DECEMBER 2020

AUTHORS

Madeleine Longwell
and Alexandra Rizzi

Protecting Beneficiary Data: Guidance for Municipal Cash Transfer Programs Responding to COVID-19

CENTER *for* FINANCIAL INCLUSION | ACCION

Acknowledgments

This report draws on insights gained through interviews conducted with managers of seven municipal cash-based assistance programs, which included the Angeleno Campaign, the City of Atlanta's emergency cash assistance program, the California Immigrant Resilience Fund (CIRF), the City of New York's COVID-19 Emergency Relief Fund, the Chicago Resiliency Fund, the Harris County COVID-19 Relief Fund, and the Left Behind Workers Fund. We appreciate the guidance of the data privacy experts who took the time to speak with us. We also wish to thank Monica Greco, Susana Liu-Hedberg, Sandra Barron, and Colleen Thouez of Open Society Foundations for reviewing and providing us their invaluable feedback on this research.

Executive Summary

In recent months, many U.S. cities have established assistance programs to help community members affected by COVID-19, often targeting those otherwise excluded from assistance such as the Coronavirus Aid, Relief, and Economic Security (CARES) Act. These cash-based assistance (CBA) programs are vital for undocumented and mixed status households that have been disproportionately affected by the pandemic.

It is essential that these municipal programs are designed and rolled out responsibly. This paper focuses on one area of responsibility: the protection of beneficiary data. In the context of CBA programs, poor data protection practices could add additional risks for low-risk individuals, including unauthorized access to applicant or beneficiary data or leakage of personally identifiable information (PII). Law enforcement increasingly relies on databases and public records for investigations of undocumented populations, so data trails increase the likelihood that individuals' digital footprints may be collected and later used to target them.

To better understand how municipalities thought about and handled these risks, CFI conducted interviews with cities, community-based organizations (CBOs), debit card providers, and privacy advocates. Encouragingly, we find that most CBA programs have prioritized data protection, though approaches to it vary widely. Furthermore, strategies such as adopting broader beneficiary criteria and working with payment providers appear to be relatively widely adopted and easy to implement.

We have identified approaches and strategies used to protect applicant and beneficiary data through four programmatic phases described below:

Targeting Beneficiaries

In this phase, programs face some trade-offs in deciding who will be the target beneficiaries. While widening the beneficiary targets beyond undocumented immigrants increases the "noise" in program data, making it more difficult to identify undocumented individuals, it might also come with less certainty that programs have reached those most in need. Cities have navigated this challenge by designing criteria for applicants around other conditions or opening programs to a wider beneficiary pool.

Outreach and Onboarding

To minimize fraud, program organizers often collect and store a significant amount of personal information about applicants. The risk that information is shared outside of a cash assistance program is particularly high for the vulnerable populations many of these programs are targeting. Programs have attempted to balance these needs with data protection by minimizing the amount of information collected and procuring data management platforms to control access to information and decentralize data storage.

Disbursement and Distribution

Programs have utilized a variety of disbursement methods for payments, but mostly pre-paid debit cards. In the selection of a disbursement method, programs have weighed factors including security and privacy, as well as efficiency and ease of distribution. We have found that prepaid debit cards can be anonymized, and information collected through cards is relatively easy to secure.

Ongoing Monitoring and Data Storage/Retention

Despite the uncertainty around when the COVID-19 crisis will end, it is important for CBA program managers to specify retention periods for applicants' and beneficiaries' personal data within their own databases as well as their partners'.

1 Introduction

As detailed in "Designing Municipal Cash Transfer Programs to Mitigate the Economic Impact of COVID-19," municipalities have been establishing cash transfer programs to get economic relief to undocumented immigrants and their families as well as other vulnerable groups that were excluded from social support provided through the CARES Act. While developing these programs, cities are making decisions about targeting beneficiary populations, conducting outreach, determining their eligibility, and getting funds to some of the nation's most at-risk residents. A paramount concern for these cities and their community-based organization (CBO) partners is how to address the unique privacy risks faced by this population.

Privacy advocates often highlight that low-income consumers face a "perfect storm" of privacy dangers in that they are often disproportionately targeted for data collection efforts and simultaneously less likely to be aware of basic protections,[1] such as avoiding posting location information on social media. Accessing even basic digital financial services, for example, can put users at risk of identity theft, misreported credit information, or cause harm to their reputations without their knowledge.[2] A 2017 study found that individuals in low-income households were more likely to face privacy risks due to their heavier reliance on mobile phones for internet access than higher-income households.[3] Using a mobile phone for internet access increases the likelihood that data will be shared because phones capture location data that can be easily and unknowingly shared, and many apps do not have clear or easily-available privacy policies.

These longstanding concerns serve as a backdrop for the harms that could result from poor data protection in cash-based assistance (CBA) programs, including unauthorized access, leakage of personally identifying information (PII), ill-understood consent forms, or weak data retention protocols. In addition to being low-income, the primary beneficiary group of CBA programs is undocumented immigrants, which further increases the level of risk in the event of a data breach.[4,5] As law enforcement increasingly relies on databases and public records for investigations, America's undocumented population faces additional risk that their personal information may be collected and later used to target them.

Municipal identification programs such as New York City's IDNYC have highlighted the concerns that come with associating financial and personal identification information for vulnerable populations. When IDNYC first considered embedding radio frequency identification (RFID) chips into the cards that would allow them to be used for electronic payments, opponents pointed out that the program would increase the amount of information the city held about cardholders. In addition to the risks that come with RFID chips—namely, they are relatively easy for anyone from a short distance to read with the necessary technology—advocates were concerned that linking financial and identity data could potentially expose cardholders to identity theft or law enforcement action. These concerns were particularly pointed given the history of Freedom of Information Act (FOIA) requests for municipal ID program data the city experienced. The addition of RFID chips to IDNYC cards would have also expanded an individual's digital footprint as financial institutions collect data from their payments systems, creating another avenue for data exposure.

The current political and law enforcement environment has also raised concerns among data privacy advocates that data trails left by municipal-led programs, like identification and cash transfer programs, could be used in the future to target undocumented immigrants. Collecting data, whether through public records, information from a private data broker, or social media, is an increasingly essential tool for U.S. Immigration and Customs Enforcement (ICE), a law enforcement agency that is part of the Department of Homeland Security. A New York Times article from October 2019 found that ICE's targeting decisions often depended on who was "findable,"[6] pointing to car registration, utility bills, tax documents, and social media as high-value sources available through FBI and DHS databases, but also through private sources like CLEAR online investigation software from Thompson Reuters. ICE also works closely with other government databases such as those belonging to state Departments of Motor Vehicles (DMVs), which can confirm immigration status by verifying Social Security numbers, vehicle registrations, and utility bill information.

While there are clearly privacy risks associated with collecting beneficiary data for CBA programs, the cash assistance itself is vital. A study by the Urban Institute found that Hispanic adults in families that include non-citizens have been disproportionately affected by the pandemic and subsequent economic crisis. Nearly half of adults (46.9 percent) from those families reported cutting back spending on food, 62.9 percent reported putting off major household purchases, and 49.9 percent reported facing cuts to savings and increases in credit card debt.[7]

Given this context, this note aims to weigh the proportional harms against the benefits, along with suggesting safeguards program managers can take to further minimize risk. It provides examples of how current CBA program managers, which include a mix of municipalities, states, and provider organizations, are grappling with the risks.

Research Approach

CFI conducted 11 semi-structured interviews with cities, program administrators, program partners (such as prepaid card providers), as well as several immigration attorneys from across the country to get a better understanding of the safeguards and risks associated with these CBA programs. All of the interviews were conducted remotely across the summer of 2020. Interviews probed for respondents' perception of the discussions around the specific privacy concerns for the populations of interest. Program administrators laid out their perceptions of the types of risks—both to the privacy of beneficiary information as well as program security—they were concerned about and how they were addressing them. This paper pulls out four phases of the CBA programs that, despite the diversity in interventions, are somewhat universal: targeting beneficiaries, outreach and onboarding, disbursement and distribution, and follow-up/program monitoring. The analysis also brings to bear CFI's work on global consumer protection issues impacting low-income individuals as well as its recent work on domestic municipal IDs.

Encouragingly, we find that most CBA programs have prioritized data protection, though approaches vary widely in terms of the level of formalization and the tools used to mitigate risk. It is essential that administrators prioritize data protection for the program and users to ensure the assistance provided is as effective and safe as possible. The most formalized data protection infrastructure we identified through the interviews was in New York City, where the Mayor's Office of Immigrant Affairs (MOIA) worked closely with the city's Chief Privacy Officer to develop an approach that significantly limited the ability to access beneficiary information. Other CBA approaches, some of which will be further expounded upon below, include avoiding collecting immigrant status, obscuring the names of partner CBOs, using database management with rigorous access controls, and tailoring disbursement methods to allow for maximum anonymity. These choices all come with tradeoffs in terms of budget and efficiency, and there is no one-size-fits-all approach.

2 Targeting Beneficiaries

One of the challenges programs initially face is how to target beneficiaries and reach the intended populations. Expanding the target population beyond undocumented immigrants can increase "noise" in program data, making it more difficult to identify undocumented individuals. The downside of this approach is that it potentially limits the amount of assistance going directly to the most vulnerable.

Introducing noise into the program has provided benefits in other contexts, such as municipal ID programs. Offering cards to all city residents prevented these programs from becoming de facto lists of undocumented residents. For example, in New York City, IDNYC tried specifically to register documented New Yorkers with cards to lower the risk to undocumented cardholders. In the context of cash transfer programs, however, increasing the number of eligible recipients decreases the amount of funding that will go to individuals who would not qualify for the CARES Act, unemployment insurance, or other assistance.

Some CBA programs have tried to navigate this challenge by designing their criteria for receiving assistance around other conditions. In Colorado, the Left Behind Workers Fund is targeted at individuals in the state who have lost their jobs due to COVID-19 and are not eligible for unemployment insurance or federal stimulus. In Los Angeles, the Angeleno Card program required applicants to prove that they lived in Los Angeles, that their income fell below the federal poverty line, and that they had been adversely impacted financially by COVID-19. These programs attempted to target the populations most in need and most likely to be excluded from other assistance because of documentation, without requiring information that would enable them to confirm immigration status. While these approaches create more "noise" in the database of beneficiaries, it might also be less clear whether undocumented immigrants, if they are the intended recipients of the program, are in fact being reached.

In New York, for instance, the MOIA and Chief Privacy Officer took steps to protect the privacy of beneficiaries at two levels; the first was to not publish the names of the CBOs with which they were partnering to disburse funds, and the second was to keep beneficiary information at the CBOs and not share it with MOIA. This hands-off approach—where CBOs were entrusted by MOIA to target, approve, and disburse funds with minimal oversight—only seemed possible due to their long-standing relationship with the city. The city trusted that these CBOs, which have worked extensively with undocumented populations, knew exactly how to reach and encourage potential beneficiaries to apply. This approach, while innovative, likely would not be feasible for a CBA program without strong, proven ties to CBOs.

3 Outreach and Onboarding

Through the application and intake process, cities, program organizers, and partner CBOs collect and store a significant amount of information about applicants such as names, addresses, contact information, and income and/or employment information. Applicants face potential risk not only by providing information such as immigration status or personal documents but by providing information through an application that is not secure or easy to monitor, such as a Google Sheets. The risks CBA program managers expressed the most concern about are the potential for fraudulent applications and the exposure or leakage of stored applicant information. In response to this influx of data, cities and CBOs—especially those with experience working with immigrant populations—have deployed several strategies to ensure data protection.

Minimize the amount of applicant information collected.

Where possible, programs embrace data minimization by limiting the amount of data collected in the application itself. By doing so, they can limit the amount of information that could potentially be leaked, shared, or used to identify recipients outside of the program. In addition to some programs not requiring information about immigration status, cities have limited the amount of other personally identifying information they collect. For example, Connective, which coordinates a cash assistance program and distributes funding through CBOs in Harris County, Texas, only collects an applicant's address, which is used for sending funds.

Use data management platforms to more strictly control access.

Another measure used by program administrators was strictly controlling who could access what types of data under different circumstances. In Colorado, the Left Behind Workers Fund designed their data collection process to simplify what was required of the partner CBOs, which facilitated applications. CBO staff would collect information on an iPad or computer, but the data was never stored locally and instead swiftly ferried over to a remote, secure server. Anyone outside of the program administrator who tried to access the saved applicant information was then required to justify the need for data and complete a two-factor authentication before it could be accessed.

Data management has been a learning curve for some programs. When the Angeleno Card was initially created in Los Angeles, the program managed applicant data using Google spreadsheets across multiple partner CBOs. While using Google Sheets enabled the program to be built relatively quickly, it also posed potential risks because any information stored on Google Sheets was available across platforms and could easily be shared. In its second iteration, the Los Angeles program built an Oracle-based system for application scheduling, intake, and document retention with their 16 partner Family Service Centers (FSCs). The Oracle system allowed for greater control over who was granted access to applicant data. It allowed program administrators to give intake workers unique usernames and allowed them to track what information was accessed and when by each user. The Oracle system also ran an audit report each night to track user searches and monitor for irregularities, such as if data had been accessed after work hours.

In Chicago, The Resurrection Project (TRP)'s 20 partner CBOs collected data from applicants and stored it in Salesforce. TRP staff reviewed all applications and made the final approval decisions. Notably, TRP mentioned that unlike LA's relatively new Oracle database venture, their Salesforce database was already used extensively for its ongoing work with undocumented immigrants and contained sensitive personally identifiable information. One staffer there said, "We are accustomed to incredibly sensitive information and [our] Salesforce [platform] has been built out keeping that in mind."

Decentralizing data storage can limit the ability of outside actors to reidentify beneficiary information.

Multiple program administrators CFI interviewed also mentioned separating where data is stored and who has access to it as a strategy to lower the risk of exposing applicant information. For example, individual CBOs may retain personal information collected during the application process, while the city or program organizers may maintain aggregate data or summary information from each CBO, with the intention that if there a FOIA request or subpoena for the program, only a limited amount of information would be turned over.

A cash assistance program in Atlanta developed such a strategy to mitigate any harm from potential law enforcement requests. The city only collected a final report with summary information from partner CBOs. City officials said that in the past, federal and state actors trying to access information typically have targeted the city. Anyone trying to access more detailed program information would need to collect information from separate CBOs, which program administrators feel is less likely. In Harris County, Texas, Connective also intentionally collected only applicant name and application process stage, using unique identifiers for applicants to further obscure their information. In addition, Connective established a system that enabled individual agencies it was working with to report how applicant information was verified without requiring either organization to upload or save applicant documents.

Design systems to protect against fraud.

Programs also designed privacy and security features around fraud prevention. Multiple programs CFI spoke to reported that applicants would sometimes engage in activities in an attempt to get duplicate benefits, such as sharing registration links for personal application appointments, applying from outside the city or state the program was run in, or trying to apply on behalf of friends or family when applications opened. Program administrators for the Angeleno Card in LA said switching from using Google Sheets to track applicants to an Oracle database made it easier to prevent people from submitting applications on behalf of other people or sharing personal links for scheduling the in-person intake portion of the application.

4 Disbursement and Distribution

After the decision has been made on who will receive the cash assistance, programs swiftly move to disbursing funds. Programs must balance secure and easily anonymized fund disbursement methods, such as providing cash directly, with more efficient and widely-used solutions such as prepaid debit cards.

Program managers CFI interviewed have made a variety of choices in methods including in-person cash disbursement, checks, transfers via Western Union, gift cards, and the most popular choice: non-reloadable prepaid debit cards.[8] In one case, the program manager, working with several dozen CBOs, allowed each CBO to determine the disbursement method based on beneficiary needs. While this certainly resulted in more administrative work for the program manager and individual CBOs, it may have also addressed localized privacy concerns or needs among beneficiaries. One data privacy advocate whom we interviewed suggested *always* giving physical cash disbursement as an option in case beneficiaries have concerns about alternative methods, although this increases physical risks.

Data protection and security seemed to partially factor into the selection of a disbursement method—though speed, convenience, and perceived usability were also cited by program administrators. For example, one program chose to mail checks rather than disburse them in person due to the risk of law enforcement learning of and targeting a large in-person distribution center. Other program managers cited the anonymity of prepaid debit cards as a benefit, though most prepaid cardholders have the option to register them with the issuer. Each method has tradeoffs from a data privacy perspective but by far, cities have opted for prepaid debit cards. Given their ubiquity, this section focuses primarily on learnings relevant for prepaid debit card programs.

Prepaid debit cards are easy to use but more information is retained than some users expect.

Registering a prepaid card entails that a beneficiary gives his or her name, email address, telephone number, and home address to the financial intermediary, often through a web portal. None of the programs we interviewed required beneficiaries to register their cards or set registration as the default option. However, one prepaid card provider noted that in order to enable the ATM withdrawal feature, it required a beneficiary name, home address, and email address. Some community-based organizations deliberately chose prepaid cards without the ATM feature for this reason, though this comes with a tradeoff of being unable to access physical cash, which might be desperately needed.

Through their partnerships, municipalities partnering with prepaid card companies do have access to aggregate data on card usage and some regularly looked at it to understand how beneficiaries were spending money. For the prepaid card company, the information is disaggregated at the level of an individual dashboard, where they can see the proxy number, whether the card has been activated, where it's been used, and the outstanding balance.

Registering the card does come with some benefits, namely that if the card is stolen, lost, or fraudulently used, beneficiaries have recourse with the provider. These protections were rearticulated recently under the Prepaid Amendment (2018) issued by the Consumer Financial Protection Bureau (CFPB).[9] Under this amendment, these protections are not extended to cardholders who have not registered. Interestingly, one prepaid card company noted that for recipients of the cash-based assistance, it had made an exception in terms of offering recourse to all beneficiaries, including those who had not

registered. This condition would likely need to be negotiated in the service agreement between the CBA program manager and the vendor.

Administrators of one CBA program felt strongly that beneficiaries needed to understand that by registering, they would be sharing personally identifying information (PII) with a third party. They negotiated with the prepaid card company to put up an additional disclaimer that the program managers themselves drafted. The disclaimer communicates to cardholders that while there are benefits to registering your card, if you want to remain anonymous, you should not register.

There are potential risks of third-party access to prepaid debit card information.

The prepaid card companies we interviewed said that the data on registered program beneficiaries is never sold at either an identifiable or aggregate level to third-party marketing firms or data brokers. Even in a de-identified state, prepaid card data would contain granular information about beneficiary behavior, including vendor information as well as date and times of purchases. In the wrong hands, this data might be combined with other databases to construct a more robust portrait of an individual.[10] This would be an important issue to verify in the contract with prepaid card vendors.

When the risk of immigration-related subpoenas was discussed, the prepaid card companies stated that this had never occurred before and that the law enforcement agency would already have to have identified an individual (or individuals) before asking the card companies for additional information. CBA program administrators also seemed to feel that the risk of prepaid card company information being targeted by immigration enforcement actors was low.

Privacy advocates and scholars have noted that there are loopholes that law or immigration enforcement actors might choose to exploit, such as the third-party doctrine. Under this doctrine, the Fourth Amendment does not afford the same protection for information handed over to third parties, like prepaid debit cards or the cloud-based storage of CBOs, as individuals surrender a reasonable expectation of privacy by entrusting their information to someone else.[11,12] To subpoena records under this approach, law enforcement needs not show probable cause, only that the information is reasonably related to an ongoing investigation, which, according to one expert, is a very low threshold. Additionally, prepaid cards have been under scrutiny in the past by law enforcement because of their use in money laundering, fraud, and cross-border trafficking. In December 2006, ICE published a memo regarding the threats associated with prepaid cards and how they could be used to enable trafficking and financial crimes.[13] Where a subpoena is overly broad or burdensome, however, there can be opportunities to respond legally, such as if a prepaid card provider has hundreds of thousands of records and ICE subpoenaed all of them.

Despite this concerning backdrop, based on conversations with program managers and partners, even though law enforcement might try to access a prepaid card provider's database of registered users, the likelihood that they would be subpoenaed appeared to be low. As one CBA program manager from Chicago said, "There's a clear pattern in how ICE operates [...] it's mainly around enforcement, for example, people getting pulled over by police. That is usually the pipeline towards deportation." Still, there are some additional steps that program administrators might consider taking, such as adding noise to the prepaid card dataset by requesting non-sequentially numbered debit cards or cards from multiple providers.

5 Follow-Up: Ongoing Monitoring and Data Storage/Retention

The speed with which municipalities and CBA program administrators mobilized the funds, targeted and approved beneficiaries, and disbursed the cash has been impressive. Unfortunately, at the time of writing, is not clear when the United States will recover from COVID-19 and the resultant economic crisis. There is likely to be longer-term need for assistance among these vulnerable populations who have been hit hard by the economic downturn and excluded from the official safety net.

All programs should specify data retention protocols

However, despite this uncertain future, it is important for CBA program managers to specify retention periods for applicants' and beneficiaries' personal data within their own databases as well as their partners'. Under the European Union's General Data Protection Regulation (GDPR)—an omnibus data protection bill often considered the gold standard for data protection globally—organizations are required to be able to clearly define the period for which personal data will be stored or, if not possible, criteria to determine that period.[14] Encouragingly, a number of programs already have clear parameters in mind. In Los Angeles the city planned on keeping documents collected during the application for a month. Other programs, including in Chicago and Colorado, retain documents only until any necessary audits are complete. In another municipality, all applicant and beneficiary information will be deleted by the end of 2020.

Program managers must also have clear requirements with their partners, whether CBOs and/or prepaid card providers, on the deletion of both PII and de-identified data. One program manager discussed the possibility of shifting a card from non-reloadable to reloadable in order to link beneficiaries with additional funds and services. On a technical level, this shift could be done easily on the vendor's backend. From CFI's perspective however, this shift would be problematic at several levels given that beneficiaries signed onto the service assuming that: a) their data would be deleted, and b) the card was not reloadable. Additionally, there are additional know-your-customer (KYC) requirements that kick in for reloadable cards that would likely require collecting even more information from beneficiaries. While reloadable cards might be a good idea for future programming efforts, it seems unwise to build it off these programs.

Notes

1 Burt Helm, "Credit card companies are tracking shoppers like never before: Inside the next phase of surveillance capitalism," Fast Company, May 12, 2020, https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism

2 David Medine, "Making the Case for Privacy for the Poor," CGAP, https://www.cgap.org/blog/making-case-privacy-poor

3 Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick, "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans," Washington University Law Review 95 (2017), 53, https:openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview

4 "Putting the Principles to Work: Detailed Guidance on the Client Protection Principles" The Smart Campaign, June 2019, https://www.smartcampaign.org/storage/documents/2019_06_19_Principles_Guidelines_FINAL2.pdf

5 Interaction with law enforcement is one of the primary ways that ICE identifies and detains people. Almost 37 percent of ICE arrests nationwide involve local jails and ICE's Criminal Alien Program, a program which identifies undocumented individuals in federal, state, and local prisons and jails and can take them into custody, regardless of if they have been charged with a crime.

6 McKenzie Funk, "How ICE picks its targets in the surveillance age" The New York Times, October 2, 2019, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html

7 Dulce Gonzalez, Michael Karpman, Genevieve M. Kenney, and Stephen Zuckerman, "Hispanic Adults in Families with Noncitizens Feel the Economic Fallout From Covid-19", The Urban Institute,May 2020, https://www.urban.org/research/publication/hispanic-adults-families-noncitizens-disproportionately-feel-economic-fallout-covid-19

8 As defined by the CFPB, "A prepaid card is not linked to a bank checking account or to a credit union share draft account. Instead, you are spending money you placed in the prepaid card account in advance. This is sometimes called 'loading money onto the card.'" "What is the difference between a prepaid card, a credit card, and a debit card?" Consumer Financial Protection Bureau, https://www.consumerfinance.gov/ask-cfpb/what-is-the-difference-between-a-prepaid-card-a-credit-card-and-a-debit-card-en-433/

9 "Executive Summary of the 2018 Prepaid Amendments" CFPB, January 25, 2018. https://files.consumerfinance.gov/f/documents/cfpb_prepaid_executive-summary_2018-amendments.pdf

10 Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy "The New York Times, December 19, 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

11 Dina Moussa "Protecting Privacy in our Financial Transactions: An Alternative Method to Thinking About our Privacy in the Digital Era" Geo. L. Tech. Rev. 342 (2017) https://perma.cc/5LSY-RD7S

12 In the most recent Supreme Court Ruling on the third-party doctrine, Justice Sonia Sotomayor has cautioned that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"....because this "[t]his approach is ill suited to the digital age." Source: Michael C. Pollack, "Taking Data" The University of Chicago Law Review , Vol. 86, No. 1 (January 2019), pp. 77–142

13 "Prepaid Cards as an Emerging Threat" The Cornerstone Report 3, issue no. 2 (December 2006), https://www.ice.gov/doclib/news/library/reports/cornerstone/cornerstone3-2.pdf

14 "General Data Protection Regulation" Official Journal of the European Union, May 4, 2016.

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