

8 REASONS WHY NYC COUNCIL SHOULD REJECT IDNYC “SMART CHIP” PLAN and preserve IDNYC as a secure identification card program

Compiled by Immigrant Defense Project, Make the Road New York, New Economy Project,
New York Civil Liberties Union, New York Immigration Coalition

December 9, 2019

This document responds to misleading and erroneous claims by the NYC administration about its current IDNYC smart chip “exploration.” The points below underscore the serious privacy, surveillance, financial, and other risks to which the smart chip plan would expose New Yorkers, and which lead us to oppose the plan. Over the past year, our organizations and others have participated in extensive meetings with the administration and City Council about the plan, and submitted testimony, comment letters and memoranda detailing our opposition. Despite the widespread concerns, the administration continues to pursue and promote the addition of a smart chip to the IDNYC.

We urge the NYC Council to pass Int. 1706, which would prohibit the addition of a smart chip to IDNYC cards and preserve IDNYC as a secure identification card program — as it was designed.

The City of New York’s IDNYC program has provided vital, safe, and equitable access to government-issued photo ID to more than a million New Yorkers. Our organizations were key members of the coalition that helped to develop, promote, and build public support and confidence in the program, working closely and productively with the de Blasio administration and City Council. The IDNYC “smart chip” exploration jeopardizes this progress. IDNYC is simply not an appropriate vehicle for the kind of financial technology the administration is proposing to embed in the cards.

If the City is serious about promoting financial inclusion, the City should work with community and other stakeholders to pursue progressive, equitable approaches that in fact achieve this critical goal.

The reality is that there is no simple product “fix” or tech solution to deeply-entrenched banking disparities. Rather, given the structure of our banking system, any meaningful solutions will require action by all levels of government. Fortunately, there are concrete actions the City can and should take, for example, to secure banks’ acceptance of IDNYC, building on the program’s five-year track record of success; support creation and expansion of cooperative and community-based financial institutions, through programmatic, policy and funding support; and work toward creation of a municipal public bank. These and other strategies will require the City’s concerted engagement with policymakers, community groups, advocates, experts, and New Yorkers to overcome long-entrenched inequities — and we look forward to working with the City to pursue this vital goal.

Opposition to the IDNYC smart chip plan is broad. Sixty-six New York-based organizations — including community, labor, immigrant, civil rights, legal services, and economic justice groups — submitted a [letter](#) (attached) to Mayor de Blasio expressing their “united and unqualified opposition” to the plan. Several others submitted testimony at an October 2, 2019 NYC Council Immigration Committee Hearing (excerpts of which are also attached). We additionally have consulted with local and national experts, who affirm our assessments of the vast risks to which the proposal would expose the very New Yorkers that IDNYC is intended to support.¹

¹ See <https://www.nydailynews.com/news/politics/ny-pol-immigration-advocates-idnyc-smart-chip-financial-20190211-story.html> and <https://thecity.nyc/2019/09/reject-idnyc-payment-chip-over-data-security-say-councilmember-and-coalition.html>

1. Contrary to the administration’s claims, the IDNYC smart chip plan would NOT expand banking access in underbanked communities.

Embedding a smart chip in IDNYC cards would not “eliminate banking deserts” or increase the number of banks and credit unions that accept IDNYC to open accounts and provide other services. What the plan would purportedly offer, in partnership with a financial technology (“fintech”) company, is a prepaid card-like “account” through which people could load and spend money—effectively turning IDNYC into a payment card. **This is NOT equivalent to expanding access to banks and credit unions and the range of services and legal protections they provide.**

Prepaid cards and their ilk offer a limited and inferior form of financial access, compared to bank and credit union accounts. For example, funds in a bank or credit union account are federally-insured up to \$250,000, and protected by strong state and federal consumer laws. By contrast, prepaid cardholders’ funds are not automatically fully protected. Prepaid card and related fintech companies do not provide branches or personnel that customers can readily access. They do not have legal obligations to reinvest in communities, and are not subject to the same financial regulations as banks or credit unions. These deficiencies have contributed to a number of prepaid card failures, including in hybrid identification-prepaid card programs attempted elsewhere.²

Crucially, embedding fintech of any kind in IDNYC cards would undermine the primary intent of IDNYC: providing New Yorkers with a *secure* form of government-issued, photo identification. The fintech industry is notorious for data breaches and a business model that relies on the collection and sale of people’s personal data.³ Considering that an IDNYC financial partner would be required under federal banking rules to collect and retain customers’ personal identifying documents, these risks are not hypothetical. In short, the IDNYC smart chip plan would likely perpetuate, rather than resolve, inequality in our banking system.

2. The IDNYC smart chip plan does NOT come from local communities or respond to needs articulated by IDNYC cardholders.

The administration has claimed that its IDNYC smart chip “exploration” responds to community and IDNYC cardholder demand. In fact, in 2014, the municipal ID coalition rejected the idea of attaching a prepaid card feature to IDNYC cards, for the same reasons groups today oppose this dangerous plan. Despite the coalition’s longstanding concerns, and without further consultation, the administration issued its IDNYC smart chip solicitation in May 2018.⁴

In April 2019—almost a year after launching its smart chip “exploration”—the administration conducted focus groups of 36 New Yorkers, in an apparent attempt to demonstrate community support for the smart chip plan. The City’s “April 17, 2019 IDNYC Card & “Smart Chip” Exploratory Study,” which reports on

² See, e.g.: <https://www.consumerfinance.gov/policy-compliance/enforcement/actions/unirush-llc-and-mastercard-international-incorporated/> and <https://www.sfgate.com/bayarea/article/Oakland-debit-card-fees-draw-criticism-4368734.php#ixzz2O5Nxqfka>

³ See, e.g. <https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector>

⁴ See <https://tech.cityofnewyork.us/2018/05/22/idnyc-nycx-rfej>; <https://www.nydailynews.com/news/politics/ny-pol-idnyc-philip-thompson-mastercard-20190111-story.html>; <https://statescoop.com/former-new-york-technology-chief-miguel-gamino-joins-mastercard/>

these focus groups, is profoundly limited and confirms only that survey recipients are concerned about their privacy and security. The research method included only a tiny sample (36 people, many of whom did not have IDNYC cards), without statistical or scientific controls. From the questions asked in the survey, it is difficult to distinguish if the City is discussing access to a bank account, which is a desire shared by many people in the survey, or if people are looking for a prepaid card with a “chip.” (As noted above, the addition of a chip to the IDNYC does nothing to give unbanked people access to a bank account.)

Indeed, the clearest focus group response revealed IDNYC cardholders’ significant concerns about any tracking of their card use. The City’s study report articulates respondents’ desire for robust privacy guarantees and a strong preference to resist any technology that could be used for tracking the cards. Similarly, the City’s August 2016 survey of more than 77,000 IDNYC cardholders found that the “single greatest reason people hesitated to get the ID was related to concerns that it was being used to monitor New Yorkers.”⁵ The 2016 survey also cited cardholders’ desire for more banks to accept IDNYC.

Cardholders’ concern over personal privacy should therefore be the starting point of analysis when considering any new design or technology elements. Contactless cards, which the administration is proposing, simply cannot meet the privacy and security need for minimizing tracking. Because RFID (Radio Frequency Identification) wireless implementation is passively powered by a secondary device (the device designed to read the card’s data), the ability to track it cannot be turned off. The person with the card reader controls the distance at which the card can be read—because the card is a tag that responds to radio waves.⁶ This enables any prospective card-reader (including hackers, law enforcement, or anyone else with the equipment and motivation) to access at least certain information from a card with contactless technology—without the knowledge or consent of the cardholder. There is little question that among the data that could be “sniffed” remotely is the simple fact that a person carries an IDNYC card—data that itself may be of immense interest to immigration authorities, for example.

3. The IDNYC smart chip plan is NOT mandated by the program’s enabling legislation, and presents reputational risks for NYC.

The administration has claimed that its fintech smart-chip pursuit responds to a “directive” by City Council. In fact, Local Law 35 of 2014, which established the City’s municipal ID card program, provides that the City shall: *seek to ... expand the benefits associated with the card, including, at a minimum, by promoting acceptance of the card by banks and other public and private institutions.*

Embedding smart chip technology directly into IDNYC cards—and designing a financial product, through contractual obligations that the City would be responsible for monitoring and enforcing—goes far beyond promoting acceptance of IDNYC cards by existing financial institutions. The administration claims that it would provide for consumer protections via its contract with vendors, but fails to explain whether or how the City would identify or enforce any breaches of any such contracted-for protections. Would the City set up the infrastructure necessary to assist the potentially hundreds of thousands of New Yorkers harmed by

⁵ See https://www1.nyc.gov/assets/idnyc/downloads/pdf/idnyc_report_full.pdf

⁶ See https://www.nyclu.org/en/publications/testimony-new-york-civil-liberties-union-opposition-smart-chip-being-added-idnyc#_ftn8

any contractual breaches? Would the City seek meaningful penalties and restitution from the vendor on behalf of any aggrieved New Yorkers?

The administration’s apparent belief that contracted-for provisions by themselves would be enough to protect IDNYC cardholders from a fintech’s bad acts reflects a fundamental misunderstanding of how difficult it can be for fintech customers to obtain any meaningful redress. We have seen fintechs brazenly flout state and federal consumer protection laws and cause grievous harm to low-income New Yorkers, who are subsequently unable to get any meaningful assistance from the fintechs’ so-called customer service departments. Unless the City were to commit significant resources to assisting IDNYC cardholders in need, the burden would likely fall heavily on NYC legal services organizations, which are already operating beyond capacity.

4. The ability to remotely identify contactless IDNYC cards is NOT “theoretical or unlikely.”

The City claims that remotely reading whether someone carries a contactless IDNYC card would only occur in a “theoretical and extremely unlikely scenario.” To the contrary, this is neither theoretical nor unlikely given ICE’s capacity and incentive. Identification of the type of contactless card someone carries can happen irrespective of encryption method and is enabled through the NFC (Near-Field Communication) protocol when initializing a communication between reader and card. By way of implementing the requested ISO 14443 A/B standard, cards would respond to an initial communication request (the technical term here is *ATQ-A/B*) with a response that could reveal the type of card (e.g., whether someone is indeed carrying an IDNYC).⁷

In addition, many NFC implementations reveal which applications are stored on a card, further allowing a reader to pinpoint the type, use, or vendor of a card. The NYCLU has conducted tests with passports, payment cards, and transit cards, which all precisely revealed the type of card to a reader. A reader can be something as ordinary as a smartphone with one of the many, free NFC-Reader apps on the Google Play or iOS App Store. Many studies have shown the feasibility of extending the read distance of NFC tags to several feet for active communication, and even farther for passive eavesdropping of an existing communication. Any tracking, hacking, or other unconsented-to communication could therefore happen remotely and unbeknownst to cardholders.

5. The City should NOT allow for an “opt-in” contactless IDNYC card, which would still expose New Yorkers to serious risks.

To date we have not seen any specific information about what an “opt-in” would look like or how card applicants would be informed of the serious surveillance risks. Given the misleading and erroneous information the City has provided thus far, we have no reason to believe that people would be sufficiently informed to make a meaningful decision, particularly given complexities of consumer disclosures.

Embedding technology that could convert *any* IDNYC card into a tracking device undermines the original purpose of the IDNYC program. Community groups have also expressed concerns about creating a “two-tier” IDNYC card program that could create confusion or differing treatment of IDNYC cardholders depending on whether or not the ID has a chip. Since its initial implementation, the administration and

⁷ Here is a list of such responses from thousands of smart cards, which clearly reveal the type of card: <https://archive.md/OXk2v>

community advocates have pushed for all cardholders to have the same IDNYC to prevent any possibility of sorting people based on the ID.

Furthermore, equipping IDNYC cards with a payment function would expose cardholders unnecessarily to risk of lost or stolen funds. No one wants a Visa logo on their passport, and we would not advocate to merge banking functions with a driver’s license—why would we push this for IDNYC cardholders?

6. The administration’s claims about smart chip encryption are incomplete and misleading.

City staffers and third parties engaged by the City have invoked “encryption” as a less-than-specific buzzword to address any privacy or security concerns advocates may have with the proposed changes to the card. The encryption on the card might protect certain information (e.g., Personally Identifiable Information, or PII), but would almost certainly broadcast that the user has an IDNYC card—a harmful revelation that could be weaponized by federal immigration authorities or hackers attempting to prey on vulnerable communities.

The unspecific and overbroad use of the term “encryption” to solve more serious privacy issues is an unfortunately common—but often hollow—refrain in many policy debates. The science of cryptography has provided many important benefits to modern technology and cryptography’s application, in the form of encryption, allows for many confidentiality, integrity and authentication functions that are necessary for everyday information systems, including banking, Wi-Fi, and internet systems. However, invoking encryption to obscure difficult questions about functional electromagnetism is a misunderstanding of which branch in the tree of scientific knowledge a project rests on. Regardless of encryption protocol, RFID/NFC systems reveal their historical bytes to all interested transmitters, because the systems require physical power from the transmitter and must reply in some form to that power.⁸ Encryption simply cannot limit the ability of third parties to surreptitiously sniff RFID/NFC cards at a distance, an ability that will only increase over time, as transmitters become more ubiquitous and powerful.

The ISO (International Organization for Standardization) standardization specifications for NFC are helpful in understanding what the designers of NFC systems are hoping their systems achieve. However, standards are written ideals that do not fully represent how the final system operates in the physical world. NFC is a standard which is designed to have a smaller read range (3-5 cm) than the incredibly broad 250-foot range of normal RFID. That is the ideal in the NFC ISO standards. However, in real life the NFC read range has been shown to be much farther; as much as 3-50 feet for sniffing or reading.⁹ This read range is always controlled by the reader, not the card, which means that as transmitters become more technologically advanced, the readers will have a more extreme range. This problem cannot be solved by encryption. It is a physics problem, to which the City can offer no technical solution other than the prohibition on this type of technology as provided by Intro. 1706.

7. Fraud risks increase with contactless NFC technology.

The City claims that the contactless NFC card uses EMV encryption in a completely secure way that is impervious to fraud. Though it is true that EMV is a successful encryption protocol, adding NFC

⁸ See https://www.nyclu.org/en/publications/testimony-new-york-civil-liberties-union-opposition-smart-chip-being-added-idnyc#_ftn10

⁹ See https://www.nyclu.org/en/publications/testimony-new-york-civil-liberties-union-opposition-smart-chip-being-added-idnyc#_ftn11

contactless technology introduces a significant vulnerability into the protocol’s implementation. This vulnerability is called a relay attack. Relay attacks allow for a nearby person to issue a charge to your NFC card without your knowledge simply by standing close to you and forwarding the charge authorization to another phone near the payment terminal. This doesn’t require the attacker to read or undermine the EMV encryption, it simply allows them to charge a card that is not theirs by successfully undermining the authentication mechanism that NFC relies on. This is an attack that can be carried out with a couple hundred dollars and a few specialized skills.

8. The IDNYC smart chip plan would expose New Yorkers to data collection, privacy and other risks -- undermining the program’s original intent and its track record of success.

Administration officials have spoken publicly about their interest in generating “big data” through IDNYC cards equipped with smart chips. Even if well-intended, connecting this kind of technology and data to vulnerable New Yorkers’ identification cards would expose people to serious risks—including dangerous experimentation or misuse by current or future administrations and private vendors. As data collection about New Yorkers—by private corporations, law enforcement, and others—increases, the City should pursue policies and practices that more vigorously safeguard people’s information or prevent it from being collected in the first place.

From the beginning, community support for IDNYC was rooted in the urgent and immediate need for *secure* government-issued photo ID that New Yorker—particularly for homeless, formerly incarcerated, gender non-conforming, young, undocumented, and other New Yorkers who face obstacles to acquiring other forms of ID. Privacy was a foremost concern from the outset. The Coalition advocated, for example, for the City to not retain any underlying documents presented by IDNYC applicants—the result being the City’s decision to retain documents for two years (rather than five), and to destroy cardholder documents by December 31, 2016.¹⁰ Today, the City no longer retains IDNYC applicants’ underlying documents.

For many New Yorkers, IDNYC is their primary—or sole—form of identification.¹¹ Keeping New Yorkers and their personal information, including purchasing and transit data, safe from law enforcement and surveillance was, and remains, a core principle for IDNYC and its stakeholders. By these measures, IDNYC has been a clear success. The smart chip plan would introduce risks that could undercut this success. As the Trump administration continues to ramp up attacks on immigrants, people of color, and other populations served by IDNYC, the City should do all it can to safeguard New Yorkers and the IDNYC program—not subject them to dangerous experimentation.

¹⁰ Fortunately, the City was able to fight off a legal challenge filed in December 2016 by two State Assembly members, who argued that destroying the records would threaten national security and that the data should be made accessible under NYS’s freedom of information law.

¹¹ According to the City’s 2016 IDNYC evaluation report, half of IDNYC cardholders surveyed use it as their primary ID; for one-quarter of respondents (and 36% of immigrant respondents), IDNYC is their only form of U.S. photo ID. See https://www1.nyc.gov/assets/idnyc/downloads/pdf/idnyc_report_full.pdf

**EXCERPTED TESTIMONY IN SUPPORT OF INT. 1706
TO PROHIBIT A SMART CHIP FROM BEING ADDED TO NYC IDENTITY CARD**

NYC Council Immigration Committee Hearing—October 2, 2019

American Immigration Lawyers Association New York Chapter: “Given the unknown security risks and privacy concerns that can imperil undocumented immigrant holders of a smart chipped IDNYC, and the devastating humanitarian toll on immigrants and their families, AILA-NY is extremely pleased that the City Council is taking a stand against adding smart chips to the IDNYC. We fully support the City Council's effort to prohibit the New York City's government from adding a smartchip to the IDNYC. There are a number of legal, policy and humanitarian reasons why it is critical for New York City to stop adding smart chips to the IDNYC. Far too many noncitizens - both longtime permanent residents and individuals without immigration status - have been swept up by an overzealous immigration enforcement system that does not see them as individuals deserving of rights and respect.”

Association for Neighborhood and Housing Development: “ANHD has been a strong supporter of the IDNYC since its inception, actively encouraging banks to accept it as primary identification and urging the regulators to support this as well. We have serious concerns about adding a so-called smart chip to the card. The risks far outweigh any benefits it might add. FinTechs are not banks and prepaid debit cards are not the same as bank accounts. Products like the prepaid debit cards the city is proposing incorporating as part of IDNYC are symbolic of a two-tier banking system that pushes underserved populations—low-income, minority, immigrants—to prepaid debit cards while higher income customers have access to full-service bank accounts that promote savings and can lay the groundwork to achieving larger financial goals, such as purchasing a home or financing a business. Some banks are rightly moving away from this system. Chase, for example, stopped offering its prepaid card and now offers instead a low-cost no-overdraft bank account. Other banks are introducing low-cost accounts and similar products to help people open an account or re-enter the banking system. Clearly, more needs to be done to improve access to banks and banking, and especially low and no-fee bank accounts, but a FinTech company providing more prepaid debit cards is not the solution.”

Families for Freedom: “IDNYC will no longer serve its purpose of protecting New York City's undocumented population once the smart chip is implemented. The changes will instead put an identifiable electronic signature in every New Yorker's wallet and add them into a mass surveillance system that is ever growing in the metropolis. People can become targets, particularly undocumented immigrants who will be vulnerable to ICE if misused. The uncertainty surrounding who's collecting the data is problematic for us. Some of our people are already on electronic shackles and are being monitored on a daily basis. Many of our members

know what it's like to be surveilled through electronic shackles. Implementing a smart-chip like this in the form of ID is an evolution of what the shackles are right now....This is a form of surveillance technology, no matter how you dress it up with words such as "financially beneficial". Who is really financially benefiting? It certainly isn't for the people.”

HerJustice: Her Justice is extremely concerned about the proposal to add a smart chip to the New York City Identity Card ("IDNYC") because of the increased risk for our clients from both the federal government and from abusers....We support efforts for immigrants to have access to secure banking, credit lines and other benefits of financial institutions. However, adding a chip to the card does not open up a range of banking options for clients to choose, but rather requires a linkage between an important identification document with a financial service. This is yet another form of coercion—one that involves financial services and exposes our clients to risks. A chip in the IDNYC would give the federal government, and potentially private citizens who are actively targeting survivors, access to information that could be used to further harm them.”

Immigrant Defense Project: The tools of police and ICE surveillance, as well as the scale of the state's efforts to identify and track people, have grown immensely over the past 15 years. ...ICE relies on data gathered by a wide array of government and private sources. Increasingly, data collection and analysis is also central to the profit-driven strategy of corporations including the financial technological sector ... Health insurance companies deny coverage or increase rates based on gathering "lifestyle" data. Globally, police regularly access smartcard data from transit usage. Privacy and security experts that we have consulted with have highlighted other concerns with this proposal: creating multiple datasets tied to the ID; narrowing the pool of IDNYC cardholders by offering (or requiring) services that are most likely to be used by people without other options, makes it easier to deanonymize the data; and "function creep"—the gradual widening of uses beyond original stated purpose—associated with ID integrations.

Legal Aid Society: “The City's proposal would expose undocumented and other vulnerable New Yorkers to financial, surveillance, and privacy risks, without expanding equitable access to banking. The Society is concerned about the lack of transparency in the development of the City's plans to integrate a smart chip with access to financial and other services. We applauded Mayor De Blasio's initial development and launch of the IDNYC program, for which extensive input was sought and received from stakeholders, including community-based organizations, advocates, and financial institutions. The current plans have moved forward quickly without proper consultation or engagement with stakeholders and the public. The Society has long supported the expansion of access to financial services to unbanked and underbanked New Yorkers. Yet, any solution must be community-informed and prioritize equity and security, and must not expose cardholders to undue risk.”

Lower East Side People’s Federal Credit Union: “We believe in the initial goal of the IDNYC program, to provide required identification so that individuals could access a complete range of

financial services. Reloadable cards come with a heavy cost, not only in terms of dollars but in lack of consumer service and consumer protections that our low-income and immigrant New Yorkers simply cannot afford. Lower East Side Peoples Federal Credit Union's community organization partners do not ask for prepaid cards, they ask for their members and clients to have: multi-lingual trained professionals who can thoroughly answer financial questions; physical branches where people can meet and reach trusted credit union representatives; access to quality financial products including low cost savings and checking accounts which help people build assets and leads them to economic security; access to fair and affordable credit; Immigrant services such as ITIN lending, DACA loans, international money wiring, etc.; and acceptance of the IDNYC as a standalone ID to open an account.”

Make the Road New York: “We don't want third parties having our information, we don't want the possibility of being tracked or surveilled when we take the subway and we don't want to further create databases with this program, we don't want opt-in options. We know surveillance, data storage or tracking of a lot of our lives already happens in different ways but we can say that is not due to IDNYC and we want to keep it that way. We understand MOIA wants to help banking deserts and bring more benefits to New Yorkers, and while we commend this thinking we don't think a chip or contactless technology in our ID NYC gets to the roots of the problems as to why banking in low income, poor and/ or communities of color are an issue or why more people don't have bank accounts. We do think the city can look into expanding the perks and who signs on to obtain the ID NYC without jeopardizing a program that is working.”

New Economy Project: “New Economy Project unequivocally objects to the administration’s planned integration of IDNYC with financial services, MTA, and other systems. Such sweeping integration would result in massive data collection about IDNYC cardholders and expose undocumented and other New Yorkers to serious privacy, surveillance, and financial risks. Our organization fights for fair access to banking -- but this is not the way to achieve that. For decades, prepaid debit card companies have touted their product as a solution to “banking deserts” and, for decades, the rhetoric has failed to match the reality. There is no compelling reason for the City of New York to steer IDNYC cardholders to this service, much less to connect it to people’s identity cards. ”

New York Civil Liberties Union: “The NYCLU supports Intro. 1706 because it ensures that the IDNYC cards do not contain any tracking or surveillance technology that could create grave risks for the vulnerable population served by the IDNYC. Its passage will help ensure that this government identification card continues to serve vulnerable communities by building on its most important asset – community trust.”

New York Immigration Coalition: “The proposed changes to the IDNYC program at the heart of today’s hearing go far beyond IDNYC’s original intent of providing safe, government-issued photo ID to immigrant, homeless and other New Yorkers who face barriers to securing other

forms of government-issued ID. In fact, it runs completely contrary to the initial goal of the program. It effectively creates a re-envisioned program that sacrifices the safety and security of the cardholders, who most rely on the IDNYC program, and trades it for potential new benefits that would be best delivered by a completely different program. The most important principle of the program, that the benefits always far outweigh the risks, is lost.”

Planned Parenthood of New York City: “Planned Parenthood of NYC opposes the addition of smart chips or financial technology in IDNYC cards. The addition of a smart chip could harm New Yorkers by creating a means through which people could be tracked, posing a threat to their safety and quality of life. This technology also poses a concern about financial strains that result from the additional fees that will be associated with the IDNYC once the microchip is added...the proposed changes to the IDNYC would undermine equal access to government-issued identification and instill fear in our undocumented and immigrant patients. With the addition of a smart chip, vulnerable New Yorkers could be tracked through their daily lives including by the MTA, financial institutions, private artificial intelligence companies, and the government, who in turn would be making a profit off them.”

SEIU 32BJ: “While we commend efforts to address banking deserts, these efforts should not be carried out in a way that would undermine other important City priorities. The New York City Identification Card (IDNYC) was originally created to address the needs of vulnerable populations such as undocumented immigrants, the homeless, and transgender people. The addition of a “smart chip” to the ID would risk discouraging these populations from obtaining the ID. Attempting to increase access to financial services might result in decreasing access to other crucial services such as SNAP, Cash Assistance, Section 8, NYC health services, library access, and so on. Those who continue to use the card may be putting their private information at risk, whether to hackers or to federal agencies like ICE. This is why multiple community groups have said that they would discourage the use of the IDNYC if a smart chip was added.”

Surveillance Technology Oversight Project: “Mayor de Blasio’s proposal to equip IDNYC with RFID tags will risk nothing less than mass surveillance....Since IDNYC is thousands of New Yorkers’ only ID, its use with [MTA’s new fare-payment system] OMNY would empower the MTA to transform the card into a tool of suspicionless surveillance. The data collected by IDNYC card processors will be nothing short of a treasure trove. But it won’t be held by the City, instead, it will be controlled by banks and credit card networks...And since many IDNYC cardholders are undocumented, location and merchant patterns could be used to create a target list for raids. We should note that the privacy impact is exacerbated by existing NYPD data sharing agreements with federal agencies. City officials responded before to these exact same privacy threats. They put in safeguards....So how can the Administration move forward with this proposal when none of these requirements extends to private sector partners? How can they use RFID technology that exposes cardholders to data breaches and identity theft?”

LETTER TO MAYOR DE BLASIO OPPOSING IDNYC SMART CHIP PLAN

September 12, 2019

[Resubmitted on October 2, 2019 with additional signatories]

Mayor Bill de Blasio
City Hall
New York, NY 10007

Dear Mayor de Blasio:

The undersigned community, labor, immigrant, civil rights, legal services, and economic justice organizations write to express our united and unqualified opposition to the administration's plan to add financial technology and a host of integrations to NYC's municipal identification (IDNYC) cards, which are held by more than 1.2 million New Yorkers.

We call on you to halt the City's pursuit of this dangerous, corporate-driven plan, which threatens to erode public confidence in IDNYC and expose cardholders -- particularly immigrant New Yorkers -- to serious privacy, surveillance, consumer protection, and other unwarranted risks. These very real risks far outweigh any purported benefits the plan would provide to New Yorkers.

Our organizations include leading members of the coalition that worked to design, promote, and help launch IDNYC in 2015. Collectively, we represent hundreds of thousands of low-income, immigrant, senior, homeless, and other New Yorkers who have benefited tremendously from IDNYC. Our opposition to the proposed IDNYC changes is rooted in our desire to protect the integrity of this vital program, and in our decades of work and expertise on privacy, consumer protection, immigration, financial services, federal surveillance, deportation and other relevant matters. Over the past year, many of our organizations have communicated our detailed concerns and steady opposition to this plan. We have participated in phone and in-person meetings with your administration, testified at a City Council IDNYC oversight hearing, submitted detailed memos, engaged community members, and consulted with national experts who have affirmed our assessments of the vast risks to which the proposal would expose the very New Yorkers that IDNYC is intended to support.

Last year, your administration began soliciting proposals from financial firms to host an EMV/RFID "smart chip" on IDNYC cards. According to the solicitation, the chip would allow cardholders to load funds onto their IDNYC cards, make payments to private vendors, and enable "integrations with public and private partners, such as the MTA's planned contactless fare payment system and NYC Health + Hospitals medical records."

If implemented, the proposed changes to IDNYC would facilitate unprecedented, wide-scale data collection about New Yorkers' travel, spending, and other activities. Indeed, administration officials have spoken publicly about their express interest in generating "big data" and revenue through IDNYC cards equipped with smart chips. Even if well-intended, connecting this kind of technology and data to vulnerable New Yorkers' identification cards would expose people to serious risks -- including dangerous experimentation or misuse by current or future administrations and private vendors -- that far outweigh any potential benefits. These risks are

particularly heightened given the Trump administration's escalating attacks on immigrant communities.

The administration has asserted that an IDNYC-financial technology (fintech) partnership would "eliminate banking deserts." This is false. Fintech companies are not banks. They do not provide branches and personnel that customers can readily access. They do not have legal obligations to reinvest in communities. And they are not subject to the strong, uniform federal regulations and consumer protections that govern banks and credit unions. Moreover, the fintech industry is notorious for data breaches and a business model that relies on the collection and sale of people's personal data. By steering undocumented and low income New Yorkers to these entities, the City would be perpetuating, not resolving, inequality in our banking system and potentially facilitating IDNYC cardholders' exploitation.

According to the City's own research, IDNYC cardholders want access to actual banks and credit unions. In fact, more than 9,000 people used IDNYC successfully to open bank and credit union accounts in the program's first year. The same research found that the top reason New Yorkers hesitated to get an IDNYC card was the concern that it was being used to monitor people. IDNYC cardholders simply are not clamoring for the type of "banking solution" that this proposal would advance. Recently, immigrant communities won passage of NYS Green Light legislation, which will allow undocumented New Yorkers to obtain driver licenses; this will go far to expand equitable and safe banking access for hundreds of thousands of New Yorkers.

The IDNYC fintech proposal is neither progressive nor effective. NYC is home to a robust landscape of nonprofit economic justice and immigrant rights activists; community reinvestment and fair lending advocates; consumer law attorneys; community development financial institutions; and many others that are eager to work with your administration to advance truly progressive solutions to bank redlining and economic inequality.

IDNYC was created for -- and must continue to prioritize the safety of -- undocumented, homeless, and other New Yorkers who, more than ever, face real privacy and surveillance risks. The proposed changes to IDNYC are antithetical to the program's original purpose and scope, and would expose New Yorkers to unprecedented risks at a time when they can least afford to be subjects of such experimentation. For the security and stability of our communities, we call on you to ensure that this exploration comes to an end.

For further information, please feel free to contact Mizue Aizeki, Deputy Director, Immigrant Defense Project (maizeki@immigrantdefenseproject.org); Natalia Aristizabal, Co-Director of Organizing, Make the Road New York (natalia.aristizabal@maketheroadny.org); Deyanira Del Rio, Co-Director, New Economy Project (dey@neweconomynyc.org); Betsy Plum, Vice President of Policy, New York Immigration Coalition (eplum@nyic.org); or Daniel Schwarz, Privacy & Technology Strategist, New York Civil Liberties Union (dschwarz@nyclu.org).

Signed,

African Communities Together
ALIGN
Arab American Association of New York
Association for Neighborhood and Housing Development
The Black Institute

Brandworkers
Brooklyn Cooperative Federal Credit Union
Brooklyn Defender Services
Cabrini Immigrant Services of NYC, Inc.
CASA – New Settlement Apartments
Center for Family Life in Sunset Park
Center for Popular Democracy
Chinese Progressive Association
Citizen Action - NYC
Common Cause/NY
Community Solutions
Cooper Square Community Land Trust
District Council 37
DRUM – Desis Rising Up & Moving
East Harlem-EI Barrio Community Land Trust
Families for Freedom
Frank Pasquale, author of *The Black Box Society*
Freedom to Thrive
GOLES
Green Worker Cooperatives
Housing Court Answers
Immigrant Defense Project
Inclusiv
Interfaith Center on Corporate Responsibility
Justice For Our Neighbors
LatinoJustice PRLDEF
The Legal Aid Society
Legal Services Staff Association, NOLSW/UAW 2320
Lower East Side People's Federal Credit Union
Make the Road New York
Men Talk
MinKwon Center for Community Action
Mixteca Organization, Inc.
Mobilization for Justice, Inc.
National Center for Law and Economic Justice
Neighborhood Defender Service
New Economy Project
New Immigrant Community Empowerment
New Sanctuary Coalition
New York Civil Liberties Union
New York Communities for Change
New York Immigration Coalition
New York State Youth Leadership Council
NYC Network of Worker Cooperatives
Pan-African Community Development Initiative
Peter Cicchino Youth Project of the Urban Justice Center
Queens Law Associates
Red de Pueblos Transnacionales

SEIU 32BJ
South Bronx Unite
S.T.O.P. - Surveillance Technology Oversight Project
TakeRoot Justice
UAW Region 9a New York Area CAP Council
UHAB
UnLocal, Inc.
Upturn
Violence Intervention Program, Inc.
Volunteers of Legal Service
The Working World
Worth Rises
Youth Represent

cc:

NYC Council Speaker Corey Johnson
NYC Council Member Carlos Menchaca
NYC Council Member Daniel Dromm
Commissioner Steven Banks, Human Resources Administration
Commissioner Bitta Mostofi, Mayor's Office of Immigrant Affairs
Laura Negrón, Chief Privacy Officer for the City of New York
Commissioner Lorelei Salas, Department of Consumer and Worker Protection
J. Phillip Thompson, Deputy Mayor for Strategic Initiatives