March 2022

Author

Alexandra Rizzi

Responsible Social Protection: Lessons from COVID-19 Digital Cash Transfers

CENTER for FINANCIAL INCLUSION | ACCION

Acknowledgements

CFI completed this work as part of our partnership with the Mastercard Center for Inclusive Growth.

A special mention to Tanwi Kumari for her substantial contributions to the research and writing of this paper. The research for this paper would not have been possible without the assistance of Alejandra Chavarria. Special thanks to Lauren Braniff, Mayada El-Zoghbi, Loretta Michaels, and Evelyn Stark for comments, advice, and guidance on this work. We'd also like to thank all those who we interviewed for their time and openness to share on this topic.

Introduction

In the first quarter of 2020, when governments realized the extent to which COVID-19 had spread across the globe, they took unprecedented and rapid steps to slow its spread. The unintended yet inevitable consequence was that economic activity froze as in-person activities were shut down, and the impacts were particularly severe for people at lower income levels. Livelihoods vanished overnight, requiring economic relief for billions of people. By May 2021, the number of social assistance responses by governments worldwide had exploded to 1,841 as compared with 103 identified in March 2020, reaching more than 1.5 billion people.[i] [ii] Many programs leveraged digital infrastructure to deliver funds quickly, without physical contact, and to reduce the risks associated with cash distribution. This massive relief effort required opening accounts for those not previously included, resulting in new account numbers at scales never seen before — 1.5 million new mobile wallets in Paraguay, 500,000 mobile wallets in Jordan, 35 million digital savings accounts for previously unbanked Brazilians (far more accounts were opened) and 700,000 new digital accounts in Colombia, to name a few.[1] [iii] [iv]

New account numbers at scales never seen before:

1.5 million
New mobile wallets in Paraguay

500,000
New mobile wallets in Jordan

35 million
Digital savings accounts for previously unbanked Brazilians

700,000
New digital accounts in Colombia

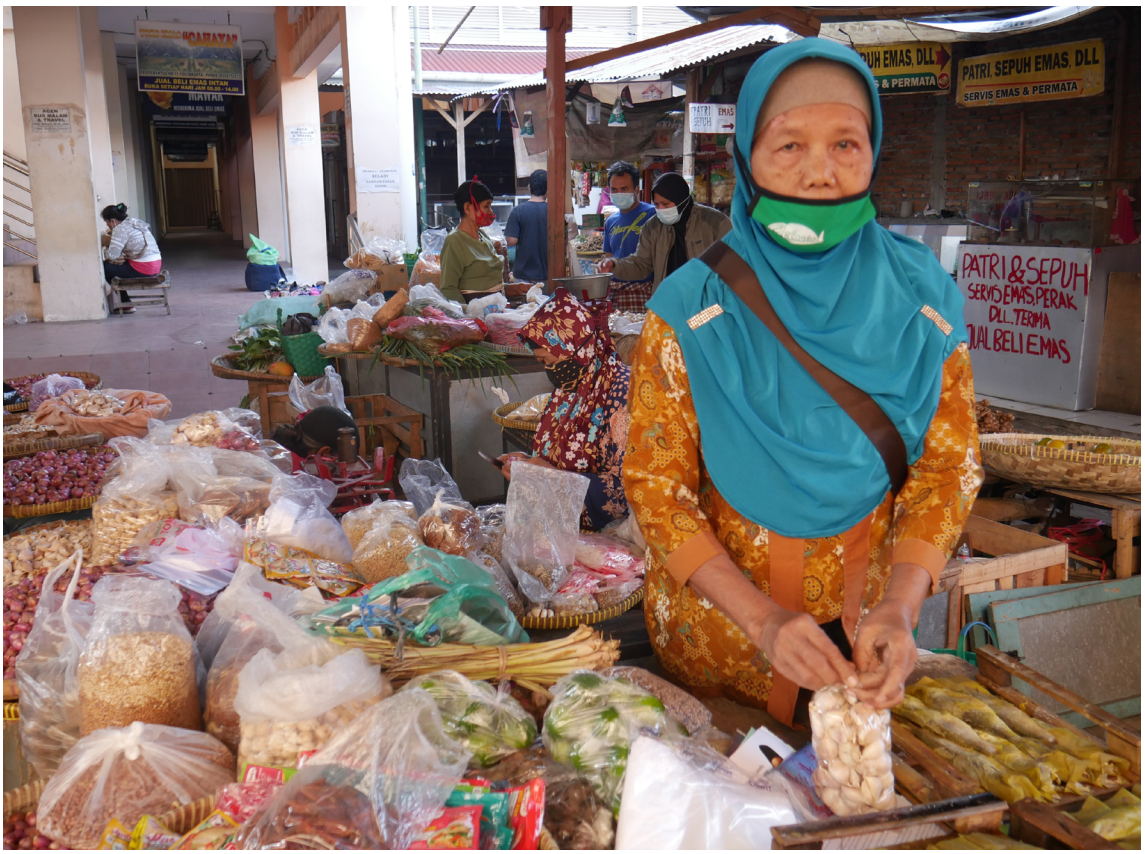
The rapid deployment of government to person (G2P) social protection payments because of COVID-19 demonstrated the extent to which these schemes increasingly rely upon a country's digital financial ecosystem — from interoperable payments infrastructure to digital IDs, partnerships with commercial payment and financial service providers (and their agent networks), and collaboration with mobile network operators. When things went well, the payments were made seamlessly and helped ease the economic burden of the pandemic. But when things did not, it was consumers who bore the brunt. Many were unable to apply for relief because they lacked internet access, proper documents, or they had been a victim of identity theft. Long lines and illiquid cash out points, as well as hotlines jammed with calls and interminable wait times without resolution also posed challenges for those attempting to apply for relief. These challenges end up harming vulnerable people, dampen public trust in such programs, and effectively reduce the intent of G2P protection schemes.

Drawing on the lessons learned from the pandemic, governments, donors, and other humanitarian groups have an opportunity to improve delivery and reduce consumer risks in future G2P program design and rollout. End-to-end program design, clear accountability across multiple service providers, and consumer-friendly redressal

1 N.B. In general, Sub-Saharan African governments were more likely to use mobile money accounts while Latin America and South Asia leveraged traditional bank accounts more heavily.

systems are critical elements of successful G2P systems. And given how inextricably linked future G2P programs will likely be with their countries' digital financial services ecosystem, such improvements might also have positive effects for consumers beyond those receiving government payments. There are also important considerations around data governance that governments need to start addressing sooner rather than later.

This report is the fourth in a series of notes looking at how economic policies enacted around COVID-19 in emerging markets and developing economies (EMDEs) have impacted low-income users and the financial service providers that serve them. It is a companion piece to CFI's December 2020 report Rapid Response for Social Payments During COVID-19, which maps out ways governments enabled rapid payments to those without existing accounts. The findings in this note come from literature review as well as key informant interviews conducted between June and September 2021. This research focused on uncovering consumer risks arising from the rapidly digitizing G2P programs aimed at the most vulnerable in society, most of whom have no prior experience with digital technology or the formal financial system. The literature review examined policy and research that captured the implementation of rapidly digitalized social protection programs, with a focus on the recipient experience. Given the recent (and even ongoing) nature of many of the programs, the literature review included less-formal sources including industry webinars. The team also conducted 20 key informant interviews with a range of stakeholders including experts in global social protection, consumer protection, and payments, as well as market actors such as governments, consumer organizations, and industry bodies in India, Nigeria, Ghana, Pakistan, Bangladesh, the Philippines, Colombia, and Brazil.



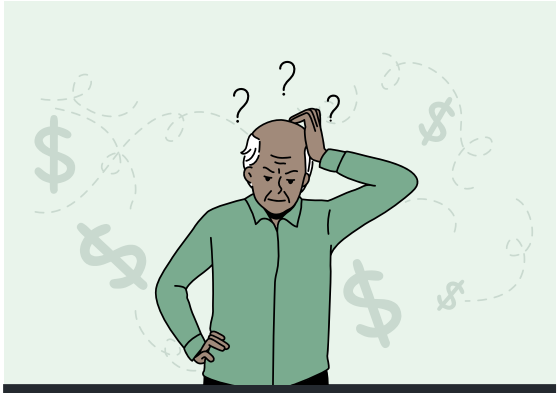
G2P Program Design Can Exacerbate Consumer Risk

The decision of many governments to rapidly digitalize and expand their G2P programs was understandable given the urgent need and the health concerns around in-person distribution. The rushed deployments, however, in some cases resulted in inappropriate or unsuitable program design that left many people confused. Essentially, governments put programs in place that were designed top-down versus bottom-up. The result was complex programs that weren't well-thought-out from the perspective of low-income, low-literacy individuals.

Recipients were confused and frustrated, and in many cases civil society organizations (CSOs) had to step in to help people navigate the systems. It would have been far better to engage the CSOs and other relevant organizations from the beginning to help design the programs. It also would have been beneficial to work early on with payment service providers (PSPs), as they have a strong understanding of the various elements and costs of payments distribution — from account opening to cash handling and customer service. Due to the need for rapid distribution, governments often missed critical elements, such as functional grievance redressal and recourse systems, and factoring in PSP costs, even though governments relied heavily on the PSPs. Recipients ended up incurring costs to enroll and fix problems (including travel costs). Reducing and/or eliminating transaction fees only exacerbated the problem for PSPs, especially those in rural areas.

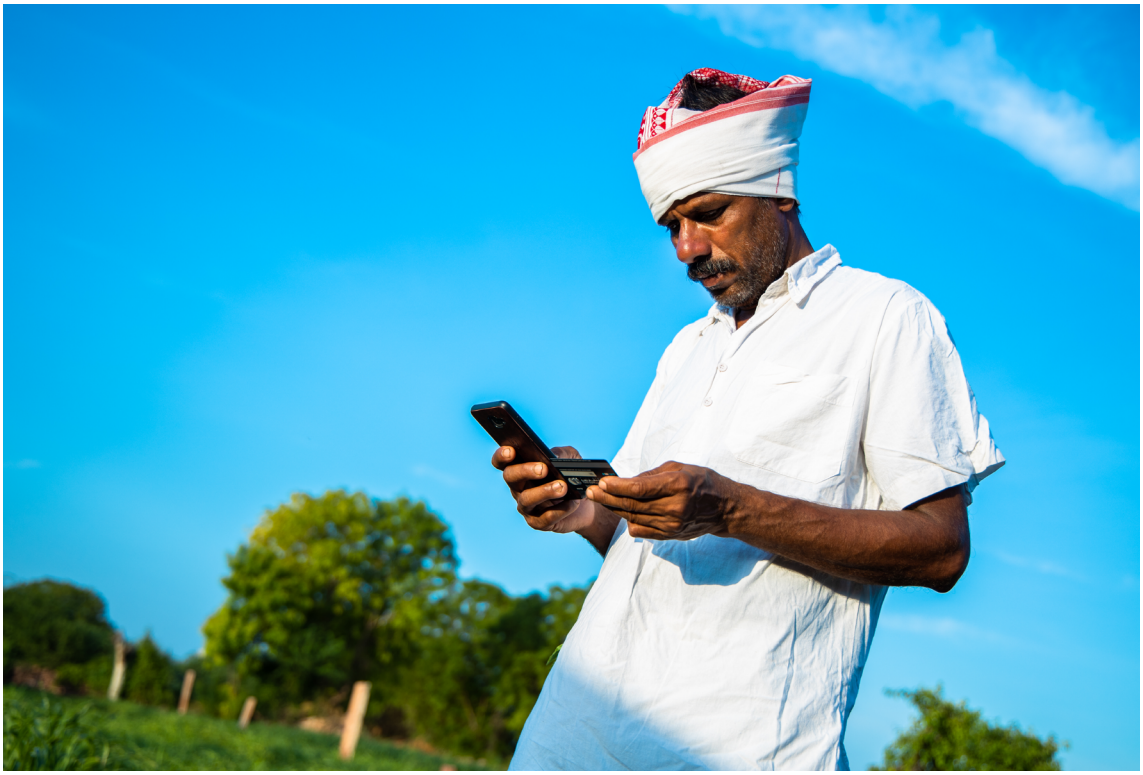
While most governments did an admirable, even heroic, job of putting digital G2P programs in place under COVID, there were still aspects of the programs that resulted in unintended consumer risk and harm. Some of the key issues observed include the following:

- **Communications campaigns were often confusing.**
  In most countries, multiple programs were announced in quick succession, targeting different groups and confusing the public. It was unclear to the different customer groups which programs were aimed at customers of banks versus non-bank financial institutions (NBFIs). At the same time, programs employed both push and pull strategies for enrolling people, further adding to the confusion. Finally, many people were unaware that they had even received payments or how they should retrieve them, leading to overcrowding at bank branches during lockdown conditions.



The rushed deployments, however, in some cases resulted in inappropriate or unsuitable program design that left many people confused.

- **Notification methods de facto excluded many eligible people.**
  In many markets, citizens were notified of their eligibility or invited to apply for benefits via websites, apps, or other digital



channels — which excluded customers with less access to or awareness of technology. For example, in Brazil, website and mobile-based platforms were created for Auxílio Emergencial relief applications. While they contributed to the reach of the program, it was estimated that at least 7.4 million Brazilians were excluded due to lack of internet access.[v] [vi] The Togolese government required citizens to have a SIM card to receive a Novissi payment, despite the fact that a 2019 survey showed that 47 percent of women and 21 percent of men reported they did not own a mobile phone.[vii] [2]

↗ Digital capabilities required for onboarding limited consumer choices.

Registration and onboarding often required capabilities that many first-time recipients did not have. For instance, registering for Togo's Novissi program required entering some basic information on a USSD platform — researchers estimated that 72 percent of those who attempted registration succeeded, with the average successful registration requiring four attempts.[viii] This was exacerbated by an environment where in-person assistance or handholding for new users was not possible and even discouraged due to health concerns.[ix] Even with simplified due diligence, the onus was on recipients to integrate and sort out various ID requirements. For example, Nigeria required people to have a bank verification number (BVN) linked to their SIM registration and national ID. Client onboarding was done through the mobile phone with the provider ensuring that the bank account and the BVN matched, but only after the customer figured out how to link all three data points.[x] Even when digital services were launched to assist, such as the Indian apps Haqdarshak and Mera, they offered little assistance for people who lacked digital, numeric, or financial literacy.[xi]

2 N.B. The research team estimated that these numbers had grown significantly since the survey was conducted.

- **Limited digital infrastructure hindered some communities' receipt of benefits.**
  Limitations in basic infrastructure and technology glitches — biometric failure, electricity shortages, and downed servers and networks — disproportionately impacted rural and remote people. In India for instance, a key informant cited a 7 percent failure rate for biometric verification, with resolution being tedious and complicated.[xii] Especially for villagers who had traveled long distances, these types of errors, and others such as absent officials or agents, not only denied the timely receipt of the benefit but added the opportunity cost of multiple trips.[xiii] In Colombia, a survey revealed twice as many complaints against mobile money vs. cash-based disbursement, with the app Daviplata cited frequently, especially in remote areas with weak or unstable cellular connectivity.[xiv]

- **Novel ways to identify recipients pose data privacy risks.**
  Several countries leveraged Call Detail Records (CDRs) from mobile phones to identify recipients. This novel analytical technique that was used by Togo and Nigeria and considered in many other markets is a harbinger for the future of targeting. While these approaches help to provide more visibility to vulnerable households and target more accurately, they raise concerns around data privacy, data retention, and the fairness and equity of the methods.[xv]

  - On data privacy, questions around data sharing between private and public actors and the management of consent and data rights must be discussed. For instance, when a consumer signs up for a mobile money account, have they consented to have their poverty level scored or to have their data shared with the government? De-anonymization — where a government can match anonymized data with other sources to identify specific individuals — and data retention deserve attention.[xvi] One interviewee emphasized that some marginalized populations already have trepidation about governments knowing anything about them; thus, private sector actors sharing more information with governments would not be well received.[xvii] Although temporary suspension of data privacy or data rights during the pandemic may have put certain data sharing and privacy concerns under less scrutiny, this should not lead to a permanent arrangement.[xviii]

  - On the fairness of targeting, as digital data trails grow into an accepted input for social protection eligibility, questions are raised around the opacity of the predictive models and their potential for bias or further exclusion. Women or other disadvantaged groups may face exclusion or misclassification due to lower rates of phone ownership, fainter representation in datasets that are used to train algorithms, data quality issues, or a misunderstanding of the relationship between how marginalized groups use their phones and their socioeconomic status.[xix] [xx] There are broader concerns around how algorithms are used to make high-stakes decisions, like who receives insurance or a loan and who those decisions might exclude.[xxi] Governments currently have limited visibility into how these models work and the incidence of harms and, particularly in emerging markets, have limited staffing and capacity to build out risk mitigation approaches.[xxii]

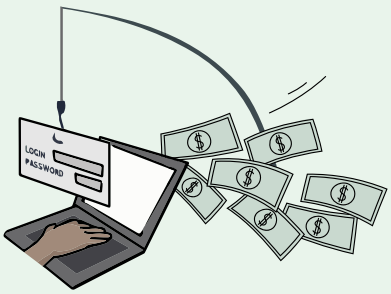
- **Data used for eligibility may increase risks of identity theft.**
  While the digitalization of social protection programs has the potential to reduce leakage, the speed and scale of the distribution of billions of dollars created a uniquely potent environment for scams and fraudsters.[xxiii] [xxiv] [xxv] [xxvi] Identity theft could rob potential recipients of the opportunity to apply to social programs. In Togo, voter registration information was required as part of the application, but unfortunately, because fragments of this information had

been made public during the previous elections, some applicants found that their information had been fraudulently used by another individual to receive benefits and the rightful individual was blocked from even applying. While Togo created an additional layer of verification to prevent against future identity theft, those whose identities had already been stolen had little recourse.[xxvii]

- **Fraud and phishing scams increased.** Once registered, applicants were vulnerable to fraudsters looking to swindle them out of their benefits. In Ghana, like many other markets, applicants received fake calls and SMSs exhorting them, "Hey, we have sent money to you today, so can you send it back to us using this link!"[xxviii] In India, if applicants used Google to look for hotlines for help in accessing their benefit, many Google search results were scammers. The scam artists "sweet talked" people into sharing information about their accounts, which ultimately led to the emptying of their e-wallets.[xxix]

- **Scammers were particularly sophisticated in Brazil.** A survey by Kaspersky identified at least 18 fake apps with the Brazilian G2P program name in the app Play Store.[xxx] There were also reports of phishing frauds related to the cash transfer program conducted over WhatsApp which were targeted at everyone, not exclusively the vulnerable population.[xxxi] Initially, the Central Bank of Brazil blamed the victims for falling prey to the scams but, in September 2021, they took mitigating steps such as limiting transfer amounts and assisting banks in public communications around criminal activity.[xxxii]

- **People were unaware of or confused by terms and conditions.** In some countries like Mexico, Brazil, and Indonesia, applicants agreed to terms and conditions during account signup which could potentially be harmful, such as sharing their account balance info with service provider agencies.[xxxiii] Additionally, cash-outs could be forced or strongly incentivized with some service providers pushing a full one-time cash-out rather than incremental drawdowns. An even more heavy-handed approach was the use of claw-backs, wherein the benefits were clawed back from an account to the government if they were not fully withdrawn within a pre-specified timeframe.[xxxiv] The timeframe varied but was extremely short in certain markets like Sierra Leone at 15 days and in Indonesia at 30 days.[xxxv] Not every beneficiary was able to quickly access a cash-out point, leading some to miss their window. This problem is particularly acute in rural areas like the Amazon, where it can take days to reach a cash-out point.

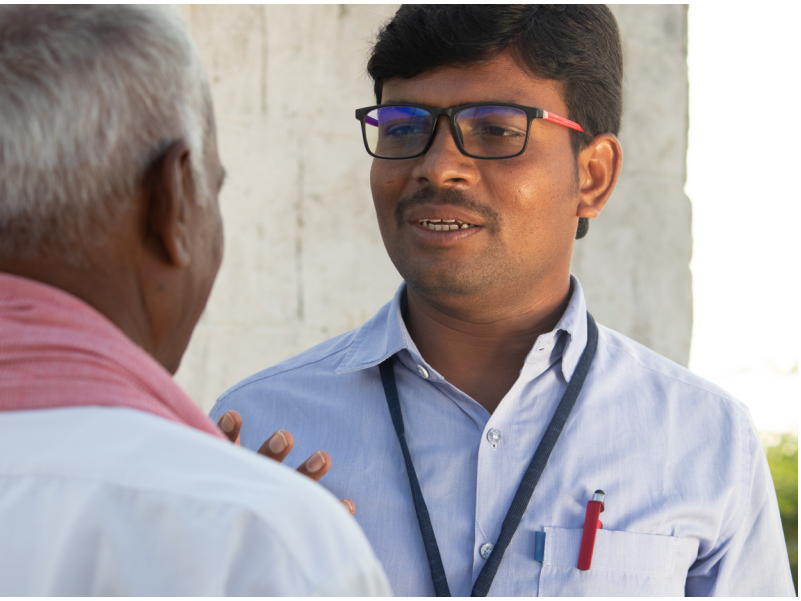


The scam artists "sweet talked" people into sharing information about their accounts, which ultimately led to the emptying of their e-wallets.

Fragmented Delivery Paths Complicate Problem Resolution

Beyond the difficulty of identifying and safely reaching vulnerable people, our research also identified operational challenges that governments and their selected providers experienced. One-size-fits-all design choices that didn't incorporate the diverse needs of people and situations were not prepared to address the various delivery problems that arose. Key informant interviews revealed that the rushed timeline gave governments little opportunity to clearly define and lay out expectations with PSP partners regarding their roles, standards of performance, complaint resolution mechanisms, or reporting structures. In some countries, there was only one payment service provider for the government to partner with; this lack of competition in the market made establishing and enforcing firm guidelines even more difficult.[xxxvi]

Some of the key delivery challenges identified include the following:



- **Overburdened and unempowered staff.**
  Government call centers were often caught unprepared for the deluge of calls they received, and staff and systems were quickly overwhelmed. A key informant from Colombia described that with such overburdened staff, it was difficult for people's issues to be properly escalated, leaving policymakers unaware and unable to address major problems.[xxxvii] Beyond a high volume of legitimate queries, systems could be clogged with frivolous or even fraudulent callers, drawing already-limited staffing resources away from real needs. Unfortunately, some of the call centers themselves were not set up to resolve issues but functioned as informational hotlines. Hotlines could answer frequently asked questions such as: Am I eligible for a benefit? How and where do I apply? How much will I receive? but could not resolve problems or issues, especially when it required fixing inaccurate data housed across multiple government ministries. Hotline staff were neither knowledgeable nor empowered enough to help individuals resolve their problems.

- **Lack of standard operating procedures weakened complaints handling.**
  Particularly in environments where there is a flood of complaints, clear standard operating procedures are vital for a functioning and accountable grievance redressal mechanism (GRM). These include clear processes on how to collate, categorize, and escalate issues, as well as associated time frames for resolution. This appeared to be lacking in several programs. In Nigeria, even though the Central Bank mandated that all complaints be rectified within 48 hours, there was no system to

differentiate, escalate, or track what was going on. As a result of the confusion, the Central Bank of Nigeria has since invested in building a complaint management system with a categorization and monitoring mechanism to understand the types and pace of complaint resolution.[xxxviii]

- **Lack of accountability due to jurisdictional and value chain confusion.**
  The multistakeholder nature of these programs led to challenges of "ownership" and accountability for problems. Because programs often involve multiple government entities — the Ministry of Finance, the Central Bank, and/or the Ministry for Social Protection or Welfare — complaints could run into cross-jurisdictional issues. They also could involve partnerships across private sector implementers: payment service providers, fintechs, or banks. When problems arose across that value chain, accountability for resolution often fell not on the entity that was accountable for the problem, but on the one that had the most accessible complaint system or was most salient. For instance, if someone was dissatisfied with the size or frequency of their benefit and the government's grievance redressal system was weak or hard-to-reach, complaints often were directed to the payment service provider. However, the PSPs had zero authority over eligibility and benefit amount. As a result of these challenges, people were often left to navigate issues on their own and governments did not have a clear sense of the extent of problems people faced.

- **Excessive or unauthorized charges by agents.**
  In Asia and Africa, there were reports of agents unofficially (without receipts) charging fees for providing services during COVID-19. In Nigeria, for instance, there were reports of agents charging unauthorized fees of around 10 percent to cover their operating costs.[xxxix] While some governments included agent commissions in the benefit amount, there were reports of agents deducting additional fees or encouraging people to split up their cash-outs so the agents could earn more fees on multiple transactions.[xl] Moreover, governments did not differentiate the commission amount for urban versus rural agents, and in most cases, rural agents faced higher operating costs to stay open during the pandemic.

- **Infrastructure and regulatory impediments.**
  Digital payment distribution was limited in many places by problems with electricity and mobile coverage, biometric challenges, and liquidity shortages, especially in rural areas. While the issue of digital financial infrastructure within the context of an overall digital economy is a huge topic for governments everywhere and beyond the scope of this paper, it is obvious that infrastructural limitations have wide-ranging impacts upon government activities that impact all policymakers. For example, few bank or mobile money accounts are linked to national ID information, which would have been useful for COVID-19 G2P payments. Policy and regulatory decisions also had unforeseen impacts. For example, many key players, especially banks, NBFIs, and mobile money agents, were not considered "essential" during the early days of the pandemic, inhibiting their ability to support payment programs. Some laws, such as India's Foreign Contribution Registration Act (FCRA), made it difficult for NGOs to access and use foreign funds to help in the fight against COVID-19. [xli]

Building the Next Generation of Digitized Cash Transfers

Improving and enhancing social protection programs and digital financial infrastructure are major undertakings for governments and involve multiple parties across the public and private sectors. Such endeavors inevitably take time. There are some steps, however, that governments can embark on immediately as they prepare for future rounds of G2P programs. CFI believes that governments have a few important levers that they can use now to: 1) improve the effectiveness of digital cash transfer programs in the future; and 2) enhance how these programs support continued participation of low-income people with digital financial services. We believe that by concentrating limited resources on these key levers — provider selection and management, fraud and complaint handling, and enhanced G2P data governance — governments can make important leaps forward that protect consumers while supporting the digital finance ecosystem well beyond government cash transfer recipients.

1. Carefully select and manage providers.

The key avenue to embed appropriate product design and delivery is through clearly delineated agreements with governments' implementing partners, be it a payment service provider, fintech, or bank. Regardless of provider type, all partners should be held to certain standards of quality, for example, through a Service Level Agreement (SLA) within which consumer protection issues feature prominently. SLAs are a common component in IT and technology contracts for parties to reach a shared understanding around services to be delivered, standards of performance, turnaround times, roles and responsibilities, and priorities. SLAs can formalize elements crucial to meeting low-income people where they are and delineate accountability across multiple partners.

Suggestions to incorporate in SLAs based on risks identified above include:

- Standards of disclosure for fees (if applicable);
- Reporting metrics on transaction failure rates, including dormant accounts;
- Justification for any use of forced cash-outs or claw-backs;
- Clear procedures around grievance redressal and delineation of issues to be covered by government vs. provider; if possible, incentives for timely redressal of problems; and
- Agreement on whether, and how, providers can market additional products and services beyond the G2P payment.

An important role that the provider fulfills, in coordination with the government program, is defining the delivery process to ensure that all recipients can access their funds. Segmentation must go beyond basic information like phone ownership to incorporate the cost of data, the quality of surrounding digital infrastructure, user capability, needs, etc. Manual channels are still needed and may never be dropped entirely, especially for groups like migrant workers who are less visible to the state. Relatedly, giving recipients a choice of which payment or financial service provider to hold an account with should be incorporated where possible; in markets with a dominant payment provider, this is obviously more difficult.[xlii] User choice and investment in interoperability can also reduce the risk that people will languish "in silos" without the ability to "transact freely or affordably across providers."[xliii]

Another important design component is the onboarding support. Ideally, SLAs with PSPs would also include onboarding support and digital financial capability building for recipients, though this is not the type of standardized service most providers offer.[xliv] If providers are unable to provide such support, governments should consider partnerships or MOUs with civil society organizations (CSOs) that can be activated in times of crisis, as CSOs can be instrumental in reaching marginalized groups, building skills, and providing insights to providers.

BOX 1

Offering Choice and Support

Governments that designed for varied capabilities took steps such as incorporating a variety of delivery channels and proactively bridging the digital divide. Multiple distribution channels, including manual, increased the chances that people without digital access or outside the state's existing social registries were able to receive relief.[3] In Colombia, the government rolled out three channels for the 3 million Ingresso Solidário recipients — 1 million who were already banked received payments (within a matter of days) through their existing accounts, 700,000 new accounts were created through partnerships with five fintechs, and the rest were reached through a hybrid of tech and touch.[xlv] Program administrators segmented households by their level of access to formal finance and mobile phones to decide the best channel for the transfer.[xlvi] In Zambia, the government proactively purchased phones for new users, and worked with local mayors and other civil servants to create lists of those receiving payments.[xlvii]

Where government support was limited, civil society organizations stepped in to meet with people who faced access or onboarding challenges. For example, in Brazil, neighborhood church groups assisted applicants in accessing online portals, while in South Africa, organizations like the African Reclaimers Organization (ARO), which works with waste reclaimers, helped members without cell phones or money for data plans fill in and submit online applications.[xlviii] Unfortunately, most of these efforts were bootstrapped and lacked resources to scale.

2. Improve fraud and complaint handling.

Understanding the incidence of fraud and scams is a critical first step for governments in addressing the problem. Unfortunately, consumers do not always report or seek recourse for fraud due to the time and hassle it takes to do so.[xlix] Investment in secondary grievance redressal mechanisms through agreed standards in complaints submissions can help with gathering data. For instance, if MNOs are required to submit their complaints data to the Ministry of Telecommunications on a quarterly basis, all providers should be held to a common template that feeds into a dynamic dashboard to monitor for scams. Academics are testing novel approaches that could soon be scaled up for market monitoring; for example, using machine learning on reams of data from Google Play finance apps to predict the likelihood that a digital finance app is fake.[l]

Governments need to invest in research and monitoring tools to better understand people's experiences and provide targeted communications, including warnings about fraud. CFI's research identified multiple channels of communications including radio, TV, social media (even TikTok!), and government websites, but they were often several steps behind the fraudsters. Another communications component would be softening the shame or stigma around falling victim to a scam that can keep consumers from reporting it.[li] Researchers are testing novel approaches such as a predictive model to reach out to mobile money

3 According to the World Bank, 55 programs in 35 countries used manual methods including cash, check, or physical vouchers. See Gentili et al. Last updated May 2021.

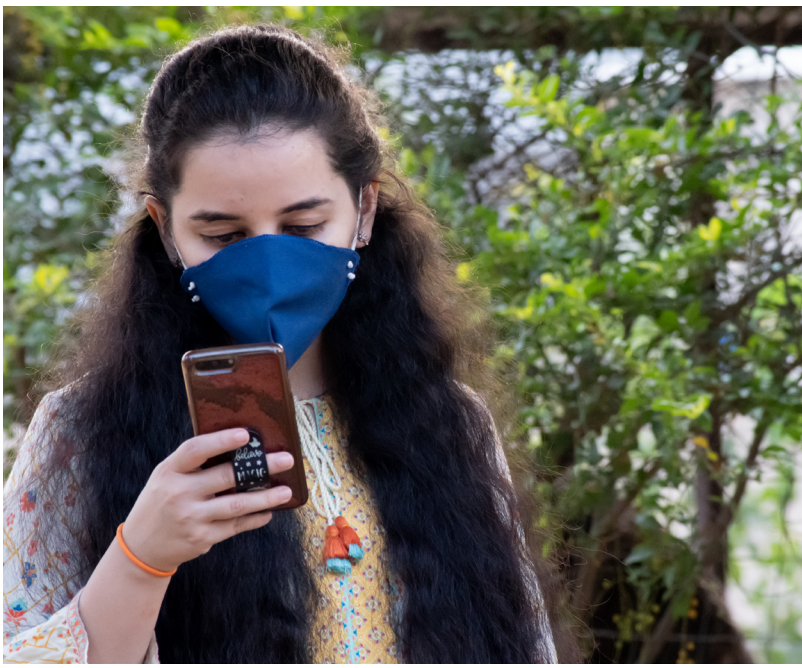
users if the incidence of fraud is growing in their geography.[liii]

To help reduce instances of fraud, improved standards on the disclosure of product terms and charges could help recipients spot agent overcharging; admittedly, this is made more difficult in a crisis when governments temporarily waive fees. Any standards must be coupled by enforcement including market monitoring tools like mystery shopping.[liii] At the same time, governments need to recognize that agents and other private sector partners cannot be expected to incur additional costs for supporting G2P programs. Without an assurance of their own long-term sustainability, these players will understandably overcharge or even refuse to participate.

But perhaps the most important means by which governments can both identify instances of fraud and misconduct as well as improve the user experience is by ensuring there are robust redress mechanisms in place for accountability. A well-functioning grievance redressal mechanism is essential to resolve individual issues as well as incorporate accountability and continuous improvement to program design.[liv]

Grievance redressal mechanisms (GRMs) are low-hanging fruit that governments can invest in to strengthen accountability for their future social protection programs that go beyond hotlines. GRM components should include:

- Organizational structures for responding to and resolving complaints, including a triage or escalation process;
- Adequate staffing with designated expansion plans for temporary or contract workers when the need arises;
- MOUs with other ministries and/or service level agreements with implementing partners (e.g., payment service providers or fintechs) that outline which issues will be handled by whom, and in what time frame;
- Assignment of responsibility for monitoring and evaluating trends in complaints and complaints handling across the organization and for identifying remedial actions (particularly given the target beneficiaries of these programs, this analysis should include gender and geographic data); and
- Regular engagement with consumer advocacy groups and CSOs that are working with impacted populations to understand what might be missing.



GRMs could also be made more transparent through public-facing dashboards on performance, progress, and pitfalls, either through real-time data and/or external evaluations or audits. In Pakistan, the government created an information portal that, as of writing, gives real-time information about the number of people served broken down by province, district, and tehsil (a local unit of administrative division, often known as a township). The portal also notes the amount deposited and the amount withdrawn.[lv] In Brazil, the Federal Court of Accounts of the Union (TCU), an agency set up to conduct audits of the executive branch, conducted an evaluation of who was incorrectly included or excluded in the programs. They estimated that 9.6 percent of people had been incorrectly included. They also admitted that exclusion was a problem but were not able measure it.[lvi]

BOX 2

Offering Choice and Support

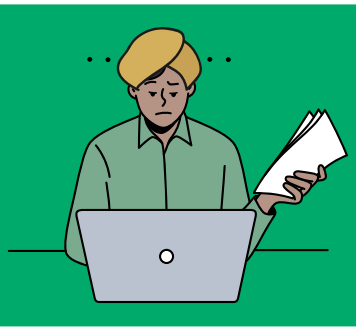
Pakistan provides an example of an effective grievance redressal system. Operationally, the authority to resolve a complaint was delegated from the Benazir Income Support Programme (BISP) Head Office to the tehsil (or township) level for a swifter and more personalized resolution. The system has been operational since 2012 and has received over 3 million complaints, with 90 percent of them being handled within 72 hours of receipt.[lvii] Given that it leveraged the pre-existing BISP system, everything was already online and linked on a real-time basis to process COVID-19-related complaints.[lviii] [lix]

In other markets, our interviews surfaced instances where pressure from civil society, rather than individual complaints, pushed the government to fix a problem. For instance, in South Africa, which experienced backend database mismatches that denied otherwise eligible people from receiving payments, it was CSOs that brought the issue to the government's attention.[lx] In India, some CSOs, including Graam Vaani, created IVRs to help consumers in states in northern and eastern India.[lxi]

Since 2012 in Pakistan:

3 million complaints

90% being handled within 72 hours



3. Enhance G2P data governance.

The safeguarding and use of consumer data within government is taking on a higher priority in the digital age. As governments around the world grapple with this overall issue, there are several actions that can be taken now to protect the data used in social protection programs. Data sharing agreements with private companies that provide governments alternative data for targeting — whether from MNOs, social media, or ecommerce platforms — should be prepared, ex ante, to be quickly deployed as the need arises. These agreements should include data minimization and retention clauses, among other standards such as data security.

a. Data minimization requires only the essential information to be shared to achieve the objective, in this case accurate targeting. However, this may create a tension in cases where machine learning is used for targeting, as more data is generally assumed to yield better models and better predictions.

b. Data retention requirements should be clear alongside sunset clauses. In its COVID-19 Privacy Guidelines, GSMA calls for the deletion of "Mobile Operator Data after a defined period or once it is no longer needed for the agreed health-related purpose."[lxii] Such sunset clauses help avoid future misuse or what privacy scholar Linnet Taylor calls "function creep."[lxiii]

c. Navigating the trade-offs between data rights and providing a critical cash transfer in a timely manner remains a difficult balance. Consumers, particularly low-income people, often are unaware of how their data is being used by providers, which dampens the long-held privacy tenet of informed consent.[lxiv] Governments should collaborate with researchers, privacy

scholars, and humanitarian agencies to try different approaches for opting in to be scored or opting out at the time of registration.[lxv]

The use of AI to determine eligibility requires more testing and evidence before it can serve as a stand-alone tool. Rather, governments should consider framing the new targeting methods and data sources as a complementary, but not stand-alone, eligibility tool that can be deployed alongside other eligibility measures.[lxvi] This approach acknowledges the nascent nature of the tools but also the limits of traditional measures or social registries to capture the entire need, particularly if a shock has rapidly changed poverty levels in a particular geography or subset. There are precedents for this approach, such as the United States' initiative to allow some firms to use alternative data only as a "Second Look" at applicants who would otherwise be denied credit.[lxvii]

At a more technical level, governments should require audits of AI models. In Togo, the researchers conducted ex-post audits through disparate impact testing, which evaluated whether models discriminated against women, different age cohorts, or ethnicities.[lxviii] The researchers concluded that their model was not biased but acknowledged that more market-specific research that articulated the groups most at risk of bias would be more robust.[lxix]

BOX 3

Using AI to Test for Eligibility

In Togo, for the second round of the Novissi program, the government worked with development economists at Innovations for Poverty Action (IPA) to identify and support 57,000 additional people to receive payments. After collecting consumption data on 10,000 individuals via a phone survey, the researchers matched that information to the subscribers' mobile phone metadata — which was shared by the Togolese mobile network operators.[lxx] This metadata included everything from airtime top-up patterns, mobile money transactions, and call details. Then, they applied machine learning techniques to train a model to predict the socioeconomic status of any Togolese mobile phone subscriber, based on their mobile behavior.[lxxi] The team also built high-resolution poverty maps to find the poorest areas of the country using a combination of satellite imagery and nationally representative surveys. For the second round of Novissi, when a mobile subscriber applied via the USSD platform, their cell phone number was checked against the researcher's predictions and if they qualified, they were paid instantly in mobile money.[lxxii]

Outside of Togo, similar techniques were used in several other markets. In Uganda, GiveDirectly partnered with two MNOs to send payments to individuals whose metadata assigned them to a "home tower" in a high poverty location.[lxxiii] In Nigeria, MTN Mobile Money shared geographic "vulnerability scores" for targeting benefits as well as anonymized and aggregated mobile account top-up and transactional data with 36 state governments.[lxxiv]

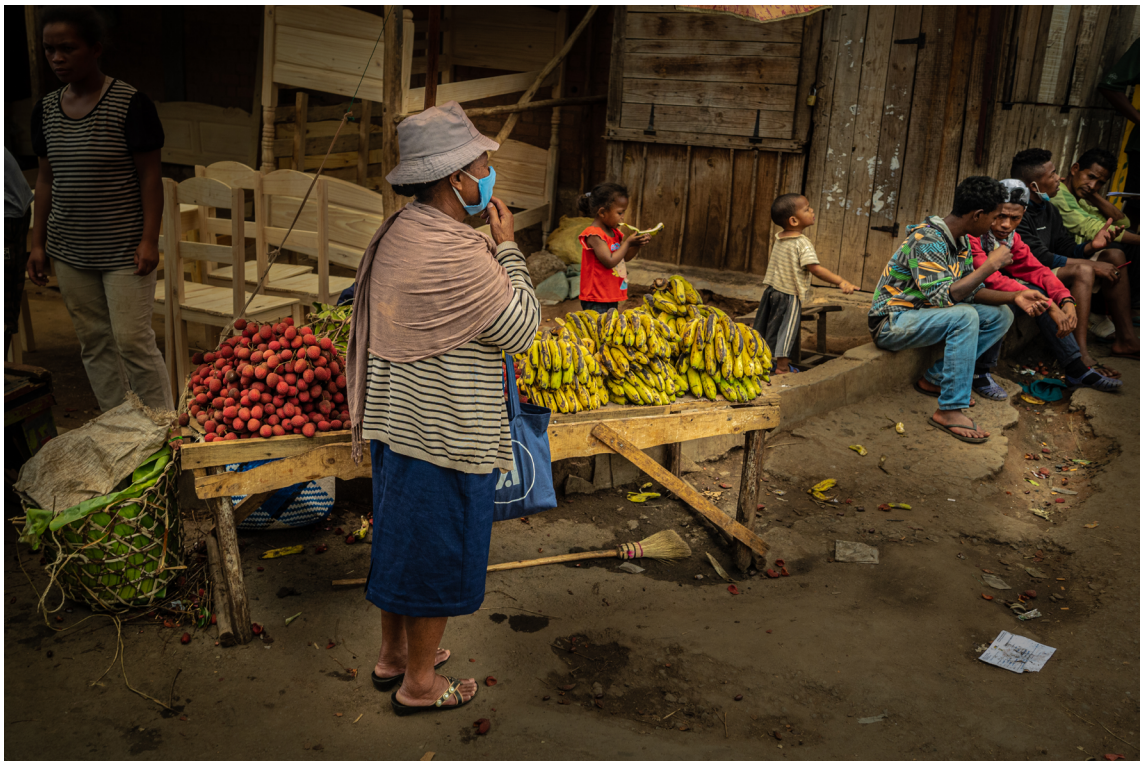
These methods have the potential to identify the otherwise invisible as well as target more accurately. During the pandemic, when governments drew from (relatively up-to-date) social registries or socioeconomic surveys, such as in Pakistan, they had a ready-made bedrock of information from which to determine eligibility. But in many countries these registries were filled with errors, as well as out-of-date or even nonexistent information, causing confusion and delays. For instance, in the Philippines, the last national survey Listahan was considered so out-of-date that eligibility was determined manually, and sometimes haphazardly, by Local Government Units like mayor's offices, each bringing their own resources (or lack thereof) to bear.[lxxv] Alternative data, such as mobile phone metadata or satellite imagery, can make households or communities not housed in any social registry, or in hard-to-reach remote areas, visible for benefits. Additionally, compared to the alternative approaches that could have been used in Togo, including occupational or geographic-based targeting, the IPA researchers estimated that their method reduced exclusion errors by up to 50 percent.[lxxvi]

Conclusion

The last two years have seen unprecedented demand for relief from the COVID-19-related economic downturn. Governments were compelled to move at breakneck speed to mitigate the negative impacts on vulnerable households' income and well-being, which they did with surprising success given the circumstances. While the COVID-19 crisis brought with it untold physical, social, and economic harm to people around the world, one potential positive outcome has been the rapid uptake in digital financial services as a means of providing relief to the most vulnerable.

The growth in digital payment accounts in many countries over the last two years has in fact outstripped previous growth projections for five or even ten years out. The parallel growth in economic activity occurring via digital platforms, across all economic strata, indicates that this digital account usage will continue and grow. We now have the opportunity to review the lessons learned from the G2P programs of the pandemic, especially as they pertain to serving low-income, otherwise excluded households, and adjust procedures and program design. Given the target population for these programs, governments should take every measure to "do no harm" and use the learnings from the pandemic to plan accordingly.

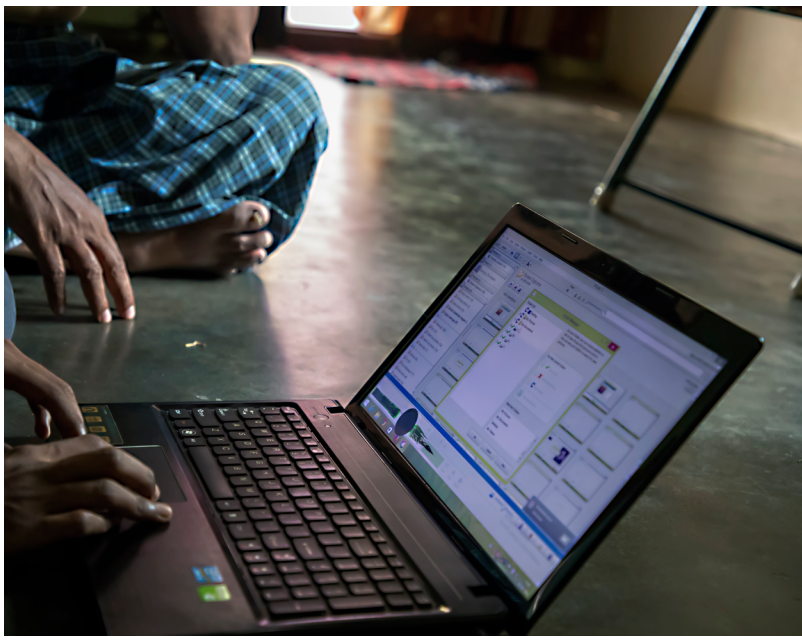
Many of the risks identified in the rapid digitalization of G2P programs are applicable to the digitalization of the financial system at large, with a particular focus on service design that can accommodate a wide range of user



capabilities and circumstances. Essentially, as client selection, onboarding, and usage are increasingly managed by a range of DFS providers with minimal human intervention, product design has become a critical moment for embedding consumer protection. This emphasis shifts protection away from individual staff behavior and focuses on what goes into the product itself, which should include a deep understanding of consumer context, needs, and capabilities.

Likewise, concerns around fraud and scams have been building rapidly in the broader digital finance space, with consumers constantly scrambling to stay ahead of evolving tactics. Fraud is costly for both the consumer and the provider, both from a financial perspective for consumers as well as a financial and (potentially irreparable) loss of trust in the service for the provider. Moreover, these challenges are growing at a time of evolving accountability across increasingly complex digital finance value chains, with multiple parties playing a role in each transaction. These parties and the roles they play may or may not be visible to users. The "modularization" of the industry — or the replacement of full-service providers by multiple institutions that specialize in discrete functions — promises efficiency, but also raises challenges when things go wrong. Instead of a single firm being at fault, the problem could lie across multiple firms, creating complications for consumers seeking accountability.

As governments make improvements to minimize risk for future social protection recipients, this paves the way for digital finance consumers at large. In particular, the expanding use of multiple data sources to identify, assess and serve customers brings with it huge ramifications for consumer protection, data privacy, and government cybersecurity. For instance, if governments advance their capacity to audit algorithms used to target beneficiaries, it will increase their general capacity to engage with other high-stakes financial algorithms, such as those being used by digital lending apps or platforms. Through service level agreements (SLAs) with payment service or financial providers that spell out standards of good practice, governments can influence the way these providers treat all their customers,



not just those opening accounts to receive benefits. And in testing and learning how best to reach recipients and help them avoid fraud and scams, governments will likely build consumers' capacity to circumvent digital swindlers in general and ultimately become functional participants in the digital financial ecosystem.

References

i Gentilini, Ugo, Mohamed Almenfi, Ian Orton, and Pamela Dale. 2020. "Social Protection and Jobs Responses to COVID-19: A Real-Time Review of Country Measures." World Bank. https://openknowledge.worldbank.org/handle/10986/33635.

ii "COVID-19 Social Protection and Economic Policy Responses by Governments: Lessons for Social Protection Readiness and Building Forward Better." 2021. United Nations. https://tracker.unescwa.org/External/Global-Policy-Brief-COVID-19%20Stimulus%20Tracker_Social-Protection-And-Economic-Policy-Responses-Of-Governments.pdf.

iii Gentilini et al., "Social Protections and Jobs Responses."

iv Key Informant Interview. Colombia, Sept. 24, 2021.

v Bastagli, Francesca and Christina Lowe. July 2021. "Social protection response to COVID-19 and beyond." ODI. https://cdn.odi.org/media/documents/ODI_Synthesis_final.pdf.

vi "Special Rapporteur on extreme poverty and human rights. Looking back to look ahead: A rights-based approach to social protection in the post-COVID-19 economic recovery." Sept. 11, 2020. United Nations Human Rights Special Procedures. https://www.ohchr.org/Documents/Issues/Poverty/covid19.pdf.

vii Aiken, Emily et al. July 2021. "Machine Learning and Mobile Phone Data Can Improve the Targeting of Humanitarian Assistance." NBER Working Paper Series 29070. https://www.nber.org/system/files/working_papers/w29070/w29070.pdf.

viii Ibid.

ix Debenedetti, Luciana. Aug. 2021. "Togo's Novissi Cash Transfer: Designing and Implementing a Fully Digital Social Assistance Program During COVID-19." Innovations for Poverty Action. https://www.poverty-action.org/sites/default/files/publications/Togo-Novissi-Cash-Transfer-Brief-August percent202021.pdf.

x Key Informant Interviews. United States, July 20, 2021, and Nigeria, July 27, 2021.

xi Key Informant Interview. India, July 21, 2021.

xii Key Informant Interview. India, Sept. 13, 2021.

xiii Key Informant Interviews. India, July 21 and Sept. 13, 2021, and United States, July 20, 2021.

xiv Londono-Velez, Juliana and Pablo Querubin. Nov. 2020. "The Impact of Emergency Cash Assistance in a Pandemic: Experimental Evidence from Colombia." Innovations for Poverty Action. https://www.poverty-action.org/sites/default/files/Covid19CashColombia_v6.pdf.

xv Blumenstock, Joshua. "Applications of Machine Learning in Humanitarian Assistance." DIDL. http://eeb.bcb.gob.bo/sites/default/files/programa/14eeb%20docs/14EEB_jblumenstock.pdf

xvi Ibid.

xvii Key Informant Interview. India, July 21, 2021.

xviii "Case Study: Data Responsibility and Digital Remote Targeting During COVID-19." Mar. 2021. The Cash Learning Partnership. https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Remote-Targeting.pdf.

xix "The Mobile Gender Gap Report 2020." May 2020. GSMA Connected Women. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf.

xx Rizzi, Alexandra et al. Mar. 2021. "The Stories Algorithms Tell: Bias and Financial Inclusion at the Data Margins." Center for Financial Inclu-

sion. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2021/03/The-Stories-Algorithms-Tell-CFI-publication-MAR21.pdf.

xxi Ibid.

xxii Rizzi, Alexandra and Pia Roman Tayag. Dec. 21, 2021. "Accountability for Algorithms: A Balancing Act for Governments." Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/accountability-for-algorithms-a-balancing-act-for-governments.

xxiii Blumenstock, Joshua et al. May 2015. "Promises and Pitfalls of Mobile Money in Afghanistan: Evidence from a Randomized Control Trial." PEDL. https://pedl.cepr.org/sites/default/files/Ghani_Promises%20and%20Pitfalls%20of%20Mobile%20Money%20in%20Afghanistan_working%20paper_0.pdf.

xxiv Muralidharan, Karthik et al. 2016. "Building State Capacity: Evidence from Biometric Smartcards in India." American Economic Review, 106(10): 2895–2929. https://www.povertyactionlab.org/sites/default/files/research-paper/Building-State-Capacity_Feb2016.pdf.

xxv Medine, David. May 2020. "Financial Scams Rise as Coronavirus Hits Developing Countries." IPS. http://www.ipsnews.net/2020/05/financial-scams-rise-coronavirus-hits-developing-countries/.

xxvi Fu, Jonathan and Mrinal Mishra. Dec. 21, 2020. "Combating the Rise in Fraudulent Fintech Apps." Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/combating-the-rise-in-fraudulent-fintech-apps.

xxvii Bastagli and Lowe, "Social protection response."

xxviii Key Informant Interview. Ghana, July 28, 2021.

xxix Key Informant Interview. India, July 21, 2021.

xxx "Aplicativos falsos do auxílio emergencial são usados em golpes; saiba como se proteger." Apr. 24, 2021. Diario do Nordeste. https://diariodonordeste.verdesmares.com.br/negocios/aplicativos-falsos-do-auxilio-emergencial-sao-usados-em-golpes-saiba-como-se-proteger-1.3076913

xxxi Key Informant Interview. Brazil, Sept. 1, 2021.

xxxii Key Informant Interview. Brazil, Sept. 1, 2021

xxxiii Key Informant Interview. United States, July 20, 2021.

xxxiv Key Informant Interview. United States, July 27, 2021

xxxv Key Informant Interview. United States, July 20, 2021; and Georgina Marin. Sept. 22, 2021. "Modern G2P Architecture." G2PX. https://assets.website-files.com/5e540242678f9f3ccb231a54/61517b16d8389feb8969350f_SA%20G2P%20workshop%20_%20Sept%2022%202021.pdf

xxxvi Key Informant Interview. United States, July 20, 2021.

xxxvii Key Informant Interview. Colombia, Sept. 24, 2021

xxxviii Key Informant Interview. Nigeria, July 27, 2021.

xxxix Key Informant Interview. Nigeria, July 27, 2021.

xl Key Informant Interviews. Philippines, September 22, 2021, Bangladesh, Sept. 20, 2021, and India, September 13, 2021.

xli Key Informant Interviews. India, July 21, 2021 and Sept. 13, 2021; and Foreign Contribution Regulation Amendment Act. Sept. 28, 2020. https://fcraonline.nic.in/home/PDF_Doc/fc_amend_07102020_1.pdf.

xlii "UN Principles for Responsible Digital Payments." Updated Edition Oct. 2021. Better than Cash Alliance. https://responsiblepayments.org/pdfs/UN-ResponsiblePayments.pdf.

xliii Ibid.

xliv Arnold, Julia and Jayshree Venkatesan. June 2020. "Building Women's Financial Capability: A Path Toward Transformation." Center for Financial Inclusion. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2021/06/Building-Women%E2%80%99s-Financial-Capability-4-1-1.pdf.

xlv Key Informant Interview. Colombia, Sept. 24, 2021.

xlvi "UN Principles for Responsible Digital Payments."

xlvii Key Informant Interview. Zambia, Sept. 27, 2021.

xlviii Key Informant Interview, Brazil, Sept. 1, 2021; and Alfers, Laura. June 16, 2021. "A Digital Bridge to Social Support." Project Syndicate. https://www.project-syndicate.org/commentary/social-programs-for-informal-workers-must-bridge-digital-divide-by-laura-alfers-2021-06.

xlix "Client Voices: Rwandans Speak on Digital Financial Services." June 2019. Smart Campaign. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/06/CFI54_SMART_rwanda_FINAL-lores.pdf; and Bird, Matthew and Rafe Mazer. Mar. 2021. "Uganda Consumer Protection in Digital Finance Survey." Innovations for Poverty Action. https://www.poverty-action.org/sites/default/files/Uganda-Consumer-Survey-Report.pdf.

l "Combatting Fraudulent Financial Technologies with Machine Learning." 2021. Innovations for Poverty Action. https://www.poverty-action.org/study/combating-fraudulent-financial-technologies-with-machine-learning.

li "Social Media Scams: Understanding the Consumer Experience to Create a Safer Digital World." May 2019. Consumers International. https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf.

lii Bird, Matthew et al. Sept. 2021. "Leveraging customer complaints data to monitor consumer protection in mobile services in Uganda." Innovations for Poverty Action. https://www.poverty-action.org/publication/leveraging-customer-complaints-data-monitor-consumer-protection-mobile-services-uganda

liii "Market Monitoring for Financial Consumer Protection." 2022. CGAP. https://www.cgap.org/topics/collections/market-monitoring.

liv "Putting the Principles to Work: Detailed Guidance on the Client Protection Principles." Aug. 2021. Center for Financial Inclusion. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2021/08/Principles-Guidelines_Aug-2021-update-1.pdf.

lv "Ehsaas Emergency Cash Dashboard." 2022. Government of Pakistan. https://www.pass.gov.pk/ecs/uct_all.html.

lvi "Follow-up on the Emergency Aid for Protection of People Under Vulnerable Conditions." Nov. 2020. Federal Court of Accounts (TCU). https://portal.tcu.gov.br/en_us/biblioteca-digital/report-on-government-policies-and-programs-ruled-cases-repp-2020.htm.

lvii "COVID-19 G2P Cash Transfer Payments. Country Brief: Pakistan." 2020. G2PX. https://thedocs.worldbank.org/en/doc/760541593464535534-0090022020/original/WorldBankG2PxCOVID19PakistanBrief.pdf

lviii Key Informant Interview. Pakistan, Aug. 9, 2021.

lix "COVID-19 G2P Cash Transfer Payments."

lx Key Informant Interview. United States, July 27, 2021.

lxi Seth, Aaditeshwar et al. Apr. 2021. "Delivery of Social Protection Entitlements in India." Dvara Research. https://www.dvara.com/research/wp-content/uploads/2021/04/Delivery-of-Social-Protection-Entitlements-in-India-Unpacking-Exclusion-Grievance-Redress-and-the-Relevance-of-Citizen-Assistance-Mechanisms.pdf

lxii "The GSMA COVID-19 Privacy Guidelines." Apr. 2020. GSM Association. https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy-Guidelines.pdf

lxiii Taylor as cited in Aiken et al., "Machine Learning and Mobile Phone Data."

lxiv Rizzi, Alexandra and Tanwi Kumari. Oct. 20, 2021. "Trust of Data Usage, Sources and Decisioning: Perspectives from Rwanda Mobile Money Users." Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/trust-of-data-usage-sources-and-decisioning-perspectives-from-rwandan-mobile-money-users

lxv Aiken et al., "Machine Learning and Mobile Phone Data."

lxvi Raftree, Linda. Mar. 2021. "Case Study: Data Responsibility and Digital Remote Targeting During COVID-19." The Cash Learning Partnership. https://www.calpnetwork.org/wp-content/

uploads/2021/03/CaLP-Case-Study-Remote-Targeting.pdf.

lxvii "Interagency Statement on the Use of Alternative Data in Credit Underwriting." Dec. 13, 2019. Federal Reserve, Consumer Financial Protection Bureau et al. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20191203b1.pdf.

lxviii Aiken et al., "Machine Learning and Mobile Phone Data."

lxix Ibid.

lxx Debenedetti, "Togo's Novissi Cash Transfer."

lxxi Ibid.

lxxii Raftree, "Case Study: Data Responsibility."

lxxiii Ibid.

lxxiv Gilbert, Joanne et al. 2021. "Using mobile big data to support emergency preparedness and address economically vulnerable communities during the COVID-19 pandemic in Nigeria." Data and Policy, Volume 3. https://www.cambridge.org/core/journals/data-and-policy/article/using-mobile-big-data-to-support-emergency-preparedness-and-address-economically-vulnerable-communities-during-the-covid19-pandemic-in-nigeria/6E3B62FD9BC5A7C46842DB173B16B58D

lxxv Key Informant Interview. The Philippines, Sept. 21, 2021.

lxxvi Blumenstock, "Applications of Machine Learning."

The Center for Financial Inclusion (CFI) works to advance inclusive financial services for the billions of people who currently lack the financial tools needed to improve their lives and prosper. We leverage partnerships to conduct rigorous research and test promising solutions, and then advocate for evidence-based change. CFI was founded by Accion in 2008 to serve as an independent think tank on inclusive finance.

www.centerforfinancialinclusion.org

@CFI_Accion

CENTER *for* FINANCIAL INCLUSION | ACCION