quality by training helpline officers on supporting women callers' independence, and supporting women's financial and digital capabilities with systematic education.

### KEY LEARNINGS

**Establish connection with all key stakeholders in the digital money value chain.** Amader Kotha was able to resolve user issues related to delays or non-payment of wages because of its direct contact with factory owners.

**Tracking gender-disaggregated data can inform implementation and decision-making.** Amader Kotha recognized the difficulties women face in accessing funds independently via their gender-disaggregated data and prioritized women's digital empowerment in upcoming programming.

**Being gender-intentional often means going beyond the obvious scope of work.** Amader Kotha made plans to facilitate childcare and sanitary pad supply given the critical barriers they place on women workers, even though these are not directly related to wage payments recourse.

## KEY CHALLENGES

**Unforeseen gender bias in mode of outreach.** Voice messages via mobile phones were the primary mode of outreach to users. However, phones in workers' households were largely handled by men, making it difficult to effectively reach women workers.

**Overcoming gender barriers, unsurprisingly, requires persistence and innovation.** Continuous learning through disaggregated data is critical to identifying issues and tailoring future actions. While most women garment workers owned a phone, gender-disaggregation of call data showed that many were hesitant to call the helpline directly and preferred informal means of support such as through family or friends. Amader Kotha has accordingly emphasized relationship-based messaging in its outreach.

© Marks & Spencer

# Recommendations

**Recognize the critical role of women** in the next billion users and prioritize them accordingly.

All members have an opportunity to **use their partnership agreements to prioritize women**, such as:

- set gender-disaggregated outreach targets
- set conditions demanding preference for women staff and agents
- selection criteria requiring strong, demonstrable experience in women-centric services.

All members can prioritize women by **tracking gender-disaggregated data** from digital payment partners and ensure a focus in all prospective research for emergent technology such as AI.

All members have the opportunity to structure partnerships that support digital payments and **create economic opportunities for women**.

All members can create partnerships to **explore innovative solutions to women's unequal access** to connectivity, identity, and digital and financial literacy.

# Recommendations

| For **GOVERNMENTS** | For **COMPANIES** | For **INTERNATIONAL ORGs** |
|---|---|---|
| **Governments can lead by example through digitizing government payments, many of which have women as beneficiaries.** | **Companies can set organizational key performance indicators to prioritize women, such as measuring women staff and the organization's board.** | **IDOs can provide technical and financial support on gender-focused financial product design and communications by working closely with providers.** |
| **Governments can enact policies that incentivize women's access to financial services, and include laws on ownership of property and bank accounts that prohibit discrimination.** | | **IDOs can provide funding and technical assistance for tools that collect and analyze sex-disaggregated data as an input to product and policy design.** |
| **Governments can empower women to take control of their data and make informed choices by including their voices, including working with civil society and community groups that are trusted, in national approaches to safeguard data.** | | |

PRINCIPLE

# 4 Safeguard client data

**The growth of digital payments is generating data** in unprecedented volumes. This creates opportunities and risks for companies, governments, and international organizations. More data mean more and better insights to inform design. This phenomenon accelerates both service adoption and, by extension, financial inclusion among the underserved.

**The counterpoint, as data flow in ever greater quantities through ever more institutions, is increased opportunity for misuse. It is this risk that supercharges the conversations surrounding data ownership, consent, and bias.**

Preventing misuse of data is fundamental to developing excluded users' trust in digital payments. Most existing data protection and privacy compliance models anchor on consent. However, users often do not understand what they are agreeing to, rendering consent meaningless. Furthermore, users often lack the tools needed to manage usage of their data (the "legitimate purpose" idea, which often drifts beyond the scope of consent) or hold providers accountable for its protection.

Remedies are being formulated, and there are a number of policies being designed to address this issue. The European Union's General Data Protection Regulation (GDPR) is a salient example, as are Ghana's Data Protection Commission, and California's California Consumer Privacy Act.

**Preventing misuse of data is fundamental to developing excluded users' trust in digital payments**

One trend is obvious: onus is increasingly being placed on providers. It is now vital that data controllers[72] empower users as guardians of their personal information. This ownership must be protected by policies that guarantee users' basic rights. Beyond this, there remains an enormous opportunity to move beyond checklists to a world in which all actors take responsibility. This opportunity requires changes in deeply rooted behaviors to cultivate the trust of the most marginalized – many of whom now view their personal data as a valuable commodity.

Indeed, users are increasingly aware of the risks of data misuse. People are consciously seeking services that protect against malicious use of personal data. In a 2017 ethnographic study of Indian consumers, users overwhelmingly valued guaranteed security and fair data use over other benefits. The failure by a service provider to offer these protections also meant many users would avoid that provider entirely.[73] Conversely, when products and services are proactively designed with user privacy in mind – specifically, privacy by design – this builds trust.

**Replacing today's flawed model of consent with a culture of user control and data stewardship will only increase this trust. Doing so alleviates three key concerns.**

### 1. Consent models are irrelevant when rights of ownership are neither understood nor exercised.

End-users lack the information and means to provide explicit, informed consent. This is often driven by low literacy, limited technical capabilities and poor network connectivity. The terms of consent are often concealed behind complex disclosures.[74] Concurrently, physical access constraints and a lack of transparency leave users unaware not only of what data are being used but also how and by whom. In fact, they are often unaware of their rights and of the resources that exist to help them take control of their data. A survey of South African consumers found that approximately 60 percent were not aware of their rights to data ownership, let alone how to exercise those rights.[75] This lack of control, compounded by a natural desire for privacy, can push users further away from adopting digital financial solutions.

### 2. Data drift to unspecified purposes unbeknown to users.

Digital payments are increasingly low-cost or free. Like many other digital services, data have become a valuable currency to support businesses. Digital payments data not only reveal valuable intelligence about users' creditworthiness, but also demonstrate spending behaviors and preferences that can become a compelling monetization opportunity. However, this also introduces the risk of "drifting" consent, where service providers push the boundaries of consensual data use in purposes to which the user did not explicitly agree. In a survey of Rwanda's online government services portal, approximately 50 percent of respondents felt that they had received either no information or ambiguous information surrounding how their data would be shared with third parties. They felt the same about whether they would be approached for consent before their data were shared.[76] Service providers, hidden behind complex internal policies and consent disclosures, exploit these ambiguities by co-opting or sharing user data for purposes that may not serve the user's best interests. Meanwhile, users are left without visibility or control.

### 3. Without regulation, few providers invest in data protection, exposing users to risk.

Regulations and policies governing the use and protection of data are often either limited in scope, nonexistent, or weakly enforced. While there is momentum to address these issues, only 66 percent of countries have adopted data protection and privacy legislation. In developing nations, this figure falls to 43 percent, many of which lack the resources to effectively enforce these frameworks.[77] Coupled with poor end-user awareness, there are few incentives for service providers to proactively invest in data protection. As a result, users are exposed to risks such as identity theft, fraud, and financial loss. A Consultative Group to Assist the Poor (CGAP) study found that 83 percent of surveyed mobile money users in the Philippines had reported fraud or scams via SMS messaging, with approximately 17 percent having lost money as a result.[78] The stakes are heightened for at-risk and excluded populations, who are not only at greater risk of discrimination via biased algorithms, profiling, and aggressive marketing, but also have less access to recourse. When users suffer financial loss in this way, they often blame themselves for giving away their data.[79] Thus, confidence in formal financial services is undermined and they are impelled towards riskier sources of informal finance.

**83% of surveyed mobile money users in the Philippines reported fraud or scams via SMS messaging, with approximately 17% having lost money as a result**

#### Behavioral science and privacy[80]

Behavioral science specialists, the Centre for Social and Behavior Change (CSBC), Ashoka University, and Busara Center for Behavioral Economics assessed whether end-users can be nudged to be more privacy-conscious, and whether better privacy practices provide a business advantage. The experiments looked at the privacy paradox that exists among users - users want to safeguard their privacy, but do not follow through in action.

**They found that:**

- users are not always capable immediately of making the right choices for themselves
- businesses are not always incentivized to put privacy first.

**The study recommended that:**

- meaningful change in the data privacy environment can be brought about by better regulation and integrating privacy features into the platform design itself.

# How can data be stewarded effectively?

Accountability is the bedrock of data privacy. On that foundation, providers must ensure that user data are only ever legitimately used and shared. Assuming this occurs, users will control how their data are accessed.

## A. User control

Legitimate purpose

### Give end-users the tools to understand and direct how their data can be accessed – equip end-users with control of who is using their data and why

- Provide multiple platforms for users to understand and manage consent so that those with lower literacy and tech access can do so independently. For unbanked customers, supplement these communications with high-touch engagement to build confidence and trust.
- Provide users flexible access to and ownership of their data after they provide consent, thereby respecting users' rights to revoke access.[81] This approach also means taking reasonable measures to ensure that third parties respect these rights and revocations.
- Ask for user consent and data on a "just in time" basis and issue a request every time these are required rather than at the time of registration. This approach enables users to express their preferences as opportunities evolve. Ensure that users are informed of the privacy implications of a particular action at each juncture.

### Reduce users' cognitive burden by highlighting key points

- Help users navigate legalese by prioritizing key elements of consent, including what is collected, explicit purpose(s), duration, parties with access, and channels to change and/or revoke consent.
- Seek consent explicitly and distinguishably,[82] using plain, local language and alternate formats that aid understanding (e.g., pictorial summaries, video consent, or phone calls).

## B. Legitimate purpose

Use gathered data legitimately

### Prioritize users' best interests when assembling use cases for data

- Ensure that uses of data (including data-sharing) are undertaken within the boundaries of the law and with the explicit, informed consent of users.[83] Clearly communicate how these uses will deliver explicit benefits or risks.
- Explore safe options to democratize financial service providers' access to anonymized data to enable better marketing and product designs that benefit the excluded.
- Ensure proposed uses are communicated to the user in a tailored way.

**India's Electronic Consent Framework**[84]

Account aggregators (AAs) are for-profit intermediaries created and supported by the Reserve Bank of India to facilitate the flow of data between customers and users of their financial information.

AAs are "data blind" and cannot view, store, use, or modify user data. They release user data only if the user has provided electronic consent for the purpose requested.

Uses a smartphone front end that includes a streamlined registration that simplifies legalese and integrates with other mobile money platforms, reducing both the cognitive burden on, and the number of steps needed to provide consent for, the user.

### Develop clear processes to guide internal data use and sharing

- Minimize collection of identifiers and other sensitive information (e.g. by collecting only relevant and necessary data to fulfil the services for which the user consented).
- Develop internal policies that set clear protocols for sharing data with other internal departments and third parties (e.g., what approvals to seek, from whom, when and how to seek consent). Disallow the sharing of large data sets to protect individual records.
- Build traceability into data-sharing processes, providing an immediate and transparent view of when, why, and with whom a particular user's data were shared.
- Train staff and relevant partners to ensure a common understanding of internal data use and sharing policies, but also universal recognition of their importance.

#### Unilever's Shakti programme[85]

The smartphone app of Unilever's Shakti program, which equips women as last-mile distributors of Unilever products in 10 countries around the world, collects sensitive data such as GPS location and real-time density mapping.

The app uses these data to support the viability of Shakti entrepreneurs' (SEs) businesses; for example, location data are used to optimize inventories.

Unilever's corporate compliance team applies strong regulatory oversight, ensuring that each new use case is captured, processed, and used in line with regional e-commerce and data privacy laws.

As the Shakti program builds on its proof of concept, data can be used for other purposes that benefit SEs (e.g., for building credit history and facilitating easier access to finance).

#### India's Unified Payments Interface[86]

India's Unified Payments Interface (UPI) collects only the minimum amount of data (e.g., no sensitive data on location) required to transact.

The platform also proactively specifies that participating payment service providers must rigorously protect user data (e.g., using encrypted channels, scrambling stored passwords).

#### Mexico's Data Analytics Tool[87]

Mexico's National Banking and Securities Commission (CNBV) engineered a storage platform that receives and houses transactional data from financial service providers. Data are automatically submitted via API.

The tool allows CNBV to compare current data against historical records, using machine learning to validate data and flag suspicious trends.

The platform renders transaction data in risk dashboards, alerts, and other reports to target on-site visits and spot checks.

### C. Accountability

Design with privacy in mind and enforce accountability

#### Embed data protection and privacy in product and system design

- Ensure privacy is central to the design of technology architecture (e.g., using data encryption and authentication protocols to restrict access, ensuring data are appropriately masked/anonymized before being stored) to prevent transmission to non-compliant systems and to obfuscate if hacked. Regularly auditing processes and policies, and testing for vulnerabilities and biases is also critical.
- Build privacy communication and user touchpoints across the consumer journey, such as training sales teams and redressal operators.
- Build in security measures by storing only critical data, using opt-in defaults, planning for destruction of data after their purposes have been served, and business continuity planning to minimize system weaknesses.
- In event of a data breach, disclose information to all users and make recourse available to those affected.

#### Empower regulators with independent oversight of data for digital payments

- At a government and policy maker level, identify independent bodies and entrust them with oversight for each segment of the ecosystem.
- Enforce liability for data breaches onto each party engaged in the flow of misused data.
- Provide oversight bodies with legal access to transaction data concerning a country's citizens, regardless of origin or storage.

#### Privacy enhancing technologies (PETs) for financial services

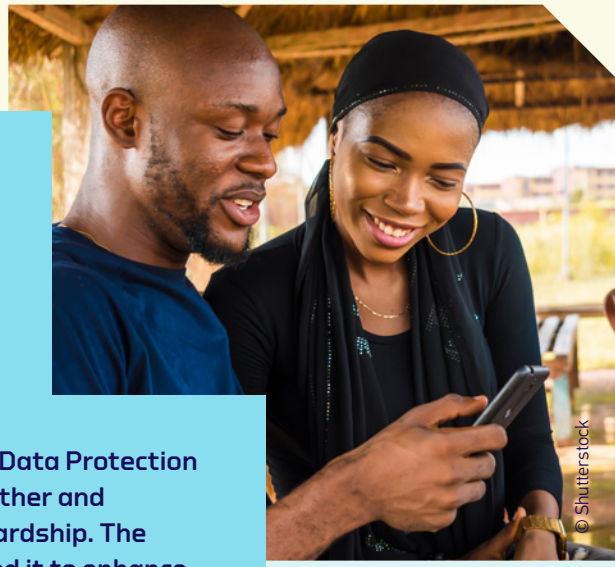
**1. Differential privacy:** techniques using approximation to protect individuals' privacy while maintaining the validity of aggregated data. This ranges from adding random noise to data, to the more complicated creation of synthetic data. All techniques anonymize the individual. Differential privacy has been used in the US 2020 Census, Windows 10 usage data collection, and Google's software usage data collection. Startups such as Hazy and Privitar, and academia (Harvard's privacy tools project) provide tools for implementing differential privacy.

**2. Zero-knowledge proofs:** this technology verifies the identity of a customer or transaction without sharing private information. Merchants can authenticate credit card validity without the credit card number or CVV. Banks can ensure that net banking is being used privately. As no sensitive information is shared, it reduces risk if a merchant site is hacked. Startups such as Zcash are deploying this in the digital currency sphere. Larger implementations include ING's Notary service, which mixes it with blockchain.

**3. Secure multi-party computation/federated learning:** FSPs often collaborate on data-driven projects but cannot share data with each other. Federated computation and learning systems allow for decentralized processing with the data-owner sharing the results. Applications include machine learning models for improving fraud detection tools. This can also be used to decentralize credit scoring. Startups including Inpher and larger firms (NEC) provide secure multi-party computation services. Intel is using machine learning tools for fraud identification. WeBank is using this for credit scoring, working with data from China's National Invoice Centre.

**4. Homomorphic encryption:** facilitates computation on encrypted data, thus protecting privacy. FSPs can process sensitive financial information for credit scoring without accessing raw data. This technology is nascent, with limited commercial implementation. IBM has run pilot implementations in the finance sector and Microsoft has been developing tools and standards for its usage.

CASE STUDY



© Shutterstock

# Ghana's Data Protection Commission

## A multi-stakeholder body guiding Ghana's data protection journey[88]

**As the standard-bearer of Ghana's Data Protection Act 2012,** the Data Protection Commission (DPC) is responsible for regulating how organizations gather and process user data while articulating the business case for data stewardship. The commission's strong policy and institutional foundations have enabled it to enhance its service as a regulator and as an anchor for Ghana's growing privacy community.

Today, the commission has registered and monitors roughly 700 entities across Ghana, including businesses and government agencies. Its growing team of 200 full-time staff – most of whom are embedded in other public and private sector organizations – monitor and provide guidance to entities that set the purpose for data use. These entities include banks (data controllers) and those that process data, such as PSPs. More recently, the commission has taken a leading role in shaping policy in Africa and provides support to other countries in the early stages of data stewardship, such as Ethiopia, Gambia, and Namibia. As the commission is relatively new – and adapting in a fast-moving space – its effectiveness will become clear in the coming years.

### Notable features

#### User control

- Advocates for redesigning consent disclosures to reduce cognitive burden on marginalized groups.
- Conducts awareness campaigns to educate the public of their rights to data ownership.
- Legitimate purpose.
- Any entity that handles personal data must register with the commission in advance, clearly evidencing legitimate grounds for use.
- Makes resources and training available to data controllers and processors seeking guidance on responsible data use and sharing.

#### Accountability

- Requires its approximately 700 registered data controllers and processors to submit regular compliance reports, enabling oversight.
- The commission can hold service providers accountable for data usage and enforces noncompliance penalties ranging from fines to imprisonment.

### Laying down a strong regulatory foundation

- Crafted rights-based data protection legislation governing data processors (including banks and PSPs).
- In doing so, Ghana drew heavily on the EU's Data Protection Directive and General Data Protection Regulation (GDPR).
- Tailored policy for Ghana's unique context. For example, to navigate low literacy, Ghana's policy requires the data processor not only to obtain explicit consent for data use, but also to guarantee legitimate grounds for use. Data processors must also register with the commission to legally collect data.

## Implementation journey

### 1. Creating and strengthening institutional mechanisms

- Formally operationalized the commission as an independent institution to provide oversight and guidance to the sector.
- Partnered with government agencies, such as the Ministry of Communications, to expand reach of public awareness.
- Hired leaders with deep global expertise to catalyze internal capacity development. Developed a training manual anchored in GDPR standards to align about 200 staff to global skill sets and best practices, enabling them to more effectively monitor and steer data processors toward data stewardship.

### 2. Guiding, supporting, and regulating responsible use of data

- Built the capacity of financial data processors on data stewardship using publicly available resources and training, which included certifications for aspiring data protection officers.
- Compartmentalized compliance functions within a new Technology and Ethics Department responsible for licensing data processors based on their proven ability to handle personal data, prove legitimate use of data, etc.
- Solicited regular "state of play" reports from registered entities for compliance monitoring and renewals of licenses for both new organizations and organizations predating the commission.

### 3. Sustaining and scaling data stewardship in Ghana and beyond

- Pursued cross-learning opportunities with other African governments (e.g., Kenya), private sector players, and IDOs to refine the processes supporting Ghana's legislations.
- Offered thought leadership and guidance to African countries with earlier-stage data protection policies, with the goal of creating a unified framework for data protection that facilitates safe cross-border remittances between African states.

## KEY LEARNINGS

**Do not reinvent the wheel.** Ghana's policies lean heavily on existing landmark regulations but have been moderately customized to meet Ghanaian needs.

**Cultivate internal technical expertise.** Early on, mismatched technical skills meant the DPC's staff were unable to effectively monitor and engage with processors. Hiring a commissioner with deep subject matter expertise was a catalyst for developing a standardized training manual, enabling the commission to train nearly 200 staff over 3 years.

**Build a community of privacy practitioners.** The DPC comprises stakeholders from government and industry and has used its position to convene across sectors. In doing so, the DPC disseminates best practices and helps resolve processors' implementation challenges.

## KEY CHALLENGES

**Limited resources, capacity, and funding have hampered the DPC's ability to scale internal capabilities for outreach and proactive oversight** (e.g., spot checks and audits). These constraints also limit the investments the DPC can make in technologies that increase the coverage and cost-effectiveness of compliance monitoring.

**A fragmented ecosystem of financial data processors hampers regulation of personal data use.** Larger FSPs are typically registered by the DPC and have systems in place to steward user data. Smaller processors are difficult to register and regulate.

**Lack of universal digital ID means that the personal data collected by FSPs are not standardized.** Discussions on the component data for a digital ID program are underway.

© Better Than Cash Alliance

Safeguard client data

# Recommendations

Members can **include clauses in their service-level agreements** with digital payments partners that ensure that users' digital payments data are protected against misuse.

Members can **commission behavioral research on user privacy** to understand how to make individuals more privacy-conscious as part of their emerging digital rights. Actions include:

- members engaging directly or through trusted local groups with first-time users, crafting consent disclosures, and informing users of their rights and how to exercise them
- members testing the privacy of payment products from the perspective of at-risk segments. This may involve removing quick balance view to protect the privacy of women using shared devices in their households
- ensuring transparency on personal data usage by making audit trail data available to regulators and end-users while ensuring that personal information is protected.

Members can protect users' data privacy rights and consent by **supporting local-level community groups and civil society** to play an active role as stewards.

# Recommendations

## For **GOVERNMENTS**

**Governments can enable institutions to set standards on data protection.**

**Governments can refer to privacy libraries that track privacy jurisprudence globally and are designed to help actors learn from each other as data governance models evolve.**

**Governments can enforce responsibility via oversight committees comprising chief regulators, industry experts, and thought leaders.**

**Governments can rank payment partners' compliance against metrics for data consent, sharing, and storage. These rankings can be aggregated from user experiences and curated by independent regulators.**

## For **INTERNATIONAL ORGs**

**IDOs can assist regulators in shaping regulatory frameworks and ensure they remain responsible as new technologies emerge.**

PRINCIPLE

# 5 Design for individuals

**Advancements in data analytics are helping to shape a future** where user experiences are personalized irrespective of wallet depth. An enormous opportunity now beckons. As digital payments proliferate, user-centric design becomes a critical determinant of success.

**Even now, development organizations are calling for product design standards in emerging markets.[89] Startups and large firms alike are investing deeply in building competencies around prototyping, segmentation, and market feedback.[90] Some governments recognize the limits of the market and have issued regulations mandating consideration of user needs and capabilities in financial product design.[91]**

While these investments in design have improved the payment value proposition for some users, many remain excluded from providers' target markets. Financial inclusion is no longer simply an issue of access, it is also a question of delivering relevant, quality product choices to those who remain excluded.[92] This underscores the pressing importance of research, design, new stakeholders, and iteration.

Further transformations are on the horizon. Advancements in data and analytics have the power to unearth much deeper insight into the ways individuals engage with digital payments in their diverse societal roles. This insight will inform the design of bespoke products, tailored to meet known needs.

Data will inevitably shape the nature of design because, used in this way, data can confer a competitive advantage when used responsibly to empower user's ownership and consent.

Indeed, during the past decade, reams of research have surfaced with insights intended to improve the user-centricity of product design. However, digital payments remain primarily designed for the average user rather than those on the margins. The barriers that hold marginalized populations back are widely documented, from low capabilities to lack of access to key infrastructure (e.g., mobile phones). Still, in 2017, the proportion of women internet users was 12 percent lower than men and 33 percent lower in the least developed countries.[93] Despite stakeholder awareness of these design challenges, financial inclusion in low-income markets remains elusive. Nearly one third of adults worldwide, especially among marginalized groups, are still unbanked.[94] To provide services that are better than cash to all users, digital payments design must move to meet people where they are.

Three dynamics define this challenge.

### 1. Billions of people worldwide remain underserved by mainstream digital payments products.

The challenge in accessing and retaining marginalized users is that many are yet to experience sufficient value from digital payments. Many providers simply roll out pared-down versions of their "mainstream" products to low-income markets, addressing affordability concerns but investing little to assess the nuances of how low-income users transact with and use the products. Insufficient private sector oversight has prompted regulators in some markets to push for more proactive design and distribution requirements through policy and product intervention powers.[95] Where traditional banking systems have failed to sufficiently adapt, digital payments may be able to accelerate financial inclusion. GoPay and other e-wallets have propelled millions of previously unbanked users in Indonesia to open bank accounts by virtue of their ease of use.[96] While digital technologies can be daunting for new users,

if designed thoughtfully, payment products' use of adaptable digital interfaces and wide agent networks that offer local assistance serve as stepping-stones to financial inclusion.

### 2. Many providers fail to tailor their products to the diversity within excluded markets.

An even deeper roadblock to digital payments penetration – and indeed to financial inclusion at large – is that low-income users are often treated as a uniform mass, with little appreciation for heterogeneity. Traditional segmentation of low-income markets typically relies on well-worn contextual and demographic categories (e.g., smallholder farmer, migrant laborer, gig worker, loan group participant). However, this segmentation masks wide and vibrant diversity in people's aspirations, behaviors, and psychology.[97] Differences in how two individual migrant workers feel about and transact with money, as well as how they use technology, consume information, plan and track their finances, can have significant ramifications for which payment products best suit them. These differences extend beyond any context they share as migrants. More nuanced segmentation and human-centered market research remain key, while technological advancements in data analytics are opening a window to harness this diversity.

### 3. Advances in technology offer novel opportunities for tailored design but come with new risks.

The need for designs to focus on excluded populations is not new. What is new are the tools available to realize this need. The massive expansion in big data analytics, artificial intelligence, and machine learning tools to mine for trends and personalize products is bringing tailored experiences within reach. Equipped with data from digital payments platforms and linked social media, telecoms, and geospatial inputs, providers can cater to an individual user's behavioral and psychological traits.

One example is the use of natural language processing to improve recourse by providing conversational, personalized support via chatbots and robo-advisors.[98] However, this opportunity opens a Pandora's box of potential privacy breaches, data security, and discrimination that we are only beginning to understand. The true litmus test is the digital payments ecosystem's ability to bring the best of these innovations to design, while also enabling consent and control throughout the user experience.

**Data will inevitably shape the nature of design**
**because data can confer a competitive advantage when used responsibly to empower user's ownership and consent**

# What constitutes successful designs for users?

To create a world where digital payments enhance everyone's livelihoods, a deep understanding of users' needs, preferences, and capabilities is essential. Stakeholders should endeavor to design not just products, but end-to-end experiences for digital payments. Doing so is a continuous process, requiring cultural shifts and investments in analysis, learning, and adaptation.

## A. Inclusive and deep understanding

Scrutinize marginalized groups and use technology to understand their behaviors, preferences, and capabilities

### Proactively include vulnerable and excluded populations in customer targeting

- Establish a baseline to better understand who is – and is not – being served today.
- Providers and designers should work with civil society representatives of vulnerable groups – for example, disability rights NGOs to deepen the understanding of needs and challenges.

### Leverage consumer data to identify demographic patterns in the consumer base and those being underserved (e.g., analytics on gender-disaggregated user data can be used to track inequities in aspects such as complaints resolution and user satisfaction)

- Define target markets and customer acquisition goals that are inclusive of "outlier" users who face unique barriers to uptake, such as people with disabilities, displaced communities, and women.
- Invest to achieve success (e.g., wide network of agents, including those who serve these communities and may face their own access barriers).

**Mexico's voluntary contributions to retirement savings**[99]

Used behavioral science to identify barriers, designing and testing interventions to encourage voluntary retirement savings via digital payments.

For example, randomized control trials conducted on sample populations showed that text messages and physical letters reminding individuals to save increased voluntary contributions by 54 percent.

### Leverage technology to deepen comprehension of user needs, preferences, and capabilities

- Seek quantitative trends from big data analytics to identify patterns in behavior and psychology that shed light on target market needs and capabilities. It is important to anchor data analysis in consent and anonymization to protect user privacy.
- Identify the "why" behind quantitative trends by investigating user preferences with ethnographic, anthropocentric research. Areas to investigate could include: modes of communication users trust, triggers that could nudge them to try new products (e.g., peer referrals), pressing needs and aspirations digital payments could solve, features they find useful (e.g., receipts), habits and routines that are important for products to fit within (e.g., income patterns), and how they like to receive support (e.g., open accounts within women's groups).[100]
- Assess users' capabilities – not limited to language, literacy, numeracy, financial skills, or physical capabilities, but also their access to prerequisites such as IDs or mobile phones. Seek user voices on how to address these constraints.

## B. Experiential design

Serve users with experiences - not product

### Meet users where they are in each aspect of the front-end user experience

- Build digital payments products that leverage user insights to create a new value proposition that exceeds that of cash – by way of ease, speed, safety, control, and transparency.
- Design interfaces that are intuitive for all, regardless of user capability.[101] Emphasize features such as local languages, clear content, visual cues, minimal clicks to access key services, notifications for transaction trails, autofill options per user history, auto-check mechanisms,[102] and safety announcements.
- Develop processes that meet users' goals across the experience journey, from outreach to onboarding, transacting, agent engagement, upselling and incentives, and recourse. For example, information on why a user wishes to transact can help ensure payment processes are designed with that user's financial end-goals in mind.[103]
- Offer teachable moments to help first-time or marginalized users overcome trust and capability barriers. Invest in user training that includes in-person touchpoints to serve users' preferences for peer-to-peer support, enabling them to retain knowledge.

**Lebanon's women-centric banking services**[104]

Conducted market research to identify gender gaps in service delivery.

Found many women were distrustful of banks and wanted more personalized support.

Designed a host of financial and non-financial services tailored to women's needs - collateral-free loans, online banking platform, mentoring/networking platforms - which increased the number of women borrowers by 82 percent between 2011 and 2015.

**Kenya's Inua Jamii G2P cash transfer program**[105]

Distributed biometric-enabled debit cards to beneficiaries after discovering user concerns about convenience and safety on PIN-enabled cards. Retained the option of PIN-enabled safety for those unwilling or unable to use biometrics.

Allowed caregivers or representatives of minors and disabled users facing barriers to register their biometrics on the user's behalf.

### Build in user-centricity and ensure all partners do the same

- Create the back-end systems and foundational infrastructure for a seamless user experience, including strong networks for reliable transacting, interoperable systems to provide flexibility across platforms, and effective, disaggregated and secure data collection and analysis.
- Direct intermediaries to keep user interests central. Select, train, set contract terms, and institute incentives and oversight measures that push agents, merchants, and other third parties to serve users' capabilities, financial conditions, and risk appetites. For example, recommend only products and services that suit users' actual needs.[106]
- Institutionalize user-centricity by taking ownership. Do not delegate to a single champion or to providers alone. Payers can leverage their proprietary data (with appropriate consent and anonymization) to collaborate with providers on service tailoring.[107]

## C. Learning and iteration

Always build in user voices

### Co-create the digital payment experience directly with users

- Bring user voices into design processes through human-centered design research, focus group discussions, and insights from agents or third parties.
- Invest in prototyping, feedback mechanisms, and piloting to gauge the impact of new features on the entire spectrum of users. Design alternative solutions when standard features are insufficient to meet outlier usage circumstances.[108]

### Learn from and adapt to changing needs

- Leverage insights from both "small" and "big" data, including disaggregating by key demographics (e.g., gender) to track progress in reaching underserved segments. Leverage real-time analytics of user behavior to adapt and refine user experiences.
- Establish sufficient controls and consent mechanisms for users to manage the trade-off between privacy and personalization.

**Peru COVID-19 relief transfers**[109]

Gathered feedback and tracked user behavior in the first iterations of welfare transfers.

Incorporated digital forms of fund transfer through mobile banking apps and mobile wallets in the second iteration of payments based on user feedback.

CASE STUDY

© Better Than Cash Alliance

# EjoHeza

## Long-term retirement savings scheme by the Government of Rwanda[110]

**In 2017, The Rwanda Social Security Board established its long-term savings scheme, EjoHeza**, to extend the protection of post-retirement pension benefits to all Rwandans, regardless of the nature of their livelihoods. The program enables even informal, non-salaried workers to contribute digitally to a national ID-linked pension account over the course of their working years. Within a year and a half, more than half a million Rwandans (10 percent of all informal workers) opened digital accounts. This uptake is attributable to the program's deep assessment and design based on user needs, together with a simple and fully digital user interface, strong community partnerships driving sign-ups and ongoing feedback and iteration.

### Notable features

#### Inclusive and deep understanding

- Learned via behavioral research that prospective users were accustomed to relying on easily available (but expansive) informal lenders, rather than on accumulated savings, and would require economic incentives (e.g., matching funds) to change attitudes.
- Used demand assessments to quantify users' high access to national IDs, mobile, and internet, justifying rollout of a digital payments solution for pension savings.

#### End-to-end experience design

- Developed simple onboarding process for users to open an account within 90 seconds using a USSD call from a feature phone.
- Allowed variable frequency in account contributions to cater to different earning formats (e.g., annually for farmers at harvest or daily for casual laborers) and income volatility.
- Created provisions for early no-cost withdrawal of up to 40 percent of accumulated savings preretirement for critical use cases: tuition, residence construction, loan collateral.

#### Continuous learning and iteration

- User feedback showed that ease in account set up led some users to do so without fully understanding its long-term nature and illiquidity. To overcome this, a callback feature was instituted to confirm new users' understanding of the scheme and commitment to long-term savings, which allowed instant closure of new accounts without penalty.

## Implementation journey

### 1. Acknowledgement of need for voluntary contribution scheme

- Noting Rwanda's demographic trends, the Finance Ministry forecasted a shortfall of funds and systems to provide sufficient financial support to people age 60+ by 2050.
- Revealed the low pension coverage (5–6 percent) which was available to only a minority of formal salaried workers. Meanwhile, the majority of Rwandans in the informal sector lacked options to sustain themselves after retirement, including farmers, wage laborers and street vendors.
- The Ministry led the charge to make pension savings a political priority, instituting a partnership with pinBox Solutions to replicate and expand their work in India.

### 2. In-depth demand and supply-side research

- Conducted demand assessments on access, behavior and attitudes toward saving to inform product design and policy. For example, lack of insurance was identified as a driver of both pension demand and scheme dropouts. To address this, the government paid life insurance premiums for users for 3 years, retaining participation, helping subscribers maintain savings, and demonstrating the insurance value proposition.
- Engaged deeply with the national ID system, social security board, digital payments firms, fund managers, insurers, and the central bank to ascertain feasibility of a national voluntary pension platform.
- Harnessed the existing digital finance ecosystem, resulting in active partnerships without requiring the set-up of new institutions.

### 3. Effective outreach and incentives

- Partnered with the local Savings and Credit Co-Operative Society (SACCOs) and local government officials to encourage account openings. Their wide reach and relationships helped shift behavior and mindsets toward long-term savings commitments via in-person nudges.
- To incentivize saving, the Rwandan government co-contributed 18,000 Rwandan francs for the first 3 years, with matching requirements based on users' income.
- The government also suggested options for guardians to open pension accounts for minors before they get a national ID, to maximize compound interest.

### 4. Systems for continuous learning

- Set up a strong technology-enabled recourse mechanism consisting of a national toll-free hotline with automated recording and escalation of complaints in defined timelines.
- Developed a centralized dashboard to track real-time complaints, irregularities in field staff communication, and mis-selling, enabling analysis of intermediary and user behavior patterns.
- Created and trained a dedicated team of 10+ staff to conduct regular meetings and focus groups to gauge user satisfaction levels and identify areas for improvement.

## KEY LEARNINGS

**Robust relationships and convenient solutions create trust.** Users maintain relationships with pension accounts for decades, so it was critical that they felt at ease in the system. EjoHeza used trusted outreach channels and centralized technology to make onboarding, contributions, and recourse easy, flexible, and dependable.

**Grassroots partnerships can enhance impact.** EjoHeza leveraged the on-ground presence of CARE International to expand users' digital and financial literacy, aiding adoption and use of the platform.

**Ongoing government support and smart collaborations are imperative for successful evolution.** Beyond catalyzing program setup, the government's commitment to finance design iterations, such as matching contributions and insurance bundling, made the difference between satisfactory and widespread impact. A nine-member team from pinBox and Mastercard had worked with Rwanda's Finance Ministry and AFR to help design, build, and roll out this government-sponsored digital micro-pension scheme.[111]

## KEY CHALLENGES

**Behavior change is a long-term game.** Convincing users to shift from a cash-based, day-to-day income to investing in long-term savings required persistent investment in outreach and incentives.

**Multi-stakeholder initiatives require clear coordination for efficient implementation.** It is critical to have a dedicated project management unit that is specifically empowered and responsible for achieving the policy, social, and business goals of the initiative. Responsibilities can include designing inputs, monitoring outcomes for review with other key stakeholders, and cooperatively developing response interventions as needed.

# Recommendations

## For **GOVERNMENTS**

**Government can consider product design and distribution regulations to ensure payment products meet the needs of target markets and are proportional to context.[112] These regulations may stipulate conducting prelaunch needs assessments, developing appropriate distribution mechanisms, ensuring post-sale product reviews, and articulating clear governance responsibilities to senior management.[113]**

**Government can empower regulators to impose restrictions on the marketing, distribution, or sale of products that meet users' needs.**

## For **COMPANIES**

**Co-create solutions with PSPs/banks centered around the needs of users and supply chain actors. Set up periodic meetings with partner PSPs/banks to discuss gaps in existing offerings and potential for modifications to better suit user requirements in last-mile areas.**

## For **INTERNATIONAL ORGs**

**IDOs can gather insights on marginalized user behavior. Research can be both quantitative (access to mobile phones and internet, literacy levels, frequency of use) or qualitative (mobility constraints, reasons for use, preference of recourse channel).**

**IDOs can provide technical assistance to and play a convening role for the digital payments industry to try new ideas in designing user-centric solutions, as well as facilitate the sharing of insights on marginalized users.**

PRINCIPLE

# 6 Be transparent, particularly on pricing

**The surging growth of digital payments services** means that providers are increasingly engaging with new users. These customers often find the software and terminology surrounding digital finance opaque and bewildering, but they are not alone. A disinclination to read the small print persists in more knowledgeable consumers, and lack of understanding breeds distrust.

**To build a thriving and inclusive payments ecosystem, the trust deficit must be bridged. A legacy benefit of the cash economy was that users were given more scope to pose questions to their providers, in branch or in person.**

To address this in terms of digital payments, transparency is pivotal. Equipping users with the information requisite for a positive digital payments experience builds a more predictable environment. Predictability fosters trust. This trust leads to better outcomes across the user journey. Sign-ups become more informed, transactions more accurate, and there is less need for recourse.

The importance of transparency is not new, but it is evolving. Transparency of product-critical information remains important. Too often, new users are locked out of their accounts because limits on daily transaction attempts have not been communicated. It is essential that users understand how their personal data are used – for or against them.

Disclosure itself is not a magic bullet. It is equally important to incorporate an outcomes-orientation and pair it with other tools including user-centric design and behavioral nudges.[114] However, it remains vital to note that users face difficulties advocating for transparency individually. Members should consider how best to represent this group.

Indeed, complexity in the digital payments ecosystem will continue to grow, meaning that members ought now to embrace a culture of transparency focused on empowering users, rather than simply meeting compliance requirements. Transparency in payments could align with the conditions of food nutrition labelling: mandatory, comparable, and digestible. Such shifts would be transformative.

Policies on sharing information with digital payments users exist in some markets (notably, the EU's Payment Services Directive) and are incorporated in various international standards (the World Bank Group's Retail Payments Good Practices).[115] Yet the push for ever more stringent disclosure requirements addresses only part of the problem.

A focus on compliance has led to a proliferation of lengthy, hard-to-decipher terms and conditions that serve only to confuse. There is a need is to empower users with the confidence to use digital payments tools in their everyday lives. It is desirable for leaders in the digital payments ecosystem to take agency over transparency, anchoring efforts on ease of comprehension.

**Complexity in the digital payments ecosystem will continue to grow. Members ought now to embrace a culture of transparency focused on empowering users, rather than simply meeting compliance requirements.**

### 1. Transparency is good for users.

When users understand their options, they can better decide what products are most suitable for them and accept the responsibilities and consequences of those choices.[116] Transparency has been shown to be more effective than education programs in building users' financial capabilities – a key driver of overall financial inclusion.[117] Visibility is crucial for users, especially as payment providers increasingly offer secondary products such as credit, where specific terms such as payment periods and interest rates can have vast and long-term impacts on a user's finances. Transparency is not a gift but an inherent right.

### 2. Transparency is good for business.

Given its foundation in user trust, transparency acts as a relationship-builder. A 2019 survey in Latin America found that distrust was the main reason people did not make more e-commerce purchases.[118] At an operational level, transparency helps users to help themselves, resulting in a more informed customer base. It also leads to fewer mistakes, reduced churn, and lower use of recourse and redressal mechanisms – ultimately decreasing costs. For businesses, governments, and international organizations, digitizing payments can in itself be an act of transparency – it enables traceability and reduces the potential for leakage, resulting in greater accountability. For the ecosystem at large, transparency promotes user choice, which increases healthy competition.

### 3. Transparency is becoming more complex.

In today's digital ecosystem, the very nature of what should be disclosed to users is changing rapidly. Astronomical quantities of data are collected, used, and stored by multiple parties to personalize products, identify security risks, or improve accountability.[119] Nevertheless, data usage is rarely explained sufficiently to enable truly informed consent. Additionally, regulations have not kept pace. A 2016 survey in the UK discovered that 92 percent of users did not understand how data collected by companies were being used and 57 percent did not trust that data would be handled responsibly. Even so, 67 percent of users said they would be happy to share more personal data if organizations were clear and transparent on how they were going to use the data.[120] Often, payers themselves are unclear on how partners are using their data and are often not the decision-makers for data use cases in their value chains.

**67% of users said they would be happy to share more personal data if organizations were clear and transparent on how they were going to use it**

# What does it mean to be transparent?

Being transparent with users means not only disclosing information about the product's own features and terms, but also how the data may be used. This is done with the goal of promoting informed decision-making.

## A. Effective transparency of products and services

### Make disclosures clear and effective to foster true user understanding

- Highlight key information for users, such as key features, fees, exchange rates, terms and conditions, transaction limits, details of the provider and service fund protection mechanisms and liability for unauthorized transactions, privacy policies, how to raise a query/complaint (#rdpg8), advice on safeguarding personal devices, and access codes.
- Ensure language is brief (e.g., minimizing scroll-down time on digital devices), localized (e.g., India's PayTM app available in 11 languages[121]), and visual to improve comprehension, especially for low-literacy users. It may be useful to provide infographic-based summaries of any legalese).[122]
- Confirm user comprehension, especially for third party add-ons (e.g., through callbacks, pre-transaction confirmations, checklists for agents, or glossaries). Seek user feedback to identify common areas of confusion and adapt accordingly.

### Provide timely information to users

- Share provider comparison details in advance of sign-up via short, standardized, one- to two-page key facts. Ideally, these should be consumer-tested before a standardized format is prescribed.[123]
- Invest in "how to" resources such as pop-ups, tutorial videos, or agent assistance when a user tries a new feature.
- Disclose fees separately from transaction amounts, provide pre-transaction confirmation and post-transaction receipts. In addition, provide continuous access to clear and simple transaction records in commonly required formats (e.g., account history statements where text message confirmations are not accepted as valid proof).
- Ensure details for recourse are provided when a user launches a complaint, including transaction data, parties involved, and complaint status.

**Mexico's entity to defend user rights in financial services**[124]

Established CONDUSEF under the Law of Defense and Protection of the Financial Consumer to:

- inform the public about financial institutions' services, fees, and complaints against them
- strengthen capacity of financial institutions to gather information necessary for reporting
- maintain a registry of users who do not want their information shared for marketing and advertising purposes
- impose sanctions on institutions who violate consumer rights.

**Government of Philippines disclosure forms**[125]

Conducted behavioral research among users and designed easy-to-understand loan costs and term disclosure forms, enabling more informed decision-making for users.

### Equip users with requisite information for informed and unbiased decision-making

- Ensure information is updated alongside product evolutions and that any changes to terms and conditions or fees are given with advanced notice.[126] These updates can be provided on digital platforms, through agents, or on a website.
- Provide candid guidance to users on the different service bundles available and limit nudges toward bundles more profitable to providers at the expense of user suitability.
- Disclose all variations in fees and other features, such as whether the payment is cash-to-cash, cash-to-account, account-to-account, or across providers or borders.[127]

## B. Increased transparency on data use

Commit to regular disclosures beyond products to the application of user data across the value chain

### Extend transparency principles throughout the value chain

- Encourage joint ownership of transparency by developing agreements among all parties regarding what data may be collected and how this may be used. This agreement might also clarify which data are not acceptable to use (e.g., identity-based information such as race, religion, gender, or disability that could lead to discriminatory denial of access).
- In the case of multiparty data use, align on which party is responsible for and bears the cost of informing users. Confirm the mechanisms for users to inquire about these data, update them, and manage consent.
- Determine which user data may be shared between discrete parties and develop interoperable, clear, and informed user consent mechanisms.
- Advocate for industry-wide regulatory standards on data transparency, especially in the use of artificial intelligence and machine learning. In the absence of regulation, issue non-binding principles to encourage ethical and responsible use by financial institutions as done in Singapore, the Netherlands, and Hong Kong.

**Singapore's principles for use of artificial intelligence and data analytics**[128]

Recommends that FSPs disclose use of artificial intelligence and data analytics to users as part of their general communication.

Advises FSPs to provide a clear explanation on what data are employed to make artificial intelligence-driven decisions, how the data affect the decision, and any consequences.

### Promote users' rights to transparency regarding the use of their data and communicate how and by whom this is provided

- Ensure providers proactively disclose the impact of the use of artificial intelligence, which includes machine learning and algorithms ("good algorithm governance"),[129] including what personal data are used across the value chain (e.g., in-product transaction history, alternative data from social media), how users may update or change their data, how such data affect artificial intelligence-driven decisions about them, and implications on their current and future financial profile (e.g., repayment frequency affecting approval for future loans).[130]
- Require providers and third parties who seek to monetize user data to disclose this practice to users and allow them to demur.
- Develop approaches that empower users to control how their data are used, allowing them to easily access, correct, and port data free of charge. Provide guidance on what data are not acceptable for use (e.g., race, religion, gender), so that users are not defrauded into sharing this information with unscrupulous parties.

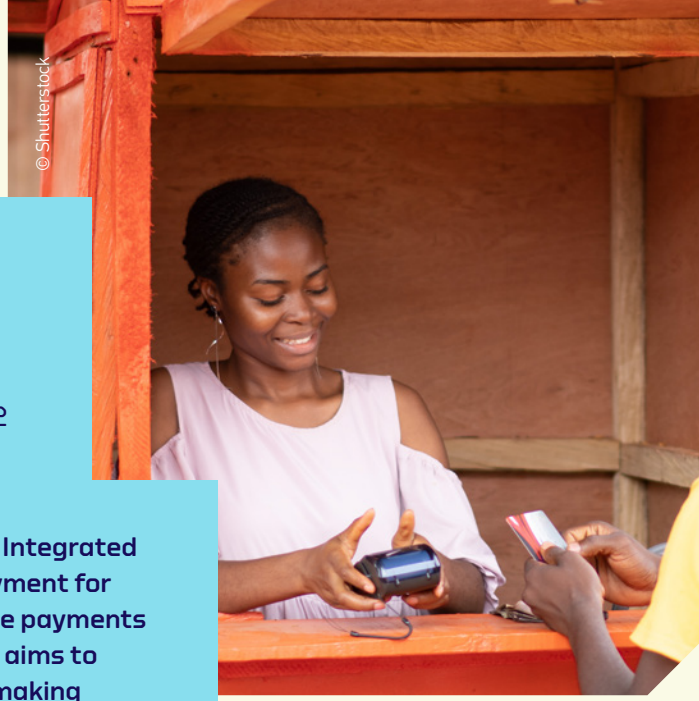
**Google's data privacy policy**[131]

Google

Communicates to users in a clear and simple manner – often using visuals and videos – issues including which user data are collected, why these are collected, user privacy controls, when data are shared, and how it protects user data.

Consistent with one of the GDPR's most crucial policies around giving users the ability to revoke consent on data; clearly depicts how users can remove their data from Google systems.

CASE STUDY


© Shutterstock

# Integrated Management Information System

## for Universal Health Coverage in Senegal[132]

**In 2019, the Agency for Universal Health Coverage (UHC)** launched the Integrated Management Information System to digitize enrolment and premium payment for the existing community-based health insurance scheme and to streamline payments between the agency, other health providers, and employees. This system aims to provide beneficiaries with relevant information to enable good decision-making related to their health insurance and to improve data management. Within 10 months of digitization, the scheme onboarded 54,000 users and reduced enrolment costs per user from US$4.7 to US$2.4. Today, 2.8 million people are enrolled. The use of a broad set of communication channels to target vulnerable and digitally averse users was key to uptake.

### Notable features

#### Effective transparency of products and services

- Partnered with providers to conduct monthly campaigns across Senegal on the health scheme, its app, and recourse features.
- Equipped beneficiaries to view and manage their insurance plans via a mobile app providing personalized information on coverage, geo-location of nearby health-care points, payment, account histories, and SMS transaction receipts.
- Built traceability into the app so that sponsors (often diaspora family members) could pay for and track health-care costs for enrolled relatives. This covers premiums, doctor consultations, pharmacy fees, and health records.
- Enabled user feedback via hotline and agent consultations.

#### Improved transparency of data

- Created a secure and encrypted data warehouse that links beneficiaries' unique insurance ID to details of illnesses, health insurance, and payments, while reporting to the regulator, the National Data Protection Commission. Access to these data is role-based to balance transparency with confidentiality.
- Informed beneficiaries about data collection, use, and security when enrolling via agents or the app. Users can control, modify, and communicate with administrators about their data.
- Appointed community-based health insurance officers to help beneficiaries with lower literacy or those less fluent in French understand the health plan and data use.

## Implementation journey

### 1. Identification of opportunity to digitize universal health coverage

- Launched a sweeping program for UHC in 2012. Enrolment reached approximately 50 percent by 2016, but penetration plateaued.
- Identified digital integration as a pathway to improve reach and designed a comprehensive and modular digital program linked by unique beneficiary ID numbers.
- Earlier manual systems for enrolment, billing, and reporting resulted in errors, confidentiality risks, deterioration of historical data, and limited ability to track personal data.

### 2. Research to identify best practices and user needs

- Conducted landscaping research on other African health and digitization projects, such as Kenya's use of USSD technology vs. online platforms to keep users informed about enrolments. Rwanda's and Morocco's achievements of high coverage via enrolment mandates were also studied.
- Conducted qualitative user research, finding that people held greater trust in public institutions than in private actors when it comes to maintaining effectiveness of the public program. Digitization was viewed as an opportunity to improve accountability and transparency within government.

### 3. Selection of partners for system development and rollout

- Partnered with telecom companies to allow e-money transfers for premium payments linked to each beneficiary's ID.
- Partnered with the Japan International Cooperation Agency (JICA), given its strong human resources footprint in Senegal, to train officers to recruit and retain database and information security experts.
- Anchored in the influential Ministry of Finance to improve buy-in and share data analysis on potential cost savings, to inform other stakeholders of the digitization process.

### 4. Launched pilots and collaborated to realize systemic improvements

- Launched pilots for the app that offered users a view of the coverage, services, benefits, and structures linked to their insurance plan. A total of 6,000 people were registered by mid-2020. Pilots showed that users were confused about the scope of services offered, so improvements were built into app design and communication was improved.
- Collaborated with other insurance providers to improve transparency on enrolment, helping to ensure that the free care provided reached the intended beneficiaries, and not those already covered by other schemes.

## KEY LEARNINGS

**Effective user transparency requires diverse channels.** The agency manages multiple channels for communication including mass media (television, radio, social media), home visits, forums in villages and schools, hospital and pharmacy providers, and messaging from influencers such as celebrities and religious leaders. Alongside the trust users placed in the agency as a public institution, this has improved user receptiveness.

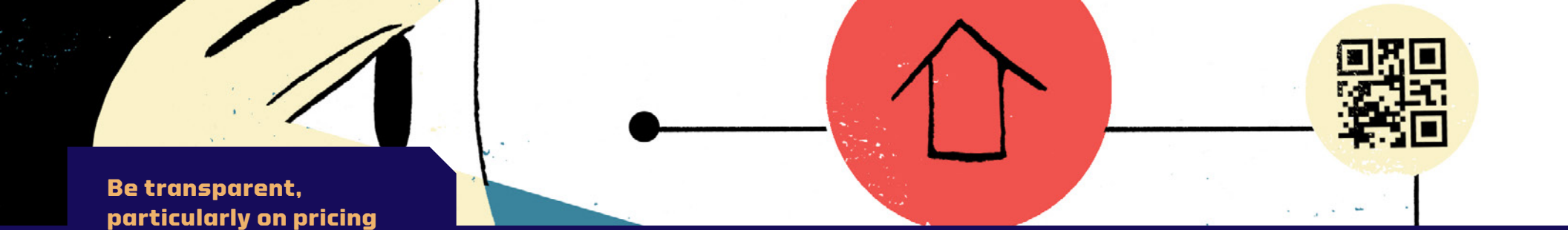
**Transparency should be embedded in the DNA of multi-sector partnerships.** Information-sharing gaps between the Ministry of Finance and health-care bodies led to a lack of clarity about drug coverage and hospital services. As a result, underinformed patients stopped paying UHC premiums. A revised retention strategy is being developed in response.

## KEY CHALLENGES

**Human resource planning and upskilling are important components of the digitization transition.** Low digital capabilities among agents and billing staff resulted in challenges for implementation. Many of the staff also saw a decrease in their responsibilities and information control because of digital efficiencies and transparency requirements. This left many feeling less valued or afraid of losing their jobs, leading to a resistance toward the shifts required in the new system.

**Just-in-time communication is critical for user-friendly service.** While users were informed of benefits during onboarding, many were unable to recall them when seeking services later on. Using digital systems to ensure all plan details are readily available may help to bridge this gap.

© Better Than Cash Alliance/Elise Fitte-Duval

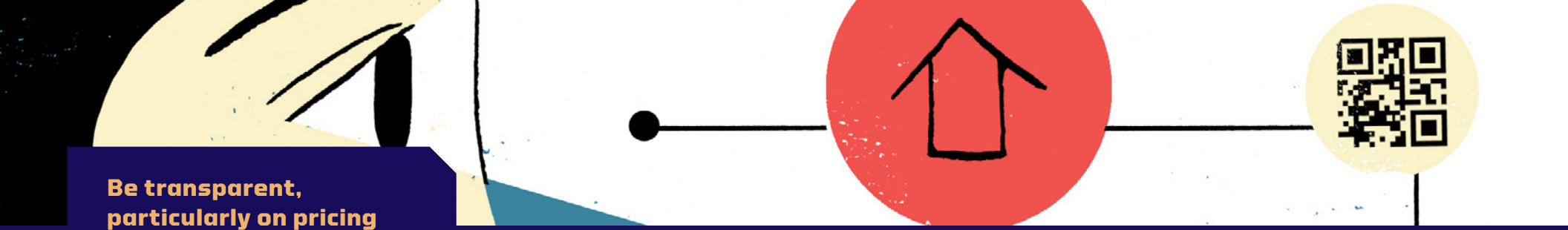


**Be transparent, particularly on pricing**

# Recommendations

Governments, companies, and IDOs can **creatively communicate information** about digital payments systems that is easily understood. This information could cover the benefits and risks of using digital payments vs. cash, how to access and use digital funds in a safe manner, and where to turn for support. Local languages and user-preferred channels should be used.

Governments can **institute service-level agreements** that clearly define the information to be shared and also prioritize user comprehension. This could include the user-focused development of limited-length communications or using visual summaries of terms and conditions to ensure disclosures serve users rather than protect providers.



**Be transparent, particularly on pricing**

# Recommendations

## For **GOVERNMENTS**

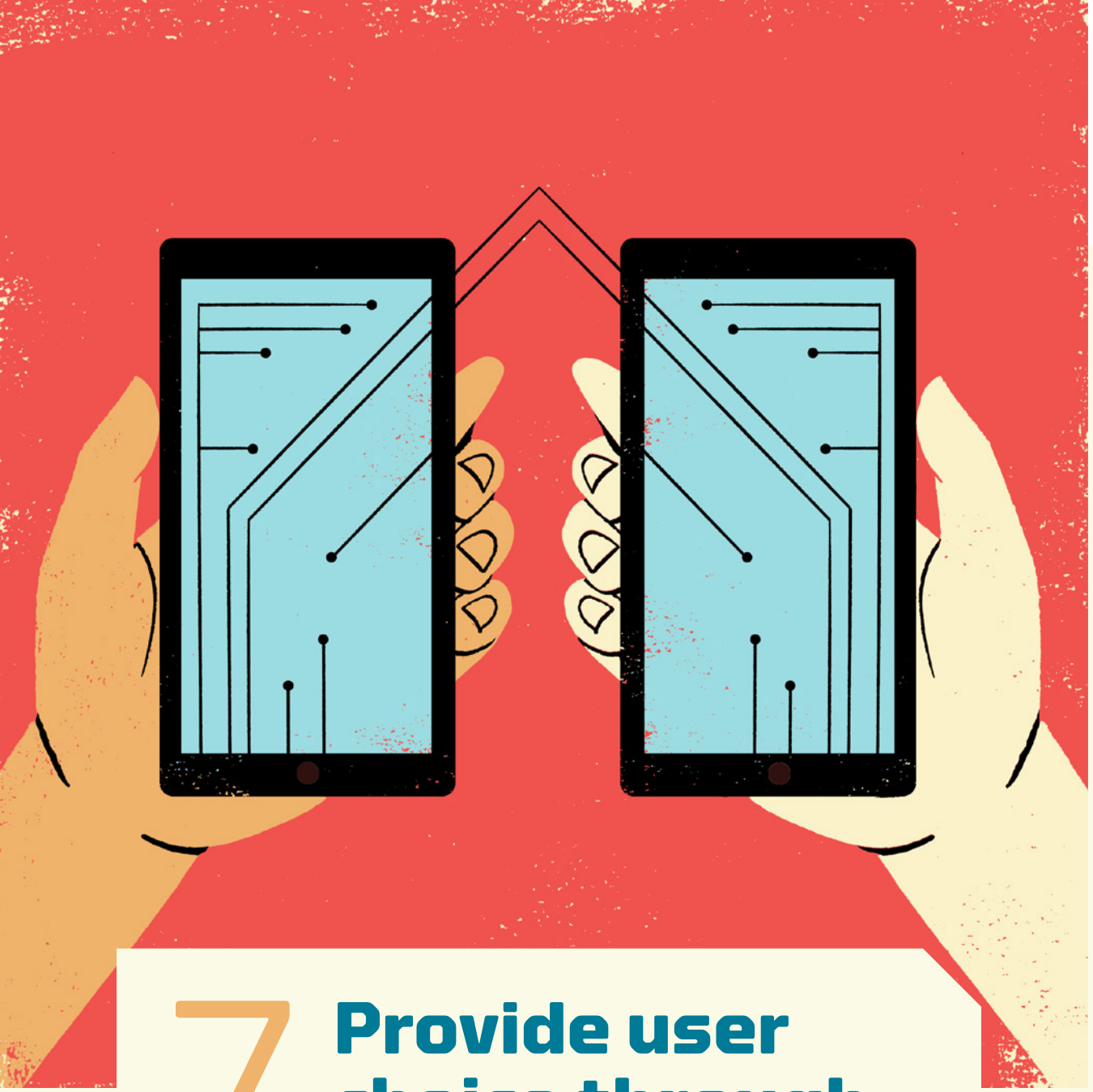
**Governments, in their capacity as regulators, can develop transparency regulations that disclose complete information in a simple and easy-to-understand manner.**

**Governments can consider publishing or requiring digital payments partners to publish Grievance Redressal Summaries frequently.**

## For **INTERNATIONAL ORGs**

**IDOs can invest in human-centered design to better understand user concerns, constraints, and preferences regarding transparency (e.g., channel and media type for receiving information).**

**IDOs can provide assistance to governments in creating regulations based on global good practice in areas such as features, risks, costs, and terms and conditions. Emerging issues such as transparency on big data, decision-making algorithms, and other technological advances also ought to be considered.**



PRINCIPLE

# 7 Provide user choice through interoperability

**The full benefits of digital inclusion** will only be unlocked when services are truly interoperable. The recent migratory flow towards digital payments has been marked and is welcome. However, many end-users languish in silos prevented from transacting freely or affordably across providers. These silos preclude digital payments from achieving the same convenience, affordability, and utility as cash.

**Many users experience services within fragmented ecosystems in which providers operate independently, neither sharing data nor transacting across one another. Some providers offer these flexibilities at a cost, which deters users from transacting with peers and retailers over platforms. This dynamic occurs commonly in different industries, use cases, and even across national borders.**

For underserved populations, many of whom reside in rural or low-income communities, binding socioeconomic constraints make this a particularly untenable prospect. For these users, the direct cost of surcharges on cross-provider transactions is galling. Supplementary opportunity costs – such as those incurred by a user physically traveling to banks because they are blocked from digitally transacting with them – only exacerbate the issue.

Progress toward a more interconnected network of digital payments solutions has been steady. Nevertheless, these connections often amount to case-specific bilateral agreements between providers. The next evolution will witness the development of shared digital infrastructure (including digital ID and mutual databases), the participatory development of policies and governance mechanisms, and the cultivation of a collaborative community of innovators. Such an environment holds the potential to unlock greater ease of use for end-users and ensure commercial viability for providers. It will also generate valuable research and data insights for supporting actors involved in governance and financing.

Furthermore, users often experience long delays or fees levied for interbank transactions and find they have limited options to transact (when their debit cards are accepted only by merchants transacting through the same bank, for instance). This reduces the value of digital payments to previously unbanked users, who become disinclined to lose the flexibility of cash. Resolution is under way, with the integration of discrete data and back-end services facilitating a more seamless transaction experience between providers.

The next leap forward hinges on how swiftly governments, companies, IDOs, and providers converge toward ecosystems[133] supported by open infrastructure. This transition represents a tangible advance to a seamlessly integrated digital payments experience, greater user choice and, ultimately, still stronger demand for digital payments.

The shape of these ecosystems remains to be determined. They may well include data registries, API-enabled information exchanges, and digital IDs, but should be shepherded by a participatory approach to governance that holds all actors accountable to agreed standards for operating in an open digital environment. They should also anchor on a commitment to promote collaborative solutions that optimize the speed, security, convenience, and affordability of the user experience[134] regardless of provider, agent, or device used.[135]

It is essential, too, to ensure that open platforms do not usher in monopolies. An open platform can have the unintended consequence of a popular provider becoming dominant.[136]

**UPI, an interoperable platform in India consistently logs**
**1.5 BILLION transactions each month**

This paradigm shift will empower users to engage with products and services from different providers with reductions in time required or financial cost, making digital payments truly better than cash. However, achieving these objectives requires addressing two concerns.

### 1. Incentives supporting ecosystem-level collaboration are weak, choking beneficial innovation.

Providers often lack the means and incentives to build and access open payments infrastructure on their own, resulting in closed-loop systems. This challenge is common across emerging economies, where fewer than half of payment systems are interoperable.[137] In Bangladesh – still early in its interoperability journey – more than one third of the population is excluded from DFS because of the high cost of transacting across platforms. Microfinance institutions, which serve approximately 40 percent of the country's population, have yet to implement any meaningful interoperability measures.[138]

Other providers may enter into ad hoc bilateral agreements that deliver a small degree of interoperability. Several countries – such as Indonesia, Madagascar, Tanzania, and Thailand – have adopted this "focused" approach to interoperability, forging case-specific business agreements between selected providers. As a result, providers are managing separate bilateral connections, which creates inefficiencies in interbank settlements and causes apprehension around introducing yet greater interoperability across a wider variety of use cases in the future. Additionally, competitive dynamics have left many players, particularly large-scale providers, reluctant to work collaboratively with their counterparts. The absence of leadership from these providers leaves transaction volumes too low to justify the initial investment for smaller-scale participants to develop their own interoperable systems. The result crowds out innovation and, ultimately, limits the value unlocked for users.[139]

### 2. Policy mechanisms struggle to balance protecting users' interests with ensuring the commercial viability of interoperable networks.

As countries trend toward interoperable systems,[140] they struggle to balance the protection of users' best interests with the facilitation of provider participation. As a result, many countries face challenges in defining and implementing a shared central blueprint for market-wide interoperability. A study of digital financial interoperability across different countries found that only 30 percent of surveyed countries have been able to do so, with most solving for interoperability in specific (often P2P) use cases without incentivizing participation by all providers. While these governance mechanisms do encourage interoperability among the pockets of engaged providers, they do little to bring in the wider ecosystem of DFS providers (especially non-banks) or link together a country's wider banking infrastructure within a shared platform.

Conversely, countries that have deployed market-wide approaches are guided by the common high bar of global industry standards, such as the EU's Payment Services Directive (PSD2). This approach enables ubiquitous service and user experience. These standards, however, may not be evenly applicable or feasible across countries and contexts. Policies that are not specifically tailored to the needs, constraints, and interests of their providers can result in a suboptimal transaction experience – ultimately affecting the user. A case in point: Pakistan's existing governance mechanisms for interoperability do not enforce clear interbank pricing rules for transactions above a certain value, creating delays in settlement processing. However, this will change with the future launch of fast payments.

**The next leap forward hinges on how swiftly governments, companies, IDOs, and providers converge toward ecosystems supported by open infrastructure**

# How can user choice be supported through interoperability?

Developing a successful open digital payments ecosystem starts with architecture that facilitates the seamless flow of data and funds. It is supported by participatory policy development and governance that suits the context of a specific country or region, protects users interests within that context, and incentivizes the continued participation of providers in the public and private sectors. Most importantly, it requires ecosystem-wide buy-in, collaboration, and collective innovation from banks, PSPs, and agent networks. Such collaboration must unlock value not only for those innovating but also for the end-user. These three streams converge to create an environment with open, competitive payments in which users, and their choices, are paramount.

## A. Participatory governance

Engage providers in shaping policies and governance mechanisms that achieve interoperability

### Play a nurturing role while providers determine the details and business case of interoperability

- Encourage industry-led solutions for interoperability that are safer bets for sustainable scale. Engage the public sector to encourage and foster these efforts, while supporting intervention when industry-led solutions increase barriers to access.
- Bring providers and industry associations into the process of drafting business operation agreements (e.g., choice of technology, protocols for settlement and clearance, interoperability charges, risk).
- Ensure new players have a seat at the table to promote innovation and competition, thereby benefiting the user.

### Institute policies that promote interoperability in payments systems

- Promote interoperable solutions aligned with applicable policies or practices (such as GDPR and the California Consumer Privacy Act for data use, PSD2 for consumer protection, EMVCo specifications for interoperability) to not only create pathways for scalability, but also enable greater compatibility with payments platforms in other countries.

**Tanzania's mobile money regulations**[141]

Tanzania's government engaged in consultative dialogs to decide on rules and operating principles to govern interoperability, yielding a broad set of participation, clearing, and settlement principles and dispute management frameworks.

To accommodate diverse needs, the Tanzanian government engaged bilaterally with providers to align on pricing structures, following guidance from the country's Fair Competition Commission.

**ASEAN's QR code standardization**[142]

To promote a more seamless cross-border payments experience, the Association of Southeast Asian Nations (ASEAN) took measures to standardize QR codes across its 10 member states.

ASEAN's Finance Ministers and Central Bank Governors Joint Committee laid down broad norms governing QR standardization (e.g., around data flows, currency exchange), but ultimately gave individual countries freedom to forge bilateral agreements that most directly met their needs.

- Establish a central agency to enforce agreements, identifying the organizational structure and operating processes most relevant to a country's context and objectives. Promote multi-stakeholder governance, including government bodies, commercial actors of various scales, and individuals to enhance transparency.[143]

### Institute policies that promote interoperability in payments systems

- Ensure that regulators have both the necessary information and authority to intervene in cases where providers are exploiting a dominant position.[144]
- Ensure that users face no penalties or surcharges and are otherwise unrestricted from transacting with accounts held with FSPs other than their own.
- Influence providers and agent aggregators to ensure that banking agent networks are as interoperable as accounts and payments solutions, at least regarding cash-in-cash-out services. Where FSPs are unwilling to concede exclusivity, ensure their agent networks and the platforms on which they operate are interoperable and interconnected.[145]

## B. Open technology

Build an open and inclusive ecosystem

**Develop a range of interoperable payments services. These services may include P2P transfers across providers, retail and bill payments, the ability to cash-out through any ATM or agent, and the ability to port data between providers. The ability to connect to accounts where users received cash transfers (e.g., G2P, humanitarian, or wage accounts) should also be included.**

- Invest in shared infrastructure, such as programs for universal digital identification.[146] Where necessary, be flexible in accounting for users' ID capabilities and encourage providers to accept multiple forms of ID for registrations and/or transactions.
- Build technology infrastructure that supports seamless use of shared data and systems, including data exchanges and registries, open stacks, and open APIs.

### WFP's blockchain-based cash transfers in Bangladesh[147]

WFP's Building Blocks technology creates a shared database of humanitarian cash assistance programs to collect disbursements from multiple agencies as a lump sum, using QR technology to facilitate a single transaction.

At the foundation of the program is a shared database of beneficiary information – including which programs they are receiving benefits from – that is stored and encrypted using blockchain technology. These "blocks" are available to humanitarian organizations as a common resource.

These blockchain-enabled QR codes are scannable not only by the organizations disbursing relief, but also by retailers (e.g., grocers) selling food and other necessities, enabling an interoperable user experience at the point of service.

### Invest in technologies appropriate to the market

- At a country or regional level, identify models for interoperability that account for specific operational constraints (e.g., network connectivity), market structure (e.g., size of banking sector, types of digital transaction accounts extant), and regulatory models (e.g., open banking policies). Account for these variations in not only the technical design of the platform, but also the nature of the business agreements supporting them.[148]
- Where feasible, deploy open-loop payments systems that can transform transaction behaviors systemically. Compromise toward closed-loop systems only in crisis situations, for instance when disbursing COVID-19 relief or in areas lacking viable payments infrastructure.

## C. Ecosystem mindset

Champion collaboration toward innovative solutions that deliver 360-degree value

### Facilitate strong relationships between platform participators

- Articulate the business case for an open ecosystem to all providers, particularly those that may be reluctant to collaborate because of perceived competitive risks. These benefits include more frequent transactions for banked users, more new/unbanked users transacting digitally, and users continuing to hold funds in their accounts vs. cashing out immediately.
- Encourage development of new solutions on top of core digital infrastructure, involving smaller players such as fintech, civil societies, and social enterprises. Foster a culture of collaboration within this innovator network, pooling collective resources to provide user-centric solutions that promote an increasingly interoperable and seamless payments environment.[149]
- Facilitate data-sharing agreements that draw insights regarding user profiles and engagement, adoption barriers, and platform performance. Analyse user data to steer the ecosystem to improve utility and user-centricity of existing solutions, develop new solutions, and refine and enforce policies (#rdpg7). Liability needs to be clear for users as well as providers.
- Develop central engines for support functions, including dispute resolution and customer support. Ensure user experience is standardized regardless of which provider they choose.

#### Singapore's ecosystem-led innovation[150]

Singapore's government has launched the InnoLeap Programme, enabling public sector agencies to collaborate with research and higher learning institutes and commercial entities to co-create innovative technology solutions.

It runs similar programs that develop solutions in consultation with prospective end-users, partnering with trade associations and unions to test solutions before their release – allowing developers to tailor solutions to user needs and increase likelihood of usage.

CASE STUDY

# India's Unified Payments Interface

## The gateway at the center of India's open and inclusive digital payments ecosystem[151]

© Shutterstock

**Envisioned by India's central government,** the Unified Payments Interface (UPI) is a combination of an information exchange protocol and white label front end. The government-endorsed Bharat Interface for Money enables the seamless transfer of funds across PSPs. The solution pairs the seamless exchange of data via open APIs with a customizable front end to democratize access to and usability of digital payments. The design elements and policies supporting the UPI protocol were conceived with the wider payments ecosystem including consultations with leading banks and fintech facilitated by the NPCI, as well as guidance from public institutions such as the Ministry of Electronics and Information Technology (MeitY) and the Reserve Bank of India (RBI).

The proposition of a structured, plug-and-play solution that can be freely innovated upon is appealing to providers, while the promise of affordable interoperability attracts users seeking to transact across banks. As of September 2020, UPI has scaled to cover approximately 170 participating FSPs and was consistently logging more than 1.5 billion transactions each month.

### Notable features

#### Participatory governance

- Government took ownership of developing a vision for an open digital payments ecosystem, collaborating with the private sector (including smaller players) to ensure buy-in and inclusivity.
- Established a governance model giving representation to established promoter banks along with new participants (selected on a rotational basis).

#### Open technology

- Facilitated the flow of information between banks, using two-factor authentication to verify data and transactions.
- Developed a modular interface that could be freely overlaid on any payments system without forgoing functionality.
- Used open, XML-based APIs to facilitate seamless flow of user data (e.g., account holder name, branch codes).

### Ecosystem mindset

- Gave providers the flexibility to remake the interface to reflect their brand identity and users' needs (through open APIs and source code), without having to develop state-of-the-art technology.
- Participatory approach to technology and policy development. Notably, working groups with commercial banks were used to inform encryption protocols to protect against fraud.

## Implementation journey

### 1. Framing the vision for an open digital payments ecosystem

- Diagnosed key challenges to the uptake of the Immediate Payment Service (IMPS), India's existing instant settlement system – especially for smaller transactions. These included low network connectivity and the lack of an accessible user-friendly front end.
- Developed the vision for an information exchange that would enable seamless flow of data and payments across banks and PSPs. Supported this development by consulting with iSPIRT – a development community – to frame design principles for the solution. Consulted the Reserve Bank of India for guidance on framing broad policies for data protection and dispute resolution.

### 2. Collaboratively developing the solution

- Developed UPI protocol through deep consultations with fintech partners, development sector thought leaders, and the ecosystem of banks and PSPs.
- Engaged banks to assuage concerns about interoperability, while seeking their inputs on both solution design and tailoring of the customer experience for each bank. Gained momentum by lobbying and enrolling the State Bank of India, India's largest FSP, creating a pull for more than 40 providers to join before launch.

### 3. Accelerating growth through ecosystem-wide buy-in

- Launched the Bharat Interface for Money (BHIM), a provider-agnostic, UPI-based application for facilitating interbank payments. The government's endorsement of BHIM as India's national payments app created a groundswell of demand, incentivizing participation by providers and giving them a basic UPI.
- Expanded eligibility to banks and non-banks, allowing for participation by diverse market players – each empowered to develop and innovate freely.
- Updated governance to reflect the views and inputs of an increasingly diverse roster of participating banks, giving voice to both original promoter banks and new participants.

### 4. Widening UPI's sphere of influence

- Evolved UPI to include new payments models (e.g., small ticket loans, cash withdrawals) and to expand into the wider payments ecosystem. For example, NPCI is actively exploring the viability of Online Dispute Resolution (ODR) for identifying failed transactions and informing efforts to protect the user from technical failures.
- Solidified UPI's reputation as the gold standard for open, interoperable digital payments, resulting in other emerging markets (e.g., Indonesia, Myanmar, Nepal) recognizing the potential to transform their digital economies.

## KEY LEARNINGS

**Public institutions have the reach and authority to lead development of a shared vision.** India's vision for a unified payments ecosystem was spearheaded by the Ministry of Electronics and Information Technology, among other government actors. The vision was sharpened in collaboration with private sector partners and development thought leaders. These principles shaped the development of the core platform.

**Interoperable solutions must be tailored by country.** UPI is supported by institutional and governance mechanisms identified based on early diagnoses of India-specific barriers, such as low network connectivity and fragmented banking.

**Engage providers as partners in the transition to interoperability, rather than passengers.** NPCI continuously collaborated with banks, PSPs, fintech, and other private sector partners.

## KEY CHALLENGES

**Many providers operated on legacy systems that made them incompatible with UPI's technical architecture.** UPI's open specifications, particularly with respect to its handling of XML-based APIs, were hard to implement for banks used to operating on outdated and heavily siloed systems.

**An open digital payments ecosystem includes more intersystem interfacing and exchange of data.** An absence of data protection legislation created ambiguity for both NPCI and participating providers. The government identified and established norms for data protection – limiting NPCI to holding only the user's unique national identification number (Aadhaar) and a basic bank identifier, rather than sensitive personal information and account details.

© iStock

**Provide user choice through interoperability**

# Recommendations

Governments, companies, and IDOs can **invest in shared infrastructure** to reduce costs and increase access to digital payments at the last mile.

For governments and IDOs, this includes **creating shared interoperable identification and enrolment systems** that can plug and play with national payment systems to improve inclusion and usage.

For companies, this entails **collaborating with competitors to invest in common infrastructure requirements** for digital payments such as merchant acceptance points at local retailers.

**Provide user choice through interoperability**

# Recommendations

## For **GOVERNMENTS**

**Governments can use open standards to promote interoperability across all systems allowing innovators and civil society to built on top.**

**Governments can shepherd a participatory approach to governance that holds all actors accountable to standards for operating in an open digital environment.**

**Governments can promote the development of innovative solutions that optimize the speed, security, convenience, and affordability of the user experience regardless of provider, agent, or device used.**

## For **INTERNATIONAL ORGs**

**Provide technical assistance to providers to forge bilateral/multilateral acceptance arrangements. Innovate on individual solutions to pursue these broader financial inclusion objectives.**

**Conduct research to quantify the impact of interoperability on end-users, payment providers, and national financial sectors. Use the findings to better articulate the business and impact case to banks and PSPs that are unable to rationalize competitive risks.**

# 8 Make recourse clear, quick, and responsive

**The dizzying proliferation of digital payments** has ushered troupes of new actors into last-mile delivery. Additionally, the COVID-19 crisis turbocharged the volume of digital governmental payments to new users. Unsurprisingly, these shifts have seen a commensurate increase in disputes and grievances, making it vital for redressal systems to advance synchronously with the sector.

**Even today, recourse systems remain a formality. Too often, they are archaic and irrelevant. Grievance redressal procedures have simply not kept pace with the increasing sophistication of payment platforms. Recourse, then, requires an overhaul.**

To begin, it is useful to re-evaluate the entire concept of recourse.

When faced with a problem, users require not only a fix but also a holistic understanding of the whole redressal process. Commonly, users have become cynical, wary, and feel that the onus of resolution rests on them.

**A 2021 survey[152] among users of DFS in Nigeria, Kenya, and Uganda revealed that 55.1 percent, 46.8 percent, and 64.1 percent reported not using the complaints redress channels when faced with issues.** Users are often left cynical and wary of the value proposition, with many feeling the onus of resolution is on their shoulders.

It should be borne in mind that, for the underserved, recourse systems act as a lifeline. Loss of funds is proportionately more important to low-income users who consequently operate from a baseline of abundant caution. A successful recourse system is therefore one that shares clear information with the user, caters for equal access, and delivers resolutions that are timely and accountable.

The latent potency of redressal data is huge. Insights and feedback generated through the recourse procedures will strengthen and improve existing structures and processes. Grievance data help to identify emergent risks and training shortfalls, and improve knowledge of market segmentation. Successful grievance systems breed trust in digital payments and ensure users are less likely to revert to cash.

**Rwanda Utility Regulatory Authority (RURA)[153]**

Regulation requires providers to acknowledge a complaint within 5 days, resolve within 15 days, and report all data to the Central Bank.

Monitors all transactions in real time and encourages customers to report issues to the Central Bank/RURA.

**In Kenya, 46.8% of respondents**
**of a 2021 survey reported not using the complaint redress channels when faced with issues**

Three issues require mitigation.

### 1. Users do not know how to complain.

When a grievance arises, many users have little to no idea about how to address it. Information on recourse is rarely available at the incidence of a problem and is often outdated and unclear. This lack of awareness of their rights, including what comprises a complaint, where a complaint might be made, and how to lodge a complaint, can be debilitating to new and at-risk users. A study on digital payments in India[154] indicated that 42 percent of respondents believed a "greater awareness on redressal mechanisms" could enhance their adoption of digital payments.

### 2. Users struggle to access badly designed recourse systems.

Often, recourse procedures do not cater to those outside the mainstream with respect to language, gender, disability, cultural norms, literacy levels, and access to technology infrastructure. For example, many complaints channeled through helplines are often unavailable or involve processes that remain anachronistic and cumbersome. These obstacles naturally exclude a large segment of users who do not own a phone but are recipients or users of digital payments (e.g., through biometric readable cards, cash cards, or G2P payment programmes). Even in 2019, about 30 percent of adults in Venezuela[155] did not own a mobile phone. Of these people, 17 percent regularly shared someone else's phone. In such scenarios, recourse systems that require individual identification become useless.

### 3. Users fail to achieve a resolution and hemorrhage trust.

Users pursuing redress face a huge burden on their time and resources, which can be disproportionately onerous for those who rely on daily payments. Recourse systems that do not respect users' lifestyles, constraints, or aspirations present a barrier to sustained digital payments adoption. For example, India has a national ombudsman.[156] However, it also has a minimum 30-day waiting period after registering a grievance. In 2019, only 31 complaints were adjudicated. Given India's massive volume of transactions, this suggests a slow and inadequate resolution rate that deters – and ultimately hurts – users.

**For the underserved, recourse systems act as a lifeline.** **Loss of funds is proportionately more important to low-income users who consequently operate from a baseline of abundant caution.**

**Bangko Sentral ng Pilipinas (BSP) Online Buddy ("BOB")**

BOB is a chat bot that handles questions and concerns by consumers via SMS, Facebook Messenger, and web chat. Automation enables real-time follow-up with financial institutions and shortens the turnaround time for complaints resolution and user-experience improvements. This builds trust with users, who are encouraged to voice their grievances, thereby reinforcing the tool's relevance and effectiveness. Through the application of AI and Big Data, BSP uncovers patterns of consumer behavior, offering early warning of financial stress, supporting overall ecosystem monitoring. Since its launch in 2020, BOB now processes over 50% of total complaints and queries received.

# What makes a successful recourse system?

A successful recourse system makes filing a complaint as easy as making a transaction. Designing in this way requires attention to the four building blocks below. While they follow a linear user journey, these blocks also reinforce each other through interaction. For instance, a predictable and interoperable back end makes it easier to share information with users.

## A. Upfront awareness

Share recourse information through multiple channels

### Offer end-to-end recourse information

- Go beyond providing a helpline to equip users to undertake recourse (e.g., share how to make a complaint or alternate avenues for resolution in the case of unsatisfactory recourse and escalation options).

### Assume the burden of informing users

- Shift the burden away from the user and create easy-to-access recourse points across the payments value chain (e.g., in precontractual disclosures, during the onboarding, after the transaction is made, and even upon making a complaint).
- Actively communicate recourse information, even if users may not need it (e.g., the kind of awareness of the emergency numbers like 911 in the United States, 112 or 999 in London, 100 in India, etc.).

### Consistently use multiple channels

- Share recourse information in different languages and formats and across locally relevant platforms to reach target segments (e.g., WhatsApp messages, pictorial process charts, interactive radio shows, or video messaging).

## B. Equal and easy access

Design appropriately for all users

### Design for the user's convenience

- Design an easy recourse system that requires minimal documentation. Offer a single point of contact, a user-friendly interface, and an accessible procedure (be sure to account for users' literacy levels and access to digital infrastructure, e.g., provision to file complaints in person or via social media).

**WFP Kenya Accountability Together Helpline**[157]

Involved more than 40 state and nonstate partners, including those with assistance programs, who collaborated on outreach through information, education, and communication materials.

Leveraged the most widely used local and county channels, and consistently delivered information (e.g., via five to seven interactive radio shows in a 9-month period).

**Amader Kotha Helpline Bangladesh**[158]

Distributed helpline cards to factory workers that are sized to fit in lanyards carrying IDs.

To improve women's access to the helpline, sent voice messages directly to workers' phones to inform them of its existence.

Used detailed step-by-step videos to train operators to be sensitive to labor conditions, to record detailed information accurately, and to follow up with workers as information becomes available.

### Respect the user's lived realities

- Make it appropriate for the target community. Consider cultural and identity differences – such as attitudinal preferences, gender barriers, disability, complainants' relationships or status, and concepts of time management – in both the design and response processes. For example, support women who are especially time-poor by making recourse available 24/7 or outside of local business hours.
- Provide the option for seeking recourse through multiple channels, including the channel users normally use to communicate with the provider.

### Treats complaints equitably

- Provide recourse free of cost. Treat all complaints or enquiries with the same due process, regardless of the complaint's "value," status, or gender or the use.
- Redressal teams should reflect the diversity of the communities they serve, allowing the most marginalized users to access the service with dignity and comfort. For example, providing users with the option to request a woman helpline operator is important in settings where gender barriers restrict interaction.

## C. Predictability of experience

Deliver timely resolution that creates predictability

### Deliver resolution that is swift and helpful

- Filing a complaint should immediately lay out an expected timetable for key process milestones and every effort must be made to resolve it therein.
- Personnel must be trained on the resolution processes. They must remain sensitive and empathetic when dealing with diverse and difficult complaints, and have received adequate training on specialized soft skills to make users feel heard (e.g., gender-sensitivity training).

### Collaborate on the back end via interoperability and track failures

- Prepare a collaborative back end where multiple parties such as governments and providers work together to assign accountability and maximize interoperability (e.g., when users direct a complaint to the wrong contact, it is quickly redirected to the appropriate contact).
- Help users through a product flow that shifts the burden of detection away from the user (e.g., calling users directly instead of them calling a helpline in the event of a transaction failure, automatically reversing transactions when an ATM erroneously dispenses cash).

**AliExpress China Buyer Protection Programme**[159]

Widely used B2B and B2C platforms, such as Amazon, UBER, and ETSY tend to be complex. This complexity poses challenges in implementing effective recourse mechanisms.

An example approach can be found at AliExpress. AliExpress has implemented a dispute resolution process that allows customers to open a direct dispute with the seller, who must settle within 15 days. If recourse from the seller is delayed, the customer is refunded first while an investigation is carried out.

If the dispute is not settled by the seller within 15 days, AliExpress offers free services to act as a mediator.

This is an emerging area in which responsible practices are developing.

### Make the experience predictable

- Let users know what to expect. Clearly document procedures and keep users informed throughout. There should be pathways for common and more serious problems.
- Approve and closely monitor the procedure at a senior management level (such as a Board).
- Minimize biases, especially when using chatbots based on artificial intelligence technologies.

## D. Accountable and engaging

Make accountability central and involve users in improvements

### Make a central and independent resolution process available to the user

- Avoid having users reach out to multiple parties. Simply providing users with the bank or provider's customer service number is not enough. All entities must have the relevant information they need to help the client (e.g., in the event of a transaction failure, information about the timing and amount of payment made should be available to the provider and the bank).
- Make resolution impartial and transparent. There should be a provision for an independent third party for dispute resolution (e.g., national financial ombudsman, dispute resolution services provided by regulators, or industry associations). This information should be shared up front with users at the time of a complaint and when notified of a decision.

### Engage users in dialog to improve the recourse system and the offering itself

- Continually improve the system via regular analysis of the frequency, patterns, and causes of grievances to help anticipate points of failure and prevent the need for recourse. Include regular reporting of complaints data in a standardized format to regulators or supervisors.
- Consult and engage users on the system's design and performance. Investing in efforts to understand user behavior can help improve programs and products for recourse.

**Togo NOVISSI Cash Transfer Programme**[160]

Complaints to the helpline are recorded and analyzed daily to guide the development of FAQs, which are shared through radio and other channels to report back to people.

**Maji Voice Kenya Water Board**[161]

Electronic feedback system enables complaints to be submitted directly to the water company.

The initiative is set up by the Water Services Regulatory Board (which has the legal mandate to protect consumers), in conjunction with the water service boards and all water sector players in Kenya for accountability.

CASE STUDY

# Awaaz Afghanistan

## Hotline for humanitarian cash transfers and other programs

**Awaaz, a toll-free, countrywide hotline for refugees,** internally displaced persons (IDPs), and returnees, has applied the principles of good recourse to improve access and register feedback on aid programs, especially cash transfers. Its success is largely a result of its full-circle communication and practice of sharing user needs and priorities with humanitarian partners to help improve programming. Over a span of 2 years, Awaaz has handled more than 100,000 calls, with request for cash transfer being the second highest reported need. This need had a 96 percent resolution rate on the first call. Awaaz has elevated the global discussion on collaboration between agencies, regulators, and FSPs alike, and has influenced both programmatic and strategic decision-making at the humanitarian programming level, especially on cash transfers.

### Notable features

#### Equal and easy access

- Multilingual operators who speak Dari, Pashto, Urdu, English, and more.
- Open every day with about 50 percent women operators to improve comfort for women given social norms.
- A small fraction of callers exercised the "right to be forgotten" and requested withdrawal of information, indicating a focus on confidentiality and consent.

#### Predictability of experience

- Awaaz shared 100 percent of referrals[162] with relevant partners within an agreed timeline of 24 hours for urgent inquiries and 1 week for non-urgent enquiries.
- Aid partners responded with action points in 86 percent of cases,[163] 75 percent of which were acknowledged within the agreed timeframe.

#### Accountable and engaging

- Awaaz has agreements in which partners must acknowledge a referred case and provide updates within a fixed time, resulting in a strong back end for smooth flow of information to users.
- More than 40 percent of users reported that communication channels with service providers were working well.

## Implementation journey

### 1. User needs assessment and pilot testing

- Surveyed affected populations (IDPs, refugees, returnees) who identified a "hotline" as the preferred channel for recourse on cash transfers and other issues, including for women.
- Early user feedback helped anchor the neutral name Awaaz ("our voice") instead of a name with negative connotations.

### 2. Timely buy-in from senior leadership

- Secured timely buy-in of the humanitarian country team[164] by forming a coordination team to seek approval and demonstrating proof-of-concept from the Iraq IDP call center experience.
- Faced concerns over inability to sustain program, but overcame these via a public launch commitment and demonstration of learning from Iraq.

### 3. Assembling and nurturing the right team

- Recruited a team with specialized skills in information management and quality assurance.
- Operated with a long-term vision, with an overwhelmingly national team and a clear leadership transition plan.
- Secured safe transport to call center for women operators, which was in line with cultural expectations, supporting their careers and staff diversity.

### 4. Building agreements with technical partners and FSPs

- Sought crucial buy-in from technical counterparts, as access to the right information to provide recourse is critical to maintaining Awaaz's reputation.
- This buy-in was captured in four ways: (i) aligning early on design of information flows (field/service level and data protection agreements), (ii) ensuring benefits were mutual and feedback from users helped improve models, (iii) retaining close ties with FSPs to ensure relevant calls were transferred to Awaaz, and (iv) regular meetings and follow-up to build relationships.

### 5. Securing clearances, funding, and launch

- Timely buy-in from senior humanitarian leadership helped reduce government and regulatory clearance for licenses, short code numbers, and equipment imports.
- For launch, secured short-term funding from WFP (5 months) and UNHCR (2 months); later extended with AHF and ECHO coming on board.[165]
- Commenced with a brief pilot and formally launched via press conference with the lead agency and government.

## KEY LEARNINGS

**Hire specialized staff, not just project managers.** Contrary to typical humanitarian program staffing, it is critical to assemble technical staff as seamless information and data-sharing is important in providing real-time recourse to users.

**Account for women's experiences.** For users, cash withdrawal can be linked to abuses of power, such as undue fees, lack of respect, or even sexual abuse. Agents should follow a strict gender sensitivity code of conduct, with referral systems to handle sensitive complaints. For operators, staffing women on a 24/7 hotline posed security and cultural challenges, so Awaaz designed special transport modes.

**Demonstrate that feedback leads to programmatic improvements.** Regularly track holistic data, share analysis publicly (e.g., via a dashboard), and follow up with improvements on program design and operation.

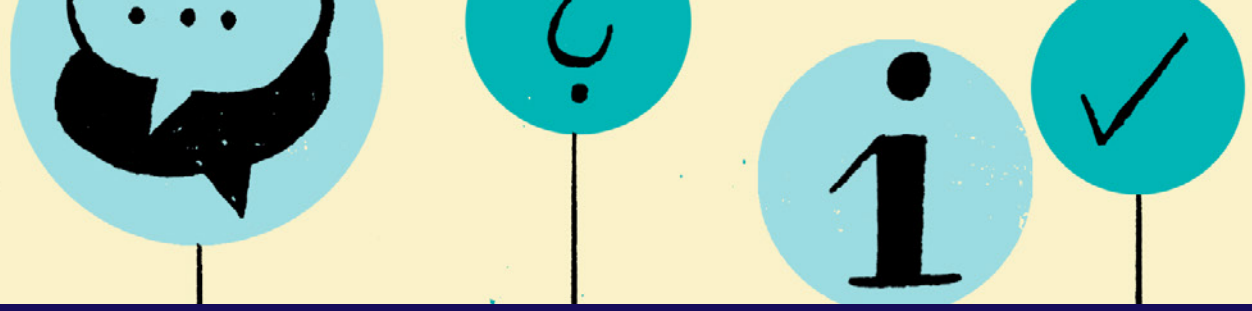
## KEY CHALLENGES

**Short-term funding cycles can hinder planning.** Short cycles, common for humanitarian programs, can make it harder to plan for more intensive and long-term goals. They can also inhibit innovation and collaboration and put the team under pressure.

**Risk of being seen as a universal solution to all grievances.** Awaaz had a clear agreement with the government not to act as the grievance redress mechanism (GRM) for their programs. However, it continued to receive complaints, given its popularity. It is important to ensure clarity in referral pathways.

**Strengthening a recourse system may risk payers or providers becoming lax.** Agencies developed a tendency to rely on Awaaz, even for issues for which Awaaz had no mandate. Clear partner accountability agreements are important to prevent this occurrence.

© WFP/Eoin Casey





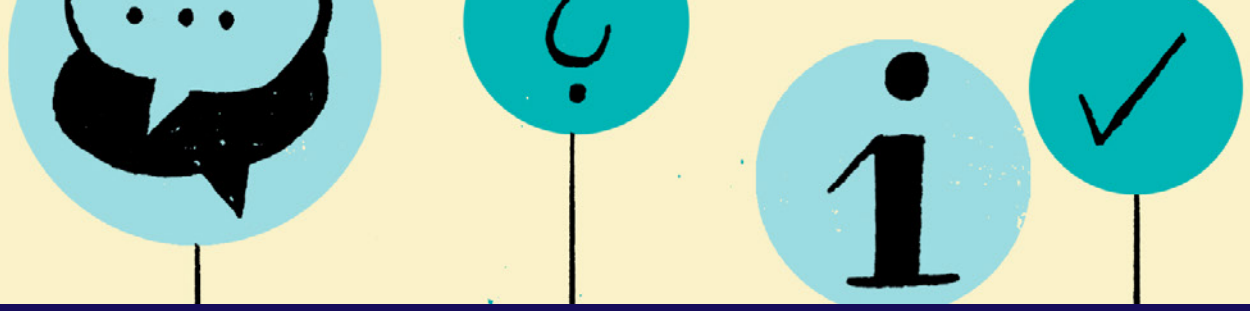
# Recommendations

Governments, companies, and IDOs can **leverage service-level agreements** to include incentives for creating interoperable and responsive recourse mechanisms.

Governments, companies, and IDOs should **ensure grievance mechanisms are toll-free** so users do not need to pay to seek help.

They can **track user feedback and complaints**, including data on frequency, referral rate, resolution status, and transaction failures. Transaction failure data can be monitored to request remedies when providers fall below a specific threshold.

- **Periodic spot checks of recourse mechanism efficacy** should be conducted to discuss feedback and suggest improvements.
- **Partnering with citizen-led initiatives** through innovative community-level campaigns can help to improve grievance resolution.



**Make recourse clear, quick, and responsive**

# Recommendations

## For **GOVERNMENTS**

**Through their different roles, governments can consider how they guide the ecosystem to be more responsive, such as by creating interoperable national or state-level helplines for recourse on G2P, peer-to-government (P2G), and business-to-government (B2G) payments.**

**Governments can support reviews of technology and artificial intelligence use cases, such as chatbots and voicebots, to identify biases and ensure outlier protections.**

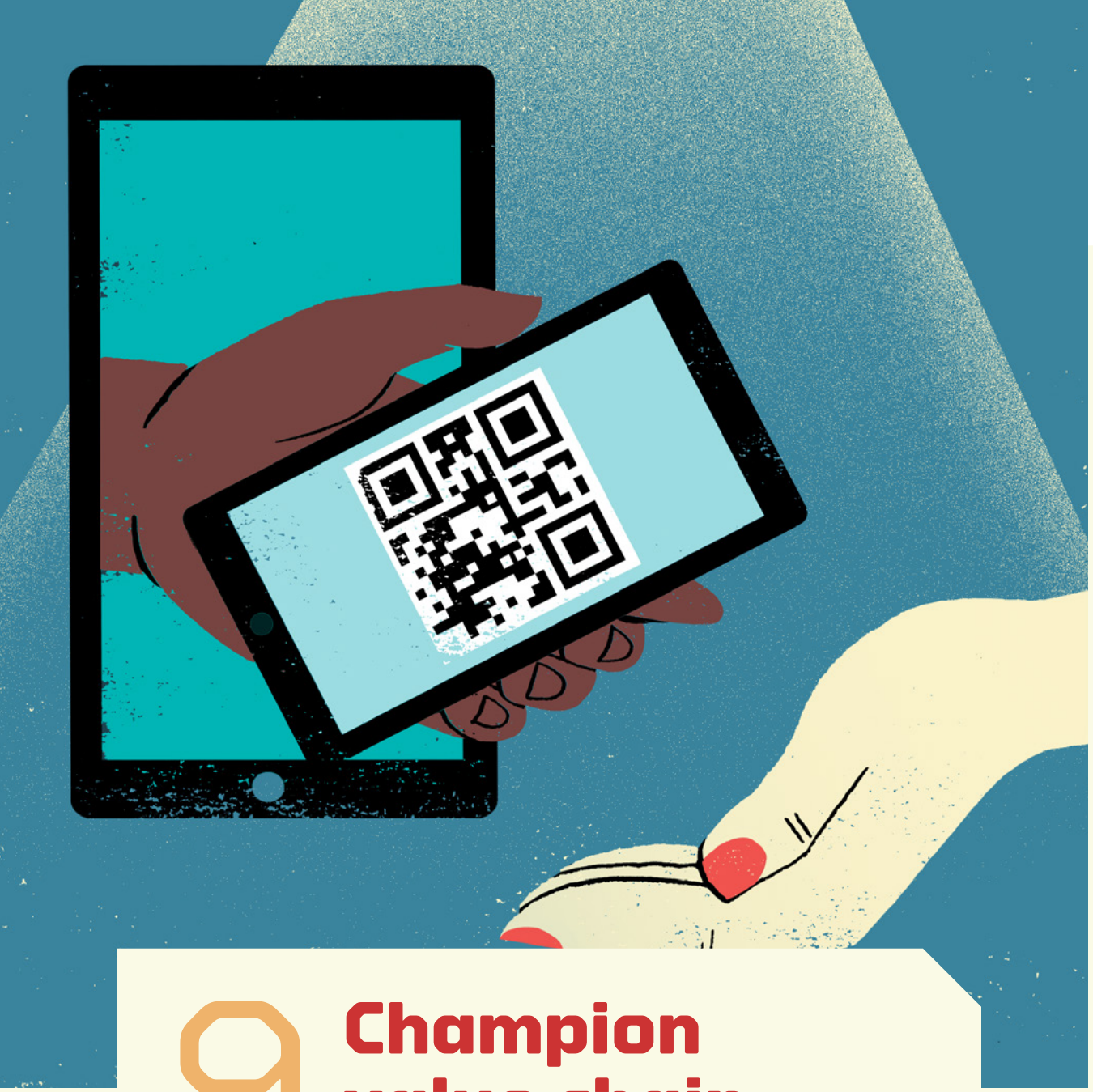
## For **COMPANIES**

**Collaborate through open standards to improve user access and experience, especially for those at risk. Proactively sharing recourse information is essential. This is even more critical for user segments that are at risk. These segments can be identified based on (and at the intersection of) prior exposure to digital payments, gender, age, income, disabilities, etc.**

## For **INTERNATIONAL ORGs**

**IDOs can collaborate with other agencies to share successes in recourse implementation and data on failures.**

**IDOs can provide technical assistance to digital payment partners and civil society on recourse as a key part of their support package.**



PRINCIPLE

# 9 Champion value chain accountability

**Businesses are rushing to digitize payments** throughout their supply chains. Indeed, digital payments have actively disrupted supply chains. Although this underlines some of the key advantages over legacy cash transfers, it also introduces new challenges. For the consumer, ease of use is steadily increasing. Yet, the back end of digital payments is becoming far more intricate.[166]

**Prominent fintech providers (and banks) are experimenting with different roles beyond payment processors. There is a rising number of aggregators built on open APIs. Agents are broadening their influence.[167] As these phenomena grow, the relationships between actors that use digital payments (merchants, suppliers, individuals) and actors that provide or enable these payments (agents, aggregators, banks) are becoming more complex. Transactions now routinely occur across a diverse ecosystem of players and platforms.**

However, in many markets, regulation has not kept pace.[168] The case for promoting responsible digital payments is clear. Many are already applying these principles to their relationships with providers. In most cases, members have delegated providers to oversee responsible behavior from agents, third parties, and others. Accountability from a compliance perspective typically rests with providers, who hold a custodial responsibility over users' funds. From the users' perspective, however, it can often be baffling to identify who is responsible for either detecting or offering recourse for problems. To realize a world in which digital payments are truly better than cash, being reliant solely on statutory provision is insufficient.

Implementation of solutions may continue to sit with providers and enablers. Regardless, it is vital for members to take a holistic approach, expanding their perspectives on responsibility beyond providers to the far reaches of their supply chains. Members can exercise considerable influence to define responsibility and align incentives to ensure all actors operate accordingly. Therein lies the prospect of a world in which responsibility is a shared construct – with stronger user trust, better value propositions, and increased adoption of digital payments.

Research has identified two key issues to address.

### 1. Roles and liabilities are enshrined in some countries' policies but missing or vitiated in others.

Roughly 75 percent of jurisdictions around the world that permit agent relationships have rules in place to hold a financial institution liable for its agents' actions or omissions.[169] More recently, regulations, such as the European Commission's Payments Services Directive (PSD2),[170] are holding registered and licensed providers accountable for any untoward activities by unlicensed partners and "any entity to which activities are outsourced." Furthermore, the General Data Protection Regulation[171] defines how responsibilities are assigned or shared between data controllers and data processors. However, many national regulations have yet to regulate the galaxy of actors that support

and enable digital payments. For example, in Tanzania,[172] a PSP is liable for omissions or errors by their agents but only within the scope of agency agreements. In Indonesia,[173] regulations hold providers liable for mistakes by their management or employees, but do not cover the behavior of agents or other third parties.

### 2. User trust presupposes a responsible ecosystem.

To recant from cash, users must know that any actor they engage with will fulfil their role in a trusted, responsible manner – and will be accountable if they do not.[174] For our members, a breach of this confidence is imbued with reputational risk. Consider a scenario where an agent defrauds a user while providing a cash-out service and the PSP refuses to take accountability. This will not only impact the user's trust in digital payments, but also the relationship with the involved institution.

As digital payments increasingly connect companies, governments, and development organizations with other stakeholders, it is essential that actors assume responsibility for their value chains. Why? Because the intersection of payments value chains with members' own supply chains is complex. It is important for IDOs, governments, and companies to have understanding of the experiential nature of transacting.

The case study highlights a sampling of risks and concerns users face while engaging with types of digital payments. Members should be mindful of these as they leverage influence with providers to promote responsibility.

© Better Than Cash Alliance/ Junarya Photography

**From the users' perspective, it can often be baffling to identify who is responsible for either detecting or offering recourse for problems. To realize a world in which digital payments are truly better than cash, being reliant solely on statutory provision is insufficient.**

# What does responsibility across the value chain look like?

**Responsibility standards across payment value chains are under construction. The coming years will provide salutary lessons for those that follow. To begin, it is important to define what being responsible means - among all actors - and to establish oversight mechanisms.**

## A. Shared understanding

Promote understanding of different actors' roles and responsible behaviors

### Require that all actors be identifiable

- Ensure providers publish a list of authorized agents. Require providers to append the names of any relevant parties to a transaction.[175]
- Document business processes across the user experience and ensure they are updated as the user journey evolves with new products and services. Any changes to this must be updated and shared.[176,177]

### Ensure all actors in the value chain understand responsible behavior

- Invest in training on responsible behavior at each step of the payments journey.
- Provide guidance on what constitutes fair treatment by agents and ensure providers similarly guide agents, especially for excluded groups (e.g., gender sensitivity).[178]
- Review remuneration and commissions to minimize unreasonable incentives (e.g., rewards to agents should not be based on account openings, number of transactions, etc.).

## B. Clear oversight

Ensure oversight across the user journey and define accountability

### Build mechanisms for due diligence and define role-based access[179,180]

- Institute background checks and standard onboarding procedures that are proportional to actors' responsibilities (e.g., similar ID verification as required from users, credit checks to identify vulnerability to bribery, criminal record review regarding fraud, business permits, and references from past engagements).
- Require providers to grant access to data or funds only to the extent that an actor's role demands, along with sufficient encryption to prevent unauthorized access.
- Ensure actors' touchpoints with payments platforms and IT systems are logged and auditable. Develop controls such that a single actor's power is limited (e.g., "four-eyes" maker/checker controls) and regularly reconcile transactions to identify irregularities.

### Define how accountability will be allotted to actors in the value chain

- Ensure providers take responsibility for and continuously monitor all employees, agents, and third party service providers in the value chain. In turn, make sure that users perceive and hold providers as accountable.
- Formalize how the division and overlap of accountability (including potential liability for compensation) is allocated across actors for mistakes, data breaches, and funds losses. Also, formalize definitions for actions such as fraud, corruption, and discrimination.[181]
- Account for new forms of liability arising from new developments around inputs for artificial intelligence (e.g., Singapore's FEAT principles[182]) as well as outsourcing to third parties (e.g., EU's PSD2).[183]

CASE STUDY

# International Rescue Committee

## Collaborations with mobile network operators

© UNICEF

**The International Rescue Committee (IRC) is a non-governmental organization leading global humanitarian aid and relief operations** in 40 countries and over 20 US cities. In 2015, the IRC committed to provide 25 percent of material assistance in cash by 2020, with a secondary goal to escalate the use of digital payments. Four years later, IRC has successfully managed to increase digital payment volumes by almost 15 percent.

In the previous financial year, IRC worked with nine mobile operators in nine countries – Burundi, Cameroon, Chad, Côte d'Ivoire, Jordan, Nigeria, Pakistan, Somalia, and Uganda. To promote responsibility across the value chain, IRC has been strategically leveraging mobile money to provide cash assistance through robust collaborations with mobile network operators (MNOs). Specifically, it provides training and supports users, convenes focus groups, and conducts joint pilots with the mobile financial services (MFS) partners prior to product launch. Such strong partnerships have paved the way for IRC to uphold mutual understanding and responsible behavior of diverse actors across the value chains.

### Notable features

#### Strategic partnerships with MNOs

- Collaborated with MNOs on training and supporting beneficiaries to use services, particularly focused on recourse mechanisms in cases when agents try to misguide or ask for undue payment.
- Conducted joint pilots with the MNO partners prior to full-scale implementation of services.
- Trained IRC staff to manage their services such as initiating payments, using payments dashboard.

#### Anticipating issues and providing timely information to MNOs

- IRC communicated its needs and plans clearly and well in advance; this provided MNOs with the necessary information in a timely manner (client's mobile number, ID, etc.).
- Collaborated with MNOs on key stages in the value chain including communications related to number of agents required, liquidity issues, etc.

### Investment thorough market assessments and hiring experts

- Developed various e-learning courses, by hiring specialized staff, for in-house use.
- Ensured MFS staff were present in regions to provide real-time support to clients, improving their ability to resolve issues.

## Implementation journey

### 1. Organizational commitment

- To meet its ambitious goals to shift to cash assistance and to deliver digitally, IRC had to undergo a significant change management exercise that involved developing new internal priorities, strategies, and processes, and forming new partnerships with MNOs.
- Developed a cash strategy globally and introduced a global payments toolkit (GPT) to establish master service-level agreements with providers of global prepaid cards and e-vouchers; mobile money providers (MMPs) and remittance agencies received training from MFS partners.

### 2. Focused on user needs and constraints

- Product understanding: In Jordan, IRC conducted FGDs focused on:
  - understanding IRC clients' general access to and use of mobile phones
  - evaluating perceptions of the potential benefits and challenges of receiving assistance via mobile money.
- Design suitability: In Pakistan, IRC enabled the Over The Counter (OTC) model to provide access to those who do not have a phone, predominantly women.

### 3. Addressed challenges related to identification

- To address the issue of lack of ID, different approaches were adopted depending on the market:
  - Kenya: Allowed clients to nominate an alternate mobile money recipient and enable consent for KYC; clients were required to confirm receipt of funds.
  - Cameroon: Clients permitted to use another community member's ID (with their permission) to open an account and receive their cash. In Cameroon, the "local authority" and "person who provided the ID," both sign an agreement, with the latter signing a full acknowledgement that they would receive no aid.

### 4. Ensuring successful delivery; learning and evolving

- To ensure better liquidity and recourse, different approaches were adopted depending on the market:
  - In Pakistan: Through MNOs, IRC increased the number of agent locations and improved liquidity to support future disbursements, assisting clients who may not have received a message notifying them of their disbursement.
  - In Kenya: Ensured consumer protection and participation through better recourse including suggestion boxes to collect information, hotlines dedicated to receiving feedback, and complaint management committees.

## KEY LEARNINGS

**IRC's experience has broader impact.** IRC's successful collaboration with MNOs had positive effects for the broader population. In Burundi, the government worked with the same MNOs to facilitate transfers to over 50,000 households in four provinces.

**Sharing responsibility through technical requirements covered in contracts with MFS partners.** IRC focused on including requirements such as MFS providers blocking lost/stolen SIM cards, ensuring providers have data protection policies in place, which played a key role in solving common issues.

**Effective communication with recipients.** IRC has invested more resources in improving accountability systems for improved communication with affected communities.

## KEY CHALLENGES

**Members to help in building a better ecosystem.** To ensure a stronger foundation of a sustained partnership, it is crucial to identify how to meet the long-term aims of both parties, as sometimes partnerships may not be commercially viable for MNOs.

**Building staff skills and ensuring the organization is aligned on the risks of going digital.** Given the risks associated with client data privacy and security, capacity-building is important to ensure both IRC and MNO plus users are aware of the risks and how to mitigate them. IRC mandated this training as company policy across the organization.

### M-Pesa Kenya oversight on agents[184]

M-Pesa agents are recruited by Vodafone after a thorough selection and recruitment process.

They are regularly monitored and trained, and Vodafone representatives revisit them frequently.

**Champion value chain accountability**

# Recommendations

Government, companies, and IDOs can **leverage service-level agreements** to enforce provider responsibility across the digital payments value chain. This approach may include providing users with a unified recourse mechanism.

Members can **conduct assessment of PSPs**, such as periodic spot checks, user ratings of agents, feedback surveys, and mystery shopper activity to suggest improvements.

**Champion value chain accountability**

# Recommendations

## For **GOVERNMENTS**

**Governments can encourage responsibility across the payments value chain and hold providers accountable for the actions of all employees and third parties in instances of losses to users through fraud or technical aberration.**

**Governments can set responsible standards for due diligence, training, and monitoring of third parties.**

## For **COMPANIES**

**Companies such as fast-moving consumer goods (FMCGs) can drive responsibility across supply chain by providing value-add incentives for distributors and merchants, and supporting these stakeholders' digital payments experiences collaboratively.**

**Companies such as global garment brands can invest in new partnerships and investments that result in greater benefits and value-add on top of digital payments accounts for workers in their supply chains.**

## For **INTERNATIONAL ORGs**

**IDOs can optimize their programming to drive systemic change and ensure that actors exhibit responsible conduct:**

- **IDOs can provide guidance on responsible behavior and promote transparency of payments at all times. Invest in capacity-building aimed at ensuring resilient supply chains.**
- **Finance research to inform actors how to promote responsibility across the value chain and ensure greater user trust.**
- **Advocate for regulators to focus on provider liability regarding activities of agents, employees, and other third parties. This might pay special regard to domains related to new technology, fraud, and data breaches.**

# Endnotes


1 Targeting Cash Transfers Within Households, World Bank, 2020

2 Igniting SDG progress through digital financial inclusion, BTCA, 2018

3 Financial Consumer Protection: 3 Steps to Better Customer Outcomes, CGAP, 2020

4 Digital Payments Survey, McKinsey, 2019;

5 Transforming Paradigms, WEF, 2020

6 ACI Worldwide and YouGov survey, 2020

7 Ransomware marketplace report, Coveware, 2020

8 It's Time to Change the Equation on Customer Protection, CGAP, 2019

9 Good Practices for Financial Consumer Protection, World Bank Group, 2017 (examples of countries that make unfair terms void legally include Nigeria, Australia and EU countries)

10 Ministry of Industry and Trade Annual Report, Vietnam, 2019

11 How VISA harnessed data and AI to prevent $25B in fraud, The Machine, 2020

12 Ghana Payment Systems and Services Act, GOG, 2019

13 Detailed Guidance on the Client Protection Principles, Smart Campaign, 2019

14 Detailed Guidance on the Client Protection Principles, Smart Campaign, 2019

15 Pan-Canadian AI Strategy, the first national AI strategy developed by any country, is a research and innovation initiative to strengthen Canada as an AI research hub, 2019

16 CGAP Algorithm Bias in Credit Scoring

17 The EEC Programme was launched by the Government of Pakistan in March 2020 as a welfare measure in response to the COVID-19 lockdown. Emergency cash payments were made largely through digital infrastructure to 17 million families; clause on roaming agents

18 Navigating the shift to digital humanitarian assistance, IRC and GSMA, 2019

19 Making Data Work for the Poor, CGAP

20 Webinar: Public-private collaboration in emergency payments response; Ingreso Solidario website; stakeholder interview

21 HASH number contains the ID and the last four digits of the cell phone number, for those that were in the database. This enables almost an automatic validation when opening a mobile wallet

22 KYC was simplified in which the control and prevention of the general risks and of money laundering is proportional to the limits of balances and transactions that each entity established without exceeding maximum limits (8 SMLV)

23 Doing Digital Finance Right, CGAP, 2015

24 Transaction Failure Rates in the Aadhaar Enabled Payment System, Raghavan, 2020

25 Digital Financial Services – Commonly identified consumer protection themes for digital financial services, International Telecommunication Union, 2019

26 Mobile Money Metrics, GSMA, 2019

27 Assessing risk in digital payments, Bill & Melinda Gates Foundation, 2015

28 G20 High-Level Principles for Digital Financial Inclusion, Principle 4

29 The Power of Smartphone Interfaces for Mobile Money, CGAP, 2015

30 Nigeria's instant payment network is enabled through the Nigeria Inter-Bank Settlement System (NIBSS), a payments switch that allows customers to make real-time payments across all commercial banks, mobile money operators and microfinance institutions in the country, Better Than Cash Alliance, 2015

31 Safeguarding Mobile Money, GSMA, 2016

32 2017 Good Practices for Financial Consumer Protection, Annex A: Retail Payments Services, Sections C8 & C10

33 EU PSD2, Article 95, 97–98

34 Examples include the use of biometrics in India's Aadhaar identification system, and UNHCR's use of iris technology to distribute cash to refugees in Jordan

35 See EU PSD2 Articles 97–98, Ghana's Payments Systems and Service Act, 2019 (section 65(1)), and Malawi's 2019 e-Money regulations (section 17)

36 India Master Direction on Prepaid Payment Instruments, Section 15.3

37 2017 Good Practices for Financial Consumer Protection, Annex A: Retail Payments Services, Sections C8 & C10

38 RappiPay from Rappi, a Colombian on-demand delivery startup, partnered with VISA to offer payment services to Latin American consumers via its QR-based digital

39 2017 Good Practices for Financial Consumer Protection, Annex A: Retail Payments Services, Section C9(d)

40 EU PSD2, Article 96

41 2017 Good Practices for Financial Consumer Protection, Annex A: Retail Payments Services, Section C9(a)

42 India's Unified Payments Interface is an instant real-time payment system developed by the National Payments Corporation of India, enabling real-time, interbank transactions (link)

43 Stakeholder interview; Cobro Digital (CoDi) – Registration Manual, Grupo Financiero Monex, 2019; CoDi: the platform for digital payments in Mexico, Latin America Tech, 2019; 18 million users would adopt Codi for digital transactions, 2020; Global Payments: Spotlight on Mexico, Icon Solutions, 2017

44 Advancing Women's Digital Financial Inclusion, GPFI, 2020; Digital Financial Solutions to Advance Women's Economic Participation, GPFI, 2015

45 Lessons on Enhancing Women's Financial Inclusion using DFS, AFI, 2020

46 The Numbers Don't Lie, Women's World Banking

47 Investing in Women, IFC, 2017

48 Women Empowerment and Economic Development, Esther Duflo, 2012

49 The Economics of Banking on Women, Global Banking Alliance for Women, 2018

50 Financial Literacy Around the World – Insights from Standard & Poor's Financial Literacy Survey, GFLEC, 2017

51 The Mobile Gender Gap Report, GSMA, 2020

52 Advancing Women's Digital Financial Inclusion, GPFI, 2020

53 The Mobile Gender Gap Report, GSMA, 2020

54 Advancing Women's Digital Financial Inclusion, GPFI, 2020; Digital Financial Solutions to Advance Women's Economic Participation, GPFI, 2015

55 Gender Intentional Social Protection in time of COVID-19, BTCA, 2020

56 Advancing Women's Digital Financial Inclusion, GPFI, 2020

57 MTN Loyalty Models in Ivory Coast, Dalberg & CGAP, 2018

58 Privacy on The Line, Dalberg and CGAP, 2016

59 The Human Account, Dalberg and Rockefeller Philanthropy Advisors

60 Advancing Women's Digital Financial Inclusion, GPFI, 2020

61 Privacy on The Line, Dalberg and CGAP, 2016

62 Focus Note: Doing Digital Finance Right, CGAP, 2015

63 Women and Money, IDEO and Bill & Melinda Gates Foundation, 2020

64 MTN Loyalty Models in Ivory Coast, Dalberg & CGAP, 2018

65 Privacy on The Line, Dalberg and CGAP, 2016

66 Superintendency of Banks and Financial Institutions (SBIF) was an autonomous state institution responsible for supervision of banking companies. In 2019, this dissolved to give way to the Financial Market Commission (CMF)

67 Kenya Matrimonial Act, Kenya Law

68 WMBL's Mama Bank is a biometric-based access point serving only women customers to ensure accessible banking considering low literacy levels. In 1 year, their customer base increased by 65 percent.

69 The HUL Shakti program set up in 2001 aimed to empower rural women by engaging them as last-mile retailers for HUL products. In 2020, digital transactions were incorporated onto the system and women entrepreneurs onboarded onto mobile app platforms

70 Digital Financial Solutions to Advance Women's Economic Participation, GPFI, 2015, p. 11 on Agent Banking in Nigeria

71 FAQs are part of the training material for helpline officers around which scripts for supporting clients are built. Stakeholder interview, Amader Kotha website

72 A data controller is the entity that determines "why" and "how" personal data will be processed, and thus bears the majority of obligations under data protection frameworks such as the GDPR. A data processor is an entity – often a third party – which processes data on behalf of the controller, Rules for business and organizations: What is a data controller or a data processor?, The European Commission, 2019

73 Industry-wide Adoption May Be Hard Without Regulatory Push, bwdisrupt.in, 2020

74 India's New Approach to Personal Data Sharing, CGAP, 2020

75 South Africans don't trust companies to protect their data privacy, de Viega, 2019

76 Information privacy practices in e-government in an African least developing country, Rwanda, Mutimukwe et al., 2019

77 Data and privacy unprotected in one third of countries, despite progress, United Nations Conference on Trade and Development, 2020; How More Countries Plan to Pass Stringent Privacy Laws in 2019, Greig, J., Techrepublic, 2019; Forrester's Global Map Of Privacy Rights And Regulations, 2019

78 How to Make Data Work for the Poor, CGAP, 2020

79 Privacy on the Line: What people in India think about their data protection and privacy, CGAP and Dalberg, 2017

80 Behavioral research experiment on end-user data privacy practices completed

81 EU GDPR Article 7, General Data Protection Regulation, 2018

82 EU GDPR Article 7, General Data Protection Regulation, 2018

83 Good Practices for Financial Consumer Protection, Annex A Retail Payment Services, World Bank Group, 2017

84 Created and empowered by the Reserve Bank of India, Account Aggregators (AAs) manage consent requests and serve as the "pipes" through which data flow from banking customers to the users of their financial information, CGAP, 2020

85 Unilever's Shakti program enables rural women around the world to become entrepreneurs in their communities by providing them with training and tools (including a smartphone application) that facilitates access to Unilever's products

86 India's Unified Payments Interface (UPI) is an instant, interoperable payment system developed by National Payments Corporation of India facilitating interbank transactions

87 To automate FSP reporting, Mexico's Comisión Nacional Bancaria y de Valores (CNBV) deployed an API-based reporting tool to directly extract transaction data from FSPs, enabling cost-effective, expansive compliance monitoring

88 Stakeholder interview, Ghana DPC website

89 Illustrative examples include Principle 1 from Smart Campaign's Detailed Guidance on Client Protection Principles, 2019 and Principle 1 from G20 High-Level Principles for Digital Financial Inclusion, 2016

90 Human-Centred Design Is More Important Than Ever, BCG, 2020

91 Illustrative regulations include those in Australia, EU, Hong Kong, South Africa, and the UK, per Product Design and Distribution, World Bank, 2019

92 Financial Inclusion Beyond Access and Usage to Quality, UNSGSA, 2020

93 ICT Facts and Figures 2017, International Telecommunications Union

94 The Global Findex Database 2017, World Bank

95 Product Design and Distribution | Emerging Regulatory Approaches for Retail Banking Products, World Bank, 2019

96 Go-Jek Sparks an Indonesian Banking Revolution, Nikkei Asia, 2018

97 Aspiring Indians I and II, Dalberg, 2019

98 Payments Aspects of Financial Inclusion in the Fintech Era, World Bank, 2020

99 The Role of Digital Financial Inclusion in Preparing for Old Age and Retirement, World Bank and BTCA, 2019 p. 8 on Nudging to save; Ideas42 is a global non-profit organization that uses behavioral sciences to solve complex social problems

100 Aspiring Indians I and II, Dalberg, 2019; How to Create Financial Products that Win with Women, Women's World Banking, 2018

101 User experience and cognitive overload: when less is more, UX Collective, 2020

102 The Power of Smartphone Interfaces for Mobile Money; CGAP, 2016

103 Aspiring Indians, Dalberg, 2018

104 BLC Bank is a for-profit financial institution, which collaborated with IFC's Banking on Women program to design a new customer value proposition for women

105 Inua Jamii is the Kenyan government's flagship National Safety Net Programme to provide cash transfers to vulnerable people

106 Good Practices for Financial Consumer Protection, World Bank, 2017

107 Product Design and Distribution, World Bank, 2019

108 One example from Tanzania is experimental research in the Behavioral Applications to Digital Finance, Busara et al. 2017

109 In 2020 responding to the COVID-19 lockdown, the Ministry of Development and Social Inclusion of Peru launched a welfare scheme transferring about US$223 to 6.8 million vulnerable households (source: stakeholder interview)

110 EjoHeza website, Extending Pension Coverage to the Informal Sector in Africa, World Bank, 2019, and stakeholder interviews

111 Great progress and positive policy outlook on Rwanda's EjoHeza micro-pension scheme, PinboxSolutions, 2019

112 For example, the EU's EBA guidelines require PSPs/banks to fulfill testing obligations before bringing a new or existing product to market by assessing how the product would fit users under a wide range of scenarios including stressed scenarios and modifying product to address poor test results

113 Product Design and Distribution | Emerging Regulatory Approaches for Retail Banking Products, World Bank, 2019

114 Financial Conduct Authority. Occasional Paper No. 1. Applying behavioral economics at the Financial Conduct Authority, 2013

115 Illustrative international standards that cover transparency and disclosure in DFS include the World Bank Group's Retail Payments Good Practices, the G20 High-Level Principles on Digital Financial Inclusion (Principle 5), the Smart Campaign's Client Protection Principles (Principle 3); Illustrative national payments and e-money legislation that cover transparency include Ghana's Payments Act 2019, India's Prepaid Payment Master Direction 2017, Kenya's National payments System Regulations 2014, Indonesia's Consumer Protection in Payments Regulation 2021

116 Detailed Guidance on the Client Protection Principles, The Smart Campaign, 2019

117 Good Practices for Financial Consumer Protection, World Bank Group, 2017; Advancing Women's Digital Financial Inclusion, GPFI, 2020

118 Analysis on the electronic commerce in Latin America and the Caribbean, Mastercard, 2019

119 Payments Aspects of Financial Inclusion in the Fintech Era, World Bank, 2020

120 Whose data is it anyway?, Chartered Institute of Marketing Survey, 2016

121 India's PayTM app in 11 languages

122 Aspiring Indians II, Dalberg, 2019

123 Disclosure and Transparency Lab Testing Tools, CGAP, 2017; Good Practices for Financial Consumer Protection, World Bank Group, 2017

124 Client Protection in Mexico, CFI, 2011

125 It's Time to Change the Equation on Consumer Protection, CGAP, 2019

126 Good Practices for Financial Consumer Protection, World Bank Group, 2017

127 Putting the Principles to Work: Detailed Guidance on the Client Protection Principles, Smart Campaign, 2019

128 Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, Monetary Authority of Singapore, 2018

129 Client Protection Principles, Smart Campaign, 2019

130 Making Data Work for the Poor, CGAP, 2020 and Client Protection Principles, Smart Campaign, 2019

131 Google Privacy Policy – Privacy and Terms

132 Stakeholder interview

133 The Potential of Open Digital Ecosystems, Omidyar Network & BCG, 2020

134 Payment Aspects of Financial Inclusion, Bank of International Settlements, 2016

135 Tracking the journey towards mobile money interoperability, GSMA, 2020

136 Indian Govt Plans To End UPI Monopoly: Google Pay And PhonePe's Loss, Facebook's Gain?, gizbot.com, 2020

137 Global Payment Systems Survey (GPSS), World Bank, 2016

138 What Is Stopping Interoperability Among The MFS?, Mahmud, 2020

139 The Potential of Open Digital Ecosystems, Omidyar Network & BCG, 2020

140 Report on open banking and application programming interfaces, Bank for International Settlements, 2019

141 Tanzania's government created a highly flexible policy framework to guide its push toward interoperable banking. Built on a foundation of global best practices, the policy was customized in consultation with individual service providers, 2014

142 The Association of Southeast Asian Nations (ASEAN) is standardizing quick response (QR) codes across the region, increasing usability and affordability of cross-border payments across its 10 member states, 2019

143 The Potential of Open Digital Ecosystems, Omidyar Network & BCG, 2020

144 Championing interoperability for financial inclusion: carrot or stick?, Lammer et al., 2016

145 In several countries, such as Ghana and Kenya, governments may even go as far as prohibiting agent exclusivity agreements

146 Payments Aspects of Financial Inclusion in the Fintech Era, Bank of International Settlements, 2020

147 The World Food Programme's COVID-19 relief efforts in Bangladesh use blockchain to promote interoperability in cash assistance programmes, 2020

148 Digital Finance Interoperability and Financial Inclusion: A 20-Country Scan, CGAP, 2016

149 The Potential of Open Digital Ecosystems, Omidyar Network and BCG, 2020

150 Singapore has undertaken several initiatives to ensure a citizen-centric approach to service delivery with wide participation from various actors such as businesses, startups, research organizations, and end-users

151 Stakeholder interview, National Payments Corporation of India and the Remaking of Payments in India, CGAP, 2019; Your guide to UPI – the world's most advanced payments system, Wharton Fintech, 2017; India: A Testing Ground for Digital Merchant Payments, CGAP, 2019; The Potential of Open Digital Ecosystems, Omidyar Network, 2020

152 Consumer Protection Survey of Digital Finance Users: Kenya, IPA, 2021; Consumer Protection Survey of Digital Finance Users: Uganda, IPA, 2021

153 RURA is Rwanda's legal body with a mandate to license, monitor, and enforce license obligations, and advise policy on certain public utilities such as telecom, water, gas

154 Digital Payment – Analysing the cyber landscape, KPMG, 2017

155 Use of smartphones and social media is common among most emerging economies, Pew Research Center, 2019

156 How to complain to digital payments ombudsman, Economic Times, 2019

157 Accountability Together is a web-based integrated complaint referral mechanism, which aims to improve accountability and quality of humanitarian aid at community level

158 Amader Kotha Helpline provides garment workers with a timely and effective communication channel to report and resolve safety and other concerns

159 Buyer Protection program of AliExpress, an online retail service of small businesses that sell to international buyers, which ensures protection of buyer's payments and refund

160 NOVISSI cash transfer program provides a direct mobile-based monetary transfer to households affected by the COVID-19 pandemic

161 MajiVoice in Kenya is an electronic feedback system to enable people to easily and conveniently reach their water company through a mobile phone or the internet

162 Referrals are defined as nonstandard calls that are shared with the respective partner for action and feedback, that is, there is no existing standard messaging or partner hotline for the issue

163 "Partners" include clusters and individual agencies. "Partner response" on referrals describes when a partner has indicated nature of referral in terms of possible action to be taken

164 A humanitarian country team is the senior leadership and serves as a strategic, policy-level, and decision-making forum that guides principled humanitarian action in Afghanistan; Awaaz Afghanistan website and stakeholder interview

165 AHF is the Afghanistan Humanitarian Fund, ECHO is the European Civil Protection and Humanitarian Aid Operations; Awaaz Afghanistan website, and dashboard and stakeholder interview

166 Building Inclusive Digital Payments Ecosystems, GPFI, 2017

167 How is the pandemic affecting agents?, CGAP, 2020

168 Digital Economy Report, UNCTAD, 2019

169 Global Financial Inclusion and Consumer Protection Survey, World Bank Group, 2017

170 Payment Services (PSD 2) Directive, European Union, 2015

171 Article 82 (1) states "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered," General Data Protection Regulation, EU, 2018

172 Tanzania Electronic Money Regulations, Regulation 37, 2015

173 Indonesia Regulation on Consumer Protection Payment System, Bank Indonesia, 2014

174 Guidelines on Mobile Money Data Protection, GSMA, 2018

175 Detailed Guidance on Client Protection Principles, Smart Campaign, 201

176 Guidelines on Mobile Money Data Protection, GSMA, 2018

177 Cybersecurity for Financial Inclusion, AFI, 2019

178 Global Financial Inclusion and Consumer Protection Survey, World Bank Group, 2017

179 Guidelines on Mobile Money Data Protection, GSMA, 2018

180 Cybersecurity for Financial Inclusion, AFI, 2019

181 Guidelines on Mobile Money Data Protection, GSMA, 2018

182 Singapore MAS Principles for use of AI

183 EU PSD2 Regulation

184 Vodafone M-Pesa FAQs

# Bibliography


AFI. Cybersecurity for Financial Inclusion: Framework and Risk Guide. 2019.
https://www.afi-global.org/publications/3146/Cybersecurity-for-financial-inclusion-framework-risk-guide

AFI. Lessons on Enhancing Women's Financial Inclusion using DFS. 2020.
https://www.afi-global.org/sites/default/files/publications/2020-05/AFI_WFI_DFS_SR_AW_digital.pdf

Australian Government (The Treasury). Financial System Inquiry Final Report. 2014.
https://treasury.gov.au/publication/c2014-fsi-final-report

Basel Committee on Banking Supervision, Bank for International Settlements. Report on Open Banking and Application Programming Interfaces. 2019.
https://www.bis.org/bcbs/publ/d486.pdf

BIS. Fast payments – Enhancing the speed and availability of retail payments. 2020.
https://www.bis.org/cpmi/publ/d154.pdf

BTCA, WBG. The Role of Digital Financial Inclusion in Preparing for Old Age and Retirement. 2019.
https://www.betterthancash.org/alliance-reports/the-role-of-digital-financial-inclusion-in-preparing-for-older-age-and-retirements

CFI. Handbook on Customer Protection for Inclusive Finance. 2019.
https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/10/Handbook-Consumer-Protection-Inclusive-Finance_FINAL.pdf

CFI. Making Digitization Work for Clients Starts with Client Engagement. 2020.
https://www.centerforfinancialinclusion.org/making-digitization-work-for-clients-starts-with-client-engagement

CFI. Oral Users and Digital Payments: Can Existing Interfaces be Adapted? 2019.
https://www.centerforfinancialinclusion.org/oral-users-and-digital-payments-can-existing-interfaces-be-adapted

CGAP. Customer Outcomes to Strive For. 2020.
https://www.cgap.org/research/slide-deck/customer-outcomes-strive

CGAP. Digital Cash Transfers in Times of COVID-19. 2020.
https://www.cgap.org/research/publication/digital-cash-transfers-times-covid-19-opportunities-and-considerations-womens

CGAP. Digital Finance Interoperability & Financial Inclusion: A 20-Country Scan. 2016.
https://www.cgap.org/sites/default/files/interoperability.pdf

CGAP. Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks. 2015.
https://www.cgap.org/sites/default/files/researches/documents/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf

CGAP. It's Time to Change the Equation on Consumer Protection. 2019.
https://www.cgap.org/blog/its-time-change-equation-consumer-protection

CGAP. Kenya Ends Hidden Costs for Digital Financial Services. 2016.
https://www.cgap.org/blog/kenya-ends-hidden-costs-digital-financial-services

CGAP. Kenya's Rules on Mobile Money Price Transparency Are Paying Off. 2018.
https://www.cgap.org/blog/kenyas-rules-mobile-money-price-transparency-are-paying

CGAP. Making Consumer Protection Regulation More Customer-Centric. 2020.
https://www.cgap.org/sites/default/files/publications/2020_06_WorkingPaper_Making_Consumer_Protection_Regulation_More_Customer_Centric.pdf

CGAP. Making Data Work for the Poor: New Approaches to Data Protection and Privacy. 2020.
https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf

CGAP. Module 1: Introduction to Behavioral Policy Making. 2018.
https://www.cgap.org/sites/default/files/publications/slidedeck/Module%201.pdf

CGAP. Module 2: Disclosure and Transparency / Lab Testing Tools. 2017.
https://www.cgap.org/sites/default/files/publications/slidedeck/Module%202.pdf

CGAP. Module 5: Financial Capability. 2018.
https://www.cgap.org/sites/default/files/publications/slidedeck/module5-updated.pdf

CGAP. Recourse in Digital Financial Services: Opportunities for Innovation. 2016.
https://www.cgap.org/sites/default/files/researches/documents/Brief-Recourse-in-Digital-Financial-Services-Dec-2015.pdf

CGAP. Smartphones and Mobile Money: Principles for UI/UX Design (1.0).
https://www.cgap.org/research/slide-deck/smartphones-and-mobile-money-principles-uiux-design-10

CGAP. Financial Consumer Protection: 3 Steps to Better Customer Outcomes.
https://www.cgap.org/blog/financial-consumer-protection-3-steps-better-customer-outcomes

Dalberg, CGAP. Privacy on the Line: What people in India think about their data protection and privacy. 2017.
https://dalberg.com/wp-content/uploads/2017/11/Privacy-On-The-Line-Final-161117_1.pdf

Dalberg, Bill & Melinda Gates Foundation. Aspiring Indians I and II. 2019.
https://dalberg.com/our-ideas/aspiring-indians-new-public-data-set-and-tool-improving-financial-health-india-launched/

Dalberg, Rockefeller Philanthropy Advisors, Bill & Melinda Gates Foundation. The Human Account. 2018.
https://www.thehumanaccount.com/

European Union Information Commissioner's Office. Guide to the GDPR. 2019.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

European Union: PSD2 Directives on Payments Services. 2015.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366

Financial Conduct Authority. Occasional Paper No 1: Applying behavioural economics. 2013.
https://www.fca.org.uk/publication/occasional-papers/occasional-paper-1.pdf

Forrester's Global Map Of Privacy Rights And Regulations, 2019
https://www.forrester.com/report/Forresters+Global+Map+Of+Privacy+Rights+And+Regulations+2019/-/E-RES141638?utm_source=blog&utm_medium=social&utm_campaign=research_social&utm_content=Iannopollo_141638

G20, OECD. High-Level Principles on Financial Consumer Protection. 2011.
http://www.oecd.org/daf/fin/financial-markets/48892010.pdf

G20. Financial Inclusion for Women: A Way Forward. 2018.
https://www.g20-insights.org/policy_briefs/financial-inclusion-for-women-a-way-forward/

G20. High-Level Principles for Digital Financial Inclusion. 2016.
https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion

Gates Foundation, IDEO. Women and Money. 2020.
https://static1.squarespace.com/static/5d94e54cb06c703e5199d288/t/5ddd853c238a18316c54b560/1574798673537/Women_Money_Global_Report_11.26.pdf

Gates Foundation. Assessing risk in digital payments. 2015.
https://docs.gatesfoundation.org/documents/Assessing%20risk%20in%20digital%20payments%20FSP.pdf

GPFI. Achieving Development and Acceptance of Open and Inclusive DP Infrastructure. 2020.
https://www.gpfi.org/sites/gpfi/files/documents/BTCA-GPFI-OpenInclusivePayments-.pdf

GPFI. Advancing Women's Digital Financial Inclusion. 2020.
https://www.gpfi.org/sites/gpfi/files/sites/default/files/saudig20_women.pdf

GPFI. Building Inclusive Digital Payment Ecosystems: Guidance Note for Governments. 2017.
https://www.gpfi.org/sites/gpfi/files/documents/GPFI%20Guidance%20Note%20Building%20Inclusive%20Dig%20Payments%20Ecosystems%20final_0.pdf

GPFI. Digital Financial Solutions to Advance Women's Economic Participation. 2015.
https://www.gpfi.org/sites/gpfi/files/documents/03-Digital%20Financial%20Solution%20to%20Advance%20Women....pdf

GSMA. Guidelines on Mobile Money Data Protection. 2018.
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Guidelines-on-mobile-money-data-protection.pdf

GSMA. Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected. 2016.
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf

GSMA. The Mobile Gender Gap Report. 2020.
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf

GSMA. The pivotal role of mobile money agents in driving financial inclusion. 2019.
https://www.gsma.com/mobilefordevelopment/blog/the-pivotal-role-of-mobile-money-agents-in-driving-financial-inclusion/

GSMA. Tracking the journey towards mobile money interoperability: Emerging evidence from six markets: Tanzania, Pakistan, Madagascar, Ghana, Jordan and Uganda. 2020.
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/06/GSMA_Tracking-the-journey-towards-mobile-money-interoperability-1.pdf

IFC Compliance Advisor Ombudsman. Guide to Designing and Implementing Grievance Mechanisms for Development Projects. 2020.
http://www.cao-ombudsman.org/howwework/advisor/documents/implemgrieveng.pdf

IFC. Investing in Women: New Evidence for the Business Case. 2017.
https://www.ifc.org/wps/wcm/connect/ac8fca18-6586-48cc-bfba-832b41d6af68/IFC+Invest+in+Women+October+2017.pdf?MOD=AJPERES&CVID=lYLVAcA

IFC. Partnership for Financial Inclusion: Interoperability (Tanzania). 2014.
https://www.ifc.org/wps/wcm/connect/region__ext_content/ifc_external_corporate_site/sub-saharan+africa/priorities/financial+inclusion/interoperability

IMF. The Bali Fintech Agenda Policy Paper. 2018.
https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda

International Network Financial Ombudsman Schemes Essential Approaches to Fundamental Principles. 2015.
http://www.networkfso.org/introduction.html

International Telecommunication Union. Commonly Identified Consumer Protection Themes for Digital Financial Services. 2016.
https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf

Journal of Money Laundering Control. Control of fraud on mobile money services in Ghana: an exploratory study. 2019.
https://www.emerald.com/insight/content/doi/10.1108/JMLC-03-2018-0023/full/html?skipTracking=true

MasterCard, Deloitte. Economic impact of real-time payments. 2019.
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-economic-impact-of-real-time-payments-report-vocalink-mastercard-april-2019.pdf

Mastercard, The Global Data Responsibility Imperative white paper. 2019.
https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf

McKinsey. Digital Payments Survey: Are convenience and rewards leading to a digital flashpoint? 2019.
https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/banking%20blog/are%20convenience%20and%20rewards%20leading%20to%20a%20digital%20flashpoint/mckinsey-2019-digital-payments-survey.ashx

MicroSave Consulting. Working Together to fight DFS Fraud. 2016.
https://www.microsave.net/2016/11/07/working-together-to-fight-dfs-fraud/

OECD. Financial Consumer Protection Approaches in the Digital Age. 2018.
https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf

OECD. Improving online disclosures with behavioural insights. 2018.
https://www.oecd.org/sti/consumer/policy-note-improving-online-disclosures-behavioural-insights.pdf

Office of the Privacy Commissioner of Canada. Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act. 2016.
https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

Omidyar Network, BCG. The Potential of Open Digital Ecosystems. 2020.
https://opendigitalecosystems.net/pdf/ODE-Report.pdf

Omidyar Network, Deloitte. Unlocking the Potential of India's Data Economy: Practices, Privacy and Governance. 2019.
https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/Privacy_and_Data_Ethics-A_Roadmap_for_India_Report_V4.pdf

Omidyar Network. Ethical OS Toolkit. 2018.
https://ethicalos.org/wp-content/uploads/2018/08/Ethical-OS-Toolkit-2.pdf

Privacy by Design. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. 2011.
https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Responsible Finance Forum. Big Data, Financial Inclusion and Privacy for the Poor. 2016.
https://responsiblefinanceforum.org/big-data-financial-inclusion-privacy-poor/

Responsible Finance Forum. Evidence and Innovation for Scaling Digital Finance. 2015.
https://responsiblefinanceforum.org/wp-content/uploads/2017/03/Evidence-and-Innovation-for-Scaling-Inclusive-Digital-Finance-Responsible-Finance-Forum-VI.pdf

The Economist. Mobile Money in Africa: Promises and Perils. 2016.
https://financialservices.mazars.com/wp-content/uploads/2016/05/FS-Digital-campaign-2016_-EIU-Mazars_Mobile-money-in-Africa-Article_WEB.pdf

The Smart Campaign. Putting the Principles to Work: Detailed Guidance on the Client Protection Principles. 2019.
https://www.centerforfinancialinclusion.org/research/consumer-protection

UN Report of Secretary-General: Roadmap for Digital Cooperation. 2020.
https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

UN Women. Leveraging Digital Finance for Gender Equality and Women's Empowerment. 2019.
https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2019/leveraging-digital-finance-for-gender-equality-and-womens-empowerment-en.pdf?la=en&vs=4715

UNCTAD. Digital Economy Report. 2019.
https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

UNDP. Supplemental Guidance on Grievance Redress Mechanisms. 2017.
https://info.undp.org/sites/bpps/SES_Toolkit/SES%20Document%20Library/Uploaded%20October%202016/UNDP%20SES%20Supplemental%20Guidance_Grievance%20Redress%20Mechanisms.pdf

UNSGSA. Financial Inclusion Beyond Access and Usage to Quality. 2020.
https://www.unsgsa.org/sites/default/files/resources-files/2020-10/UNSGSA_2020_Annual_Report_Digital.pdf

USAID. Fintech Partnerships Checklist: Identifying and Strengthening the Right Digital Finance Partner. 2017.
https://www.usaid.gov/sites/default/files/documents/15396/USAID_-_Checklist_for_Fostering_Private_Sector_Investment_in_Digital_Finance.pdf

Women's World Banking. How to Create Financial Products that Win with Women. 2018.
https://www.womensworldbanking.org/insights-and-impact/how-to-create-financial-products-that-win-with-women/

Women's Financial Inclusion Data Partnership. The Way Forward: How Data Can Propel Full Financial Inclusion for Women. 2020.
https://data2x.org/wp-content/uploads/2019/08/The_Way_Forward.pdf

WBG, Bank for International Settlements. Payment Aspects of Financial Inclusion in the Fintech Era. 2020.
https://www.bis.org/cpmi/publ/d191.pdf

WBG, Bank of International Settlements. Payment Aspects of Financial Inclusion Report. 2016.
http://documents1.worldbank.org/curated/en/806481470154477031/pdf/107382-WP-REPLLACEMENT-PUBLIC-PAFI-Report-final-in-A4.pdf

WBG, George Washington University. Financial Literacy Around the World: Insights from Standard & Poor's Global Financial Literacy Survey. 2016.
https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x38887

WBG. Brief – Deposit Insurance and Digital Financial Inclusion. 2016.
https://openknowledge.worldbank.org/handle/10986/25707

WBG. Championing interoperability for financial inclusion: carrot or stick? 2016.
https://blogs.worldbank.org/psd/championing-interoperability-financial-inclusion-carrot-or-stick

WBG. Complaints Handling within Financial Services Providers: Principles, Practices, and Regulatory Approaches. 2019.
http://documents1.worldbank.org/curated/en/773561567617284450/pdf/Complaints-Handling-within-Financial-Service-Providers-Principles-Practices-and-Regulatory-Approaches-Technical-Note.pdf

WBG. Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting. 2018.
http://documents1.worldbank.org/curated/en/677281542207403561/pdf/132035-WP-FCP-New-Forms-of-Data-Processing.pdf

WBG. Global Financial Inclusion and Consumer Protection (FICP) Survey. 2017.
https://www.worldbank.org/en/topic/financialinclusion/brief/ficpsurvey

WBG. 2017 Good Practices for Financial Consumer Protection. 2017.
https://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection

WBG. RAI Knowledge into Action Notes: Grievance Redress Mechanisms. 2018.
https://olc.worldbank.org/content/rai-knowledge-action-notes-grievance-redress-mechanisms

WBG. Payment Systems Worldwide: A Snapshot – Summary Outcomes of the Fifth Global Payment Systems Survey. 2020.
http://documents1.worldbank.org/curated/en/115211594375402373/pdf/A-Snapshot.pdf

WBG. Product Design and Distribution: Emerging Regulatory Approaches for Retail Banking Products. 2019.
https://documents.worldbank.org/en/publication/documents-reports/documentdetail/993431567620025068/product-design-and-distribution-emerging-regulatory-approaches-for-retail-banking-products-discussion-note

WBG. Public Sector-Operated Price Comparison Websites: Case Studies and Good Practices. 2013.
https://openknowledge.worldbank.org/bitstream/handle/10986/15978/787830REVISED00price.comparison.eng.pdf?sequence=1&isAllowed=y

WBG. Social Protection & Jobs: Extending Pension Coverage to the informal Sector in Africa. 2019.
http://documents1.worldbank.org/curated/en/153021563855893271/pdf/Extending-Pension-Coverage-to-the-Informal-Sector-in-Africa.pdf

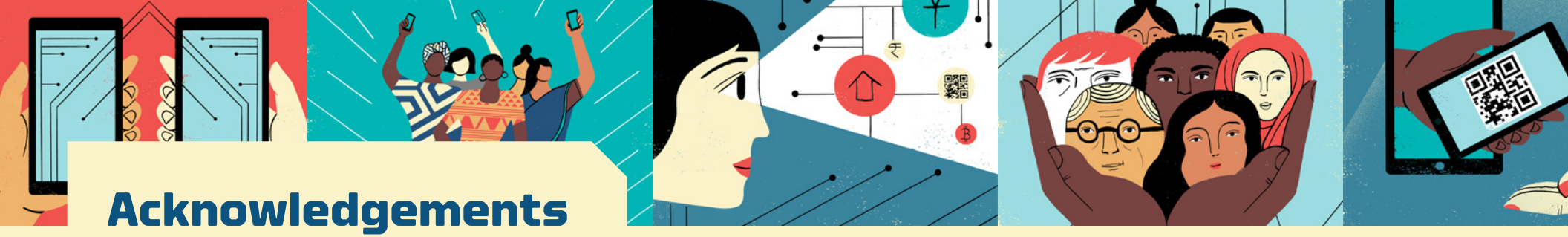
WBG. Using Big Data to Expand Financial Services: Benefits and Risks. 2019.
https://olc.worldbank.org/system/files/Using-Big-Data-to-Expand-Financial-Services-Benefits-and-Risks.pdf

WBG. Women, Business and the Law. 2020.
https://openknowledge.worldbank.org/bitstream/handle/10986/32639/9781464815324.pdf

WBG. The Global Findex Database 2017.
https://globalfindex.worldbank.org/

World Development Report 2021: Data for Better Lives.
https://www.worldbank.org/en/publication/wdr2021

World Economic Forum, University of Cambridge. Transforming Paradigms: A Global AI in Financial Services Survey. 2020.
http://www3.weforum.org/docs/WEF_AI_in_Financial_Services_Survey.pdf



# Acknowledgements


## The Secretariat Team

Team Leads: Keyzom Ngodup Massally and Camilo Tellez.

Team: Sajib Azad, Marjolaine Chaintreau, Tanu Chhabra Bahl, Angela Corbalan, Gisela Davico, Fareeza Ibrahim, Oswell Kahonde, Raza Matin, Jean Pascal Mvondo, Lucy Nshuti Mbabazi, Mia Ryan, Prerna Saxena, Shruti Sharma, Isvary Sivalingam, and Tidhar Wald

The UN Principles for Responsible Digital Payments* were developed by the United Nations-based Better Than Cash Alliance, guided by its member governments, companies and international organizations. The Secretariat Team would like to thank members for their bold leadership in responsible payment digitization practices and their insightful contributions to these Principles. This flagship resource responds to the UN Secretary General's Roadmap for Digital Cooperation.

This report benefited from the strategic direction of Dr. Ruth Goodwin-Groen, Managing Director of the Alliance. We are grateful to Angela Corbalán and the Alliance Communications & Advocacy Team for their invaluable contributions.

This report would not have been possible without the significant contribution from our members, the Executive Committee, the Editorial and Publications Committee.

We would also like to express our gratitude to our Editorial and Publications Committee (EPC) in helping us to deliver this work with sufficient clarity, depth, and breadth - Maria May (Bill & Melinda Gates Foundation), Loretta Michaels (independent), Bjørn Skjelbred (Vipps), Daniel Schwartz (MasterCard Worldwide), Amina Tirana (Visa Inc.), Stella Klemperer (Flourish), Harish Natarajan (World Bank), and Paul Nelson (USAID - Chair of EPC).

We would like to thank our Executive Committee (EXCOM) for providing us with strategic guidance - Kabir Kumar (Flourish), Fernando Maldonado (USAID), Ravi Aurora (MasterCard Worldwide), Amina Tirana (Visa Inc.), and Michael Wiegand (Bill & Melinda Gates Foundation - Chair of EXCOM).

We would like to recognize the thorough technical review and the thoughtful insights shared by Loretta Michaels, Ros Grady, David Medine, and Bob Annibale. Their guidance and steering helped significantly improve this report. We would also like to thank Vikram Sinha (IDFC Institute) and Subhashish Bhadra (Omidyar Network) for their peer review, and Rafe Mazer (IPA) and William Blackmon (IPA) for providing relevant data.

The Alliance would like to express gratitude to Dalberg, a technical partner commissioned by the Alliance to help conduct research - particularly Vineet Bhandari and Swetha Totapally, who contributed with their insights as well as to the research, analysis, and writing of our members' and partners' experiences.


** The name does not mean all UN member states endorsed or committed to follow this set of principles, which are for guidance purposes only. This resource was developed by the United Nations-based Better Than Cash Alliance, responding to the UN Secretary General's Roadmap for Digital Cooperation, and UN leaders added their voices in support of these responsible practices for payment digitization.*

ISBN 978-1-946173-35-5

BETTER THAN CASH ALLIANCE

## About The Better Than Cash Alliance

The Better Than Cash Alliance is a partnership of governments, companies, and international organizations that accelerates the transition from cash to digital payments in order to reduce poverty and drive inclusive growth. Based at the United Nations, the Alliance has over 75 members, works closely with other global organizations, and is an implementing partner for the G20 Global Partnership for Financial Inclusion.