ID4D
IDENTIFICATION FOR DEVELOPMENT

Public Sector Savings and Revenue from Identification Systems:

Opportunities and Constraints

WORLD BANK GROUP

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Contents

About ID4D iii

Acknowledgments iv

Acronyms v

Executive Summary vi

1. Introduction 1

Methodology 1

Scope 2

Organization 3

2. The Potential of ID for Fiscal Savings and Revenue 4

2.1. Key Features 4

Digitization 6

Unique Identifiers 7

Integration and Interoperability 8

Digital Authentication 9

2.2. Conditions and Constraints 10

3. Evidence of Savings and Revenue 12

3.1. Reducing Fraud in G2P Transfers 13

Eliminating Multiple or Ghost Enrollments 15

Identifying Ineligible Beneficiaries 20

Preventing Impersonation and Leakage 22

3.2. Reducing Administrative Costs 23

Reducing Transaction Costs 25

Eliminating Redundancy in Identification Systems 27

3.3. Increasing Tax Collection 29

3.4. Charging User Fees 32

3.5. Additional Sources of Savings 34

4. Guide for Practitioners: Toward a Savings Model 37

4.1. Assessing Savings and Revenue Opportunities 37

Reducing Fraud Targeting in G2P Transfers 37

Reducing Administrative Costs 42

Increasing Tax Collection 45

Charging User Fees 47

4.2. Key Considerations 48
Cost of Systems 49
Exclusion 49
Privacy and Fair Use 50
Vested interests 51
5. Conclusion 52
References 53
Appendix: Cases 58

Tables

Table 1: System Features Associated with Fiscal Savings and Revenue 5
Table 2: Mechanisms for Public Sector Savings and Revenue from ID Systems 12
Table 3: Identity-Related Fraud in G2P Programs 14
Table 4: Role of Identification Systems in Reducing Transaction Costs 25
Table 5: Stylized Example of Reduced Fraud from Identification Systems 39
Table 6: Suggested Metrics for Evaluating the Effect of Identification Systems on Fraud 42
Table 7: Example Inventory of Identity-Related Assets and Procedures 43
Table 8: Exclusion Errors vs. Fraud Detection 50

Figures

Figure 1: Identity Lifecycle 6
Figure 2: Endogenous Factors That Constrain the Fiscal Benefits of Identification Systems 10
Figure 3: Pathways to Savings by Reducing Fraud in G2P Transfers 15
Figure 4: Pathways to Savings by Reducing Administrative Costs 24
Figure 5: Pathways to Generating Revenue by Increasing Tax Collection 30
Figure 6: Pathways to Generating Revenue by Charging Fees for Identity Services 32
Figure 7: Illustration of the Difficulties in Measuring Fraud Reduction in G2P Registers 41
Figure 8: Stylized Savings from Reducing Transaction Costs for Identity Verification/Authentication 44
Figure 9: Potential Effects of ID on Tax Collection 46

About ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from World Bank Group, Bill & Melinda Gates Foundation, and Omidyar Network.

To find out more about ID4D, visit worldbank.org/id4d.

Acknowledgments

This report was authored in 2018 by Julia Clark as part of the Identification for Development (ID4D) initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions. It was made possible through the generous support of the partners of the ID4D Multi-Donor Trust Fund (Bill & Melinda Gates Foundation and Omidyar Network).

This report benefited greatly from the inputs and reviews of the World Bank Group staff including Robert Palacios, Luda Bujoreanu, Jonathan Marskell, Kamya Chandra, Anna Metz, Anita Mittal, Rinku Murgai, Ernest Wasake, Cem Dener, Ana Bellver, Bernard Haven, Sebastian S. James, Joey Raymond Ghaleb, Raul Felix Junquera-Varela, Marijn Verhoeven, Carlo Rossotto, Ambrish Shahi, and John Blomquist, under the supervision of Vyjayanti Desai.

In addition, this report would not have been possible without the insights and feedback provided by Dr. Pan Ananapibut (Ministry of Finance, Thailand), Dasha Cherepennikova (One World Identity), Alan Gelb (Center for Global Development), Kaelyn Lowmaster (One World Identity), Tariq Malik (former chair of NADRA, Pakistan), Patricia Mongkhonvanit (Revenue Department, Thailand), Ilan Muhereza (Ministry of Public Service, Uganda), Felix Ortega (RENIEC, Peru), Rehman Qamar (NADRA, Pakistan), Arun Sharma (DBT Mission, India), and Jaap van der Straaten (CRC4D).

Acronyms

AP	Andhra Pradhesh (India)
APBS	Aadhaar Payment Bridge System (India)
API	Application Program Interface
BISP	Benazir Income Support Program (Pakistan)
CNIC	Computerized National Identity Card (Pakistan)
CUIT	*Código Único de Identificación Tributaria* (Argentina)
DBTs	Direct Benefits Transfers
DHA	Department of Home Affairs (South Africa)
eID	Electronic Identity Document
FPS	Fair Price Shop (India)
FRR	False Rejection Rate
G2P	Government-to-Person
ICT	Information and Communications Technology
IDPs	Internally Displaced Persons
IEC	Independent Electoral Commission (South Africa)
IPPIS	Integrated Payroll and Personnel Information System (Nigeria)
IRS	Internal Revenue Service (United States)
KYC	Know Your Customer
LPG	Liquefied Petroleum Gas (subsidies, India)
MEC	Malawi Electoral Commission (Malawi)
MOAC	Ministry of Agriculture and Cooperatives (Thailand)
MPS	Ministry of Public Service (Uganda)
NADRA	National Database and Registration Authority (Pakistan)
NID	National ID
NIDA	National Identity Agency (Rwanda) or National Identification Authority (Tanzania)
NIN	National Identity Number
NIRA	National Identification and Registration Authority (Uganda)
NIST	National Institute of Standards and Technology (US)
NREGS	National Rural Employment Guarantee Scheme (India, aka MNREGA, MNREGS)
OMCs	Oil Marketing Companies (India)
OTP	One-Time Password
PAHAL	Pratyaksha Hastaantarit Laabh (India)
PAN	Permanent Account Numbers (India)
PDS	Public Distribution System (India)
PKI	Public Key Infrastructure
POS	Point-Of-Service
QR code	Quick Response code
RENIEC	*Registro Nacional de Identificación (*Peru)
SINTyS	*Sistema Nacional de Identificación Tributaria y Social* (Argentina)
SSP	Social Security Pensions (India)
SSN	Social Security Number (US)
UID	Unique Identifier (e.g., a UIN)
UIDAI	Unique Identification Authority of India (India)
UIN	Unique Identity Number
VAT	Value-Added Taxes

Executive Summary

Background

Inclusive and robust identification systems can offer many concrete benefits for governments, as well as individuals, private companies, and development partners. By providing a secure and accurate way of identifying the population, these systems can facilitate the delivery of a wide variety of services that expand financial inclusion, boost economic opportunities, improve access to social safety nets, increase gender equality, and more. In addition to these developmental uses, evidence suggests that strong identification systems have the potential to generate savings and revenue for the public sector, to the tune of millions of dollars per year (or even billions for larger economies).

To date, however, our understanding of the full fiscal impact of identification systems is limited due to the scarcity of publicly available data and the methodological challenges associated with quantifying and attributing the effects of these systems. This paper is a first step toward filling this gap. Using the experiences of a handful of countries where data are available, it attempts to summarize existing case studies and build a framework for analyzing the potential fiscal benefits associated with investment in identification systems, including the features, mechanisms, and conditions that may generate (or limit) savings and revenue.

In addition to aggregating existing knowledge and developing an analytical framework, this paper also provides a *Guide for Practitioners* with concrete steps to assist governments and other stakeholders when estimating expected savings and revenue from investment in identification systems. In order to conduct a full cost-benefit analysis, readers are encouraged to consult a complimentary World Bank report on the cost of identification systems (World Bank 2018d) and a companion paper on the financial benefits of these systems for the private sector (World Bank 2018c). We hope that these resources will not only broaden the evidence base and tools available to implementers, but will also encourage practitioners and researchers to undertake more rigorous evaluations of the impact of identification systems on public finances and the broader economy.

The Potential of ID for Fiscal Savings and Revenue

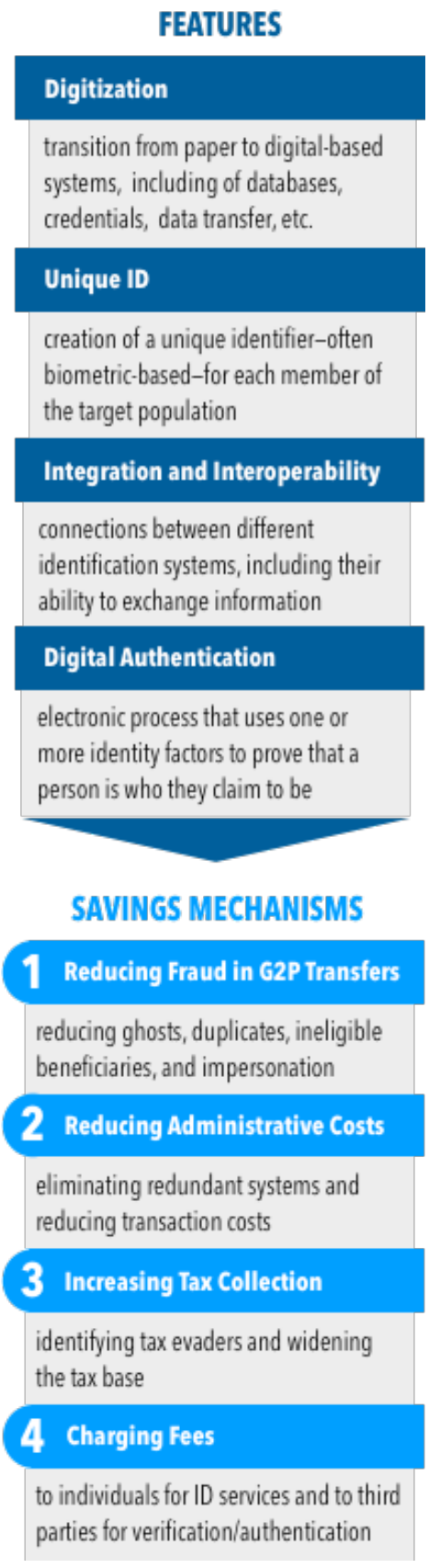
In order to address the heterogeneity of identification systems and country contexts, this paper highlights four **key features** of these systems that are most associated with potential cost savings and revenue generation opportunities for the public sector. Focusing on these features—which may be absent or present in various combinations in a given country—allows for a more precise understanding of how and when identification systems can contribute to savings. Each feature may facilitate fiscal savings and revenue generation either directly or by enabling or strengthening other features:

1. **Digitization.** Creating, managing, and using identities can be labor intensive when done in a paper-based system, and frequently involves high transaction costs for officials and individuals. On its own, digitization throughout the identity lifecycle—particularly in terms of database creation, management, and data transfer—allows for the simplification, automation, or elimination of many of these tasks and expenses, which can reduce operational and labor expenditures. Digitization can also play an indirect role in savings and revenue generation by enabling the deployment of other

identification system features, including unique identifiers, integration and interoperability, and digital authentication.

2. **Unique identifiers.** By establishing a unique identifier—e.g., a unique ID number or UIN—via biometric deduplication or another method, identity providers can directly reduce administrative errors and increase the efficiency of identity records management over time and across agencies that leverage the identifier. When integrated into other systems, unique IDs can help deduplicate records, serve as the key for communication and queries across databases, and provide a credential for secure verification and authentication procedures. They therefore help facilitate integration and interoperability, and typically precede and strengthen the robustness of digital authentication processes and services.
3. **Integration and interoperability.** The integration or connections between different identification systems within a country—e.g., via a common UIN, an interoperability platform, online query systems, or the dependency of one system on another—can enable or improve the efficiency of identity-related transactions that rely on multiple sources of information (e.g., verifying eligibility) and reduce the need for duplicative data collection exercises or credentials. Integration of a unique ID into other databases can also help deduplicate records, while interoperability platforms and other interfaces can enable fee-charging models for identity verification and authentication services.
4. **Digital authentication.** By providing a secure process for ensuring that a person is who they claim to be, digital authentication can reduce instances of identity theft and impersonation in a variety of transactions, including government-to-person (G2P) payments. In addition, digital authentication can simplify and automate procedures for proving one's identity—reducing transaction costs and enabling more efficient modes of service delivery such as remote payments—and create opportunities for identity providers to generate revenue by charging third parties for these services.

However, the ability of these features to contribute to fiscal savings and revenue generation depends on a number of endogenous and exogenous variables. First, fiscal benefits are likely to be maximized where there has been **sufficient investment** in the identification system to ensure high levels of **coverage** in the population and the **robustness** (i.e., accuracy, security, and integrity) of databases, credentials, and processes. Second, other **contextual factors**—including the levels of fraud and inclusion errors in G2P transfers, the volume of identity-related transaction, status quo inefficiency of the identity ecosystem, and levels of tax fraud—also affect the range of potential savings and revenue from identification systems.



Evidence of Savings and Revenue

Although there are limited data quantifying the impact of modernized identification systems, we can use existing reports of savings and revenue in particular sectors and ministries to draw some initial conclusions about the source and range of fiscal benefits to the public sector. These cases illustrate a variety of mechanisms through which the features of identification systems elaborated in the previous section can decrease expenditures, increase public revenue, or both.

This includes (1) reducing fraud in G2P transfers, (2) reducing administrative costs, (3) increasing tax collection, and (4) charging fees for various identity-related services. Naturally, savings and revenue are maximized where multiple mechanisms are enabled; however, not all may be feasible or desirable in a given context. Note that given data limitations, the figures in this paper should be taken as indications of the possible location and range of savings, rather than as precise estimates (see the Appendix for a summary of all cases).

1. **Reducing Fraud in G2P Transfers.** A first group of cases demonstrates how identification systems can generate savings by reducing fraud and inclusion errors in government-to-person (G2P) transfer programs. This includes, but is not limited to, public wage bills, pensions, and social protection programs such as food and commodity rations, unemployment benefits, grants for veterans and disabled people, child support, conditional cash transfers, and health insurance programs. The fraud-reduction mechanism operates through three distinct pathways, each relying on the implementation of different combinations of features:
    a. ***Eliminating multiple and ghost beneficiaries.*** With sufficient coverage and robustness, the integration of a unique ID credential or database with a G2P register can deduplicate a list of beneficiaries and eliminate fake or deceased beneficiaries. In Uganda, for example, the government reportedly saved US$6.9 million in less than a year by verifying the identities of civil servants against the national ID database, removing some 4,664 ghost workers from the public payroll.
    b. ***Identifying ineligible beneficiaries.*** Interoperability or integration between a strong unique ID system and *multiple* other registers can also help G2P providers better identify ineligible beneficiaries by facilitating verification of identity attributes across disparate sources. In Thailand, for example, the national ID number was used by a cash transfer program to cross-check the eligibility of beneficiaries against tax, occupational, and other databases, saving between US$29.7–59.4 million.
    c. ***Preventing impersonation and leakage.*** By ensuring that a person is who they claim to be, robust digital authentication can help curb fraud by reducing beneficiary impersonation. When combined with digital payment mechanisms, it can also help create an electronic trail of transactions that reduces leakage. In one limited application in India's State of Andhra Pradesh, for example, biometric smart cards reduced leakage in social wage benefits by approximately 10.8 percentage points, and in pension benefits by approximately 2.9 percentage points.
2. **Reducing Administrative Costs.** A second opportunity for decreasing government expenditures comes from the ability of identification systems to reduce operating costs within a country's identity ecosystem. These benefits accrue to a variety of agencies that operate or rely on an identification system to identify, verify, or authenticate individuals, issue credentials, or collect and manage personal data. The administrative-cost mechanism operates through two primary pathways:
    a. ***Reducing transaction costs.*** Creating, verifying, and authenticating identities entails a variety of transactions between individuals and governments and between government agencies themselves. Transitioning from a paper-based system to a digital one, creating a unique ID,

increasing interoperability and integration, and building digital authentication capacity have the potential to reduce the cost of many of these transactions. Furthermore, these features can enable digital payments and e-Government services that further increase efficiency. In Estonia, for example, the identification system—including the electronic identity document (eID) and X-Road data exchange layer—saves an estimated 2 percent of GDP each year by reducing identity-related transaction costs and facilitating online services.

b. ***Eliminating redundant systems.*** In addition to improving the overall efficiency of identity-related transactions, interoperability or integration between identification systems with sufficient coverage and robustness can create the opportunity to reduce or eliminate some redundant aspects of the identity ecosystem. This can include avoiding duplicate data collection or eliminating obsolete databases or credentials. In Malawi, for example, integration between the national ID and voter registration eliminated the need for a separate voter ID card, saving approximately US$44 million ahead of the 2019 elections.

3. **Increasing Tax Collection.** Integration between unique identification systems and tax administration can help improve taxpayer identification, potentially broadening the tax base and improving compliance. Where the coverage of the identification system is high, authorities can better identify the total base of potential taxpayers who may not yet be registered by the tax system. Furthermore, as with G2P transfers, a unique ID can be used to deduplicate tax records and identify individuals who use multiple tax IDs to decrease their liabilities. Similarly, identification systems that link the tax administration with other data sources—e.g., land records, vehicle registers, customs databases, and social benefits registers—can better identify businesses or individuals who are underreporting their earnings or assets and generate risk scores to better target audits. In Argentina, for example, integration between tax databases and other registers via a unique ID improved tax audits, generating approximately US$44 million in additional revenue from a reduction in tax fraud.
4. **Charging User Fees.** In addition to increasing tax collection, identification systems—particularly those with digital platforms for identity verification and authentication—have the potential to create an additional revenue stream through the ability of identity providers to charge fees to certain services. This includes fees for "luxury" services to individuals such as optional smart cards or expedited processes, as well as authentication and verification services to third parties. In Peru, for example, identity-provider RENIEC has earned approximately US$45 million in revenue annually by charging fees for verification services, mostly to private sector companies. However, while charging fees can be an important revenue stream for identity providers and offers some level of fiscal autonomy, overcharging for services can depress demand and undermine the principle that identification should be a universal public good.

Beyond the above mechanisms, identification systems can have other fiscal benefits for governments that are indirect or more difficult to quantify, such as facilitating trusted voter identification that reduces the probability of election disputes and violence and their associated human and economic costs. In addition, these systems can also have parallel and positive financial impacts on individuals, donors, and the private sector.

Key Considerations

In addition to using the Guide provided in Section 4 of this paper to assess potential fiscal savings and revenue generation opportunities, any cost-benefit analysis of identification systems should take into account a number of additional factors. To begin, this should include a detailed assessment of **costs,** including initial investments needed to build an identification system with sufficient coverage and robustness, as well as the costs of adapting other systems and registers to be able to leverage its benefits.

Beyond costs, it is crucial that identity stakeholders also consider that certain measures that generate fiscal savings and revenue may also **risk increasing exclusion.** Exclusion may occur, for example, if a cash transfer register or other database is seeded with a unique ID that does not have truly universal coverage. If individuals who cannot provide a unique ID are declared "ghosts" and removed, this may include real people who have not yet enrolled in the identification system. Similarly, individuals may be excluded from enrollment or authentication procedures that require biometrics if they are unable to provide fingerprints or iris scans and no contingency measures are in place. Charging high fees for identity-related services can also be cost prohibitive for some individuals and firms—or firms may pass these costs onto their consumers.

In addition to the risk of exclusion, certain identification system features and savings mechanisms—particularly integration and interoperability between databases—have important implications for **data protection and privacy.** Although integrating or interoperating multiple databases can help identify ineligible G2P recipients and reduce administrative costs, it must be done in a way that upholds the *Principles on Identification* (World Bank 2017b). For example, stakeholders should ensure that government agencies and third parties have access only to the minimal amount of information necessary for reconciling or verifying identity records across databases. Interoperability and integration should be also be underpinned by legal frameworks and procedures that clearly specify who has access to different data and under what conditions, ensure user control, and include robust security measures to ensure data protection.

Finally, although governments at large may benefit from savings and revenue generated by robust and inclusive identification, the source of these benefits may go against the **vested interests** of certain actors. This includes those officials, service providers, intermediaries, and private individuals who currently benefit from weak or inefficient identification systems that offer opportunities for corruption and fraud. To the extent that they are able, these groups may actively work against reforms to identification systems to the extent that these reforms will generate savings at their expense. Creating incentives for compliance is therefore crucial to the success of many identification projects.

Conclusion

This paper presents early evidence that identification systems can create opportunities for fiscal savings and revenue generation through a variety of mechanisms. However, the full extent of these benefits remains difficult to quantify. As such, this paper has highlighted the need for more data and research to develop a reliable model of expected return on investment for identification systems. As more data become available in the future, we can develop more advanced models to help countries maximize savings opportunities in a way that supports the Sustainable Development Goals.

What remains clear, however, is that opportunities for savings and revenue require identification systems that are sufficiently robust, have high levels of coverage, and are designed with the goal of maximizing efficiency. This requires overall up-front investment in identification infrastructure, and costs associated with adapting systems to enable savings and revenue generating mechanisms. In addition, the scope of potential benefits is highly dependent on country context.

Furthermore, practitioners must carefully weigh the potential fiscal impacts of certain features and mechanisms—particularly interoperability and integration, efforts to identify fraud and leakage, and fee-charging models—against risks to privacy and exclusion. While some of the benefits of identification may be fiscal, many are not. In the end, identification should be a public good, provided to facilitate the rights and inclusion of individuals and to improve administration and service delivery. Through thoughtful design countries should be able to achieve these goals while maximizing long-term fiscal sustainability.

1. Introduction

Inclusive and robust identification systems offer many concrete benefits for governments, as well as individuals, private companies, and development partners. By providing a secure and accurate way of identifying the population, these systems can facilitate the delivery of a wide variety of services that expand financial inclusion, boost economic opportunities, improve access to social safety nets, increase gender equality, and more. With high levels of coverage, identification systems are also important tools for government planning, emergency response, and free and fair elections. Indeed, the foundational role that identification plays in so many development activities has motivated its inclusion in the Sustainable Development Goals' (SDGs) Target 16.9, "to provide legal identity for all, including birth registration, by 2030."[1]

In addition to these developmental uses, evidence suggests that strong identification systems have the potential to generate savings and revenue for the public sector, to the tune of millions of dollars per year (or even billions for larger economies). This is good news given the fact that building modern—and particularly digital—identification systems requires significant up-front investment. To the degree that governments are able to harness the value of inclusive and robust systems to partially offset their costs, they will be closer to achieving the goal of fiscal sustainability enumerated in the *Principles on Identification for Sustainable Development.*[2] To date, however, our understanding of the full fiscal impact of identification systems is limited given the scarcity of publicly available data. In particular, little work has been done to develop a systematic understanding of how and when identification systems can save governments money or boost revenue.

This paper is a first step toward filling this gap. Using the experiences of a handful of countries where data is available—varying by region, income level, and system type—it attempts to build a framework for analyzing the potential fiscal benefits associated with investment in identification systems, including the features, mechanisms, and conditions that may generate (or limit) savings and revenue. The goal of aggregating existing knowledge and developing this framework is twofold. First, it provides a tool for governments and other stakeholders involved in planning or funding such systems to begin to estimate expected fiscal returns on their investments. Second, we hope that this paper will inspire and guide country practitioners, donors, and researchers to undertake more rigorous evaluations of the effects of identification systems. Strengthening this evidence base is crucial for helping countries maximize the positive impacts of these systems while mitigating risks in a way that facilitates the sustainable development agenda.

Methodology

Evaluating the effect of modern identification systems on the public purse is challenging for a number of reasons. To begin, there is the aforementioned problem of scarce data. Few governments or development partners have rigorously assessed fiscal impacts during or after the implementation of identification-related projects. Furthermore, where estimates do exist, the assumptions and figures behind these calculations

1 For a fuller discussion of the ways in which identification systems can further developmental goals, see Gelb and Clark (2013a), Dahan and Gelb (2015), and World Bank (2017b).

2 See Principle on Identification number 7, "Planning for financial and operational sustainability without compromising accessibility" (World Bank 2017b).

are often not made public, and both governments and identity solutions providers may have incentives to inflate the efficiencies gained by identification systems.

Furthermore, it is difficult to establish appropriate counterfactuals to assess identification-related savings and revenue within—and particularly between—countries. This stems from the fundamental problem of causal inference, as well as challenges related to operationalizing and measuring complex policy interventions like identification systems. Few truly "greenfield" identification projects exist; most consist of iterative or piecemeal reforms of existing systems. Considering the impact of going from "ID system = 0" to "ID system = 1" is therefore not practical in many cases. The design and use of identification systems is also multilayered and rarely equivalent across countries or ministries, making it difficult to define a uniform "identification intervention" or directly compare savings and revenue outcomes across a variety of sectors and agencies.

Finally, because the effects of identification systems are likely to be multiplied by complimentary and often bundled reforms—such as investment in information and communications technology (ICT) infrastructure including broadband connectivity, the introduction of mobile payment systems, development of e-Government services, or better targeting mechanisms for cash transfer projects—it is challenging to isolate the impact of identification alone. If sufficient data become available in the future, these issues could be overcome with appropriate research designs. At present, however, our ability to create a valid quantitative model of identification-related savings and revenue for the public sector is limited.

Instead, this paper aggregates a handful of existing cases based on primary and secondary sources and proposes an analytical framework for assessing the range of identification-enabled savings and revenue possible in a given context. This framework addresses heterogeneity in the design and maturity of identification systems by unbundling them into important "features," including (a) digitization of core databases, processes, and credentials; (b) the introduction of unique identifiers; (c) integration and interoperability between systems; and (d) digital authentication. Focusing on these features—which may be absent or present in various combinations—allows for a more precise understanding of how and when identification systems can contribute to savings.

In addition, this paper attempts to provide analytic clarity by detailing four primary mechanisms through which these features can create positive fiscal impacts for the public sector: (1) reducing fraud and leakage, (2) decreasing administrative costs, (3) increasing tax collection, and (4) charging fees for identity-related services. Which mechanisms are enabled in a given country—and the amount of savings or revenue they generate—depends on the particular features adopted, the overall robustness and coverage of the identification system, and a variety of context-specific factors discussed throughout this paper.

Scope

There are some important limitations to the scope of this paper. First, its focus is on savings and revenue enabled by *foundational* identification systems: those created for general public administration and identification (e.g., civil registries, national IDs, and population registers), and which serve as the basis for a wide variety of public and private transactions, services, and derivative identity credentials. However, given the relative scarcity of available data on foundational systems as a whole, some examples from *functional* identification systems—those created in response to demand for a particular service or transaction (e.g., voter lists, social safety net program registers, drivers' licenses, etc.)—are included where they illustrate similar mechanisms.[3]

3 Throughout the remainder of this paper, the term "identification system" therefore implies a *foundational* system, unless otherwise specified. See Gelb & Clark (2013a) for a discussion of the foundational vs. functional typology.

Second, it explores only those mechanisms through which these identification systems may produce *direct, quantifiable, fiscal benefits* for *governments* in the form of decreasing expenditures and/or increasing revenues. As a result, this paper may considerably understate the potential for savings and revenue generation across the economy as a whole and in terms of improved individual well-being. We know that identification systems can also produce direct savings for individuals, private companies, and donors, in addition to indirect or difficult to quantify savings through a number of channels (Boston Consulting Group 2012). For example, a voter roll generated from a robust and trustworthy national ID system may decrease the likelihood of election violence and its associated human and financial costs (Gelb and Diofasi 2016). While a full assessment of the economy-wide benefits of identification systems is beyond the scope of this paper, these additional sources of savings are discussed briefly in Section 4. In addition, a companion piece to this paper focuses on the financial benefits of identification systems for the private sector (see World Bank 2018c).

Third, this paper notably does not consider the *costs* of identification systems—a necessary ingredient to understand their overall net benefits. Although the identification systems features enumerated in Section 2 offer various channels to decrease expenditure and generate revenue for some areas of government, their implementation requires investments that outweigh these benefits. In order to make a full cost-benefit analysis of these systems, readers are therefore encouraged to reference the World Bank's forthcoming work to develop a costing database and model (see World Bank 2018d).

Finally, it is important to note that fiscal impacts are only one lens through which we should measure the effectiveness or desirability of a particular identification system or ID-related policy. The cost saving and revenue generating features and mechanisms described in this paper may also have broader developmental and societal benefits, such as promoting trust and increasing the participation of marginalized groups. At the same time, they also come with important risks—particularly to privacy and inclusion—as discussed in Section 4 under *Key Considerations.* The features and mechanisms presented in this paper are therefore not intended to be prescriptive. Rather, they are a descriptive framework used to categorize a diverse set of country experiences. As such, we hope this paper will serve as a point of departure for carefully weighing the advantages and disadvantages of different identification system features, policies, and institutional arrangements.

Organization

This paper is organized as follows. Section 2 defines key features of identification systems associated with fiscal savings and revenue for the public sector, along with the factors that condition or constrain these potential benefits. Using examples from countries that vary in terms of region, income level, and sophistication of their identity ecosystems, Section 3 illustrates how these features can reduce costs or generate revenue through a variety of mechanisms. Section 4 then provides a guide built on this framework that governments and other stakeholders can use to begin estimating expected fiscal benefits from identification systems, including key considerations that should shape this exercise. Section 5 provides concluding thoughts.

2. The Potential of ID for Fiscal Savings and Revenue

Over the past decade, numerous countries have embarked on efforts to "modernize" various aspects of their identity ecosystems; the collection of databases, registers, and credentials[4] used for managing personal data across a variety of agencies. These reforms frequently involve a transition from paper-based to digital systems, including electronic data capture, the use of biometric data such as fingerprints and iris scans, electronic identity documents (eIDs), and digital authentication capabilities. In addition, many countries have worked to harmonize and rationalize fractured identity ecosystems using a variety of integration and interoperability models. A cornerstone of such projects—and the focus of this paper—has often been the creation or upgrading of foundational identification systems, such as national IDs, civil registers, and national population registers, with the goal of providing general databases and credentials to underpin a variety of uses and services.

However, while the trend toward digital and integrated identification systems has gained significant momentum, the reality is that most developing countries are in the early or medium stages of modernization. Furthermore, no two systems are exactly alike. This poses challenges for understanding the average benefits that we might expect from these identification projects. Where reforms are incremental and heterogeneous, it becomes difficult to discuss the overall impact of "an identification system" on the public purse. Saying that the system in country X saved millions of dollars, for example, may be of little use to country Y if their planned system differs in form and function.

In order to address the variation and uneven development in identification systems, it is therefore necessary to unbundle the specific *features* of these systems that directly and indirectly create opportunities for fiscal savings and revenue generation but may be adopted in different combinations in different contexts. This section defines these features and enumerates the various factors and conditions that enable or constrain their ability to lower costs or increase revenue in the public sector.

2.1. Key Features

Identification systems are complex, and may involve a host of processes, technology, databases, credentials, and legal frameworks associated with the capture, management, and use of personal data for the general identification of the population. Many countries also have multiple foundational systems, including civil registers, national ID databases and cards, unique ID numbers, and/or national population registers, with different roles in different contexts.

Within any configuration of modern identification systems, however, there appear to be four primary features most associated with fiscal savings and revenue: (1) *digitization* of databases, credentials, data transfer, etc., (2) the creation of a *unique identifier* (unique ID or UID), (3) *integration* and *interoperability* between various foundational and functional systems within a country and potentially across borders, and

4 An identity credential can be defined as "a mechanism, process, device, or document that vouches for the identity of a person through some method of trust and authentication" (World Bank 2016). Common types of identity credentials include—but are not limited to—ID cards, certificates, ID numbers, passwords, and PINs.

(4) *digital authentication* of individuals (see Table 1). Generating opportunities for identification-enabled savings and revenue in the short-, medium-, and long-terms requires up-front investment in one or all of these technologies.

Table 1: System Features Associated with Fiscal Savings and Revenue

Feature	Description	Key Benefits
Digitization	transition from paper to digital-based systems, including of databases, credentials, data transfer, etc.	• *Direct:* reduces operating and transaction costs • *Indirect*: enables unique ID, integration, digital authentication
Unique ID	creation of a unique identifier –often biometric-based–for each member of the target population	• *Direct:* eliminates duplicates; increases efficiency • *Indirect*: enables integration; boosts digital authentication
Integration and Interoperability	connections between different identification systems, including their ability to exchange information	• *Direct:* reduces operating and transaction costs; enables identity verification across databases, fee-charging
Digital Authentication	electronic process that uses one or more identity factors to prove that a person is who they claim to be	• *Direct:* decreases risk of impersonation; reduces transaction costs; enables fee-charging revenue models

In general, these features are complementary, somewhat sequential, and may have either direct or indirect effects on fiscal savings and revenue. For example, digitization of databases is generally a prerequisite for the creation of a unique ID, digital authentication, and/or integration and interoperability between systems. And although digital authentication and some level of interoperability are possible without a unique ID,[5] the latter typically precedes and strengthens the former features. Still, despite their interdependence, each feature can (in theory), produce independent effects on savings and revenue. That is to say, gains may be maximized where an identification system has each of these features, but it is not necessary to implement all features in order to see concrete benefits. For example, in contexts where the primary source of leakage is fake beneficiaries, implementing a unique ID to deduplicate the program register may be sufficient to generate substantial savings.

Furthermore, the efficacy of these features in reducing expenses and generating revenue depends on a number of endogenous and exogenous variables, including the overall coverage and robustness of the system, as well as the status quo levels of fraud, inefficiency, and identity-related transactions. Each of these features and conditioning variables are described below. Broader limitations on the potential

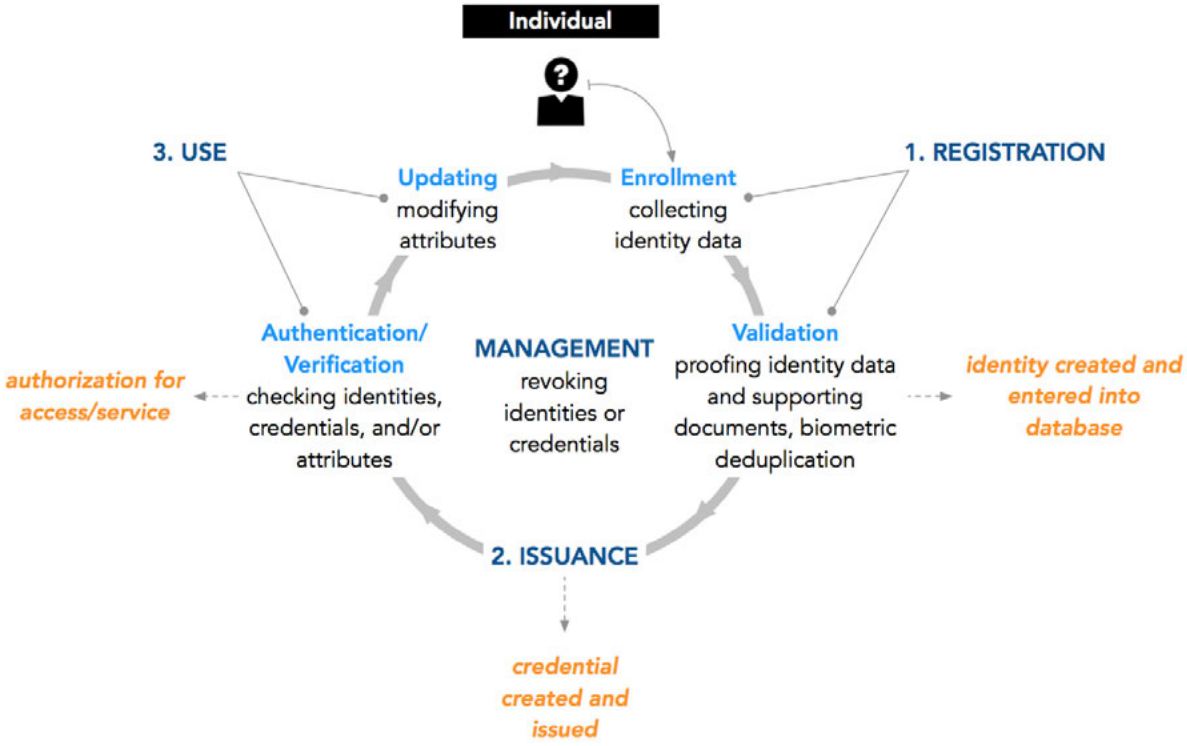
5 For example, a country that had not deduplicated its national ID register could issue eID cards and use these to authenticate online transactions. Although this would improve the security of authentication by making it harder for someone to impersonate the cardholder, one person could still hold multiple cards under false names.

fiscal benefits of identification systems—including system costs, vested interests, and concerns related to exclusion and privacy—are discussed later in Section 4.

Digitization

"Digitization" of identification systems refers to the transition from paper-based, analog systems to electronic ones. This digital transition applies to the various processes and outputs of the identity lifecycle (shown in Figure 1), including enrollment of individuals, validation of their identities via "identity proofing" and often biometric deduplication, database storage and management, issuing credentials, verification and authentication procedures at the time of service delivery, and updating records. Digitization of some aspects of the lifecycle—e.g., electronic databases, the use of digital biometrics for deduplication, eID cards, etc.—often occurs in the first phase of identification projects, while other aspects such as electronic enrollment forms and digital authentication are typically added at later stages.[6] For this reason, digital authentication is treated as a separate feature, and discussed in more detail below.

Figure 1: Identity Lifecycle



Source: Adapted from World Bank (2016).

Creating, managing, and using identities can be labor intensive when done in a paper-based system, and frequently involves high transaction costs for officials and individuals. It takes significant staff time to process paper-based applications and to validate and update paper-based records. This can involve phone

6 This is true in a majority of developing countries, where the issuance of eID cards has preceded any digital authentication infrastructure, oftentimes by many years or decades. A notable exception is India's Aadhaar program. The Unique Identification Authority of India (UIDAI) made authentication a central purpose of its identity scheme and moved to roll out this functionality early in implementation.

calls and sometimes physical travel to other agencies to verify residency or citizenship, manually searching for records, and even visual fingerprint matching.[7] In addition to time and labor, these manual processes can require non-trivial outlays for expenses such as printing and photocopying, postage, and the rental or purchase of buildings large enough to house millions of records.

On its own, digitization throughout the identity lifecycle—particularly in terms of database creation, management, and data transfer—allows for the simplification, automation, or elimination of many of these tasks and expenses, which can reduce operational and labor expenditures. While direct savings from digitization are likely to be insufficient to fully offset the costs of implementation, these reforms also play an indirect role in enabling the deployment of other identification system features, including unique identifiers, integration and interoperability, and digital authentication. Many countries, for example, have a long history of issuing paper-based cards with national ID numbers (NINs). However, creating a robust and unique ID number generally requires a computerized records system and technology capable of deduplicating applicants to a high level of accuracy (e.g., digital biometrics or other matching algorithms). Similarly, although it is possible to manually reconcile two sets of paper registers in order to cross-check or link records, this process is also highly inefficient compared with digitally integrated or interoperable systems that allow for near instant queries.

Unique Identifiers

A unique identifier (unique ID or UID) is an identity attribute[8] or credential that uniquely identifies a person or entity within a given population. In other words, an identifier is unique if no two individuals in the system share the same value of the identifier. In the context of foundational identification systems, this often takes the form of a unique ID number (UIN), assigned to each resident or citizen of the country after a process of validating their identity and uniqueness (i.e., ensuring they have not registered in the system multiple times or under multiple names).[9] In a small but growing number of cases—e.g., Peru, Thailand, Estonia—residents are issued UINs as part of the birth registration process, and carry these identifiers throughout their lifetimes. More commonly, unique IDs have been issued when registering for national ID systems at age 16 or 18.

Unique IDs, and particularly UINs, have long been features of identification systems. However, they have rapidly increased in their robustness and utility over the past few decades due to advances in technology on two fronts. The first is the computerization of databases, which provides the capacity to easily generate, store, and reconcile unique numbers and other identifiers across a large population. The second relates to improvements in the accuracy and reliability of biometric identification technology to establish uniqueness based on physical or behavioral characteristics such as fingerprints, irises, facial images, gait, keystrokes, etc.

Digital biometric identification involves comparing a template generated from a live biometric sample to a previously stored biometric in order to determine the probability that they are a match. One-to-one matching is a comparison against a single template (e.g., one stored on an eID card) and is typically used for authentication and verification. One-to-many or 1:N matching is a comparison against all or a subset of templates stored in a database, and can be used for *identification* (e.g., a criminal record search)

---

7 In Côte d'Ivoire, for example, it takes 2–3 months to issue a national ID because of manual processes. In order to validate identity information for new applicants, for example, a staff member physically travels to consult civil records (World Bank 2017c). This can cause significant delays, particularly when records are in remote locations with poor road infrastructure, or when staffing is insufficient.

8 An attribute is commonly defined as "a named quality or characteristic inherent in or ascribed to someone or something" (NIST 2013). In foundational identification systems, common characteristics include name, age, sex, place of birth, address, fingerprints, photos, signatures, identity numbers, the date and place of registration, etc.

9 Although the unique IDs discussed in this paper are primarily those assigned to people, unique IDs can also be assigned to businesses and other entities.

or *deduplication* (i.e., ensuring that each individual exists only once in the database). In principle, 1:N deduplication allows identity providers to establish statistical uniqueness in a population.[10] If live biometric samples are required for enrollment or authentication, this technology can also ensure that a person is living.[11] Although biometric technology is not the only solution for creating a unique ID, these characteristics have led to its rapid proliferation in modern identification systems.

Regardless of the technology used to generate them, however, robust unique IDs offer a number of benefits that explain their increasing adoption. By ensuring that each person is unique, they reduce errors in the identification system and increase the efficiency of identity records management over time and across agencies. These improvements can have direct financial benefits by reducing operating and administrative costs for identity providers. Furthermore, unique IDs can indirectly increase savings and revenue generation opportunities by enabling other features of identification systems. For example, when used as a "key" or common reference across identity databases and systems, unique IDs enable many of the benefits associated with integration and interoperability described below. In addition, unique IDs typically precede and strengthen the robustness of digital authentication processes and services.

Integration and Interoperability

Broadly defined, the level of integration within the identity ecosystem refers to the degree to which different foundational and functional systems are connected—in terms of both their architecture and use. Interoperability refers to the ability of different systems to talk to each other, exchanging information and queries. Integration can take a variety of forms. In the most extreme case, countries may adopt a "single warehouse" for all identity information and/or a multipurpose credential to manage verification and authentication for most services (e.g., the MyKad eID card in Malaysia). More commonly, however, countries maintain a number of separate databases and credentials, and then adopt different integration models to facilitate communication between systems. In some cases, databases are directly connected or "tightly coupled," allowing for real-time data exchange and updating (e.g., Botswana's civil register and NID databases). In others, databases are interoperable via a trusted third-party exchange layer that facilitates queries between systems (e.g., Estonia's X-Road system).

An important element of database integration and interoperability is the use of common identifiers such as a UIN that is recorded in each register. In a "loosely coupled" model, for example, databases remain separate, but each contains a common identifier that allows records to be easily reconciled across systems. Even in the absence of a direct connection or integration layer, this can help streamline the identity ecosystem. For example, identity providers can develop online platforms such as application program interfaces or (APIs) that allow users from one institution limited access to query the database of another institution via the UIN (e.g., Aadhaar in India, or Peru's RENIEC system). Similarly, using a foundational database (e.g., a population register) or credential (e.g., a national ID) as the authoritative source of basic identity information for a variety of other registers and programs can also help harmonize identification systems, reducing the need for multiple registration exercises and streamlining authentication and verification processes.

In contrast to those with high levels of integration, fragmented identity ecosystems have few or no connections between disparate identification systems. In the absence of a common identifier, the lack of

10 Although no biometric system will be error free, it remains the most accurate technology available for identifying large populations. However, as the population size increases, more data (e.g., multiple fingerprints and iris scans) are needed to achieve the same level of accuracy. See Gelb & Clark (2013b) for further discussion.

11 Of course, fingerprints can also be captured "latently" as done in crime scene investigations. However, although the technology to remotely capture digital biometrics exists (e.g., for authentication against mobile phones), in-person enrollment is typically required for identification systems, and many biometric readers now include technology to ensure the "liveness" of the sample. Still, there is always the risk that biometrics can be faked or "spoofed." This may be a particular concern for authentication in remote or "self-service" transactions where users do not come into direct contact with service providers.

interoperability between systems means that databases are unable to communicate and instead operate as silos. Oftentimes, fragmented systems also produce a multitude of credentials for distinct purposes that are expensive to maintain and inconvenient for users. In general, fragmented systems are more inefficient than integrated ones. Despite many of the same information needs (e.g., name, age, sex, address, etc.), each agency or department conducts separate exercises to collect individuals' attributes and then builds parallel information systems to manage this data. Without the exchange or verification of information across databases, each agency must undertake its own labor-intensive process to validate the identity attributes it collects. Individuals must also spend time and resources to register separately for each identification program and obtain multiple credentials.

Increasing integration across identification systems can therefore directly contribute to savings for governments by decreasing redundancies within the system and lessening administrative burdens related to identity proofing and authentication. With high levels of integration, countries may even be able to eliminate duplicative identification systems and credentials that have become obsolete. For example, if a national ID card serves as proof of citizenship, age, and address, there may be no need to issue separate voter cards. In addition, the integration of a unique ID into various government registers—e.g., via a "seeding" process that links each record in the existing database to the person's UIN—can deduplicate functional databases, eliminating multiple or fake enrollments. Integration between various functional databases can also help increase tax revenue by reconciling records (e.g., tax and property databases) to better identify fraud and discrepancies. Finally, interoperability between identification systems and third parties (both public and private) can enable fee-charging models for identity verification and authentication services. However, as discussed in Section 4, countries must carefully balance the efficiencies gained by integration and interoperability with concerns regarding data security and privacy.

Digital Authentication

At its most abstract, authentication is the process of proving that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more "factors" or "authenticators" to a service provider to "assert" their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person *is* (e.g., their fingerprints), *knows* (e.g., a password or PIN), *has* (e.g., an ID card, token, or mobile SIM card), or *does* (e.g., their handwriting, keystrokes, or gestures). For service providers, digital authentication offers more protection against identity theft and impersonation at the point of transaction than traditional methods of manually examining credentials (e.g., visually comparing a photo on an ID card to the person presenting it) (OWI 2017; NIST 2013).

However, not all authentication processes are created equal. The level of trust or "assurance" digital authentication provides depends on the type of factors or credentials used, along with the nature of the authentication protocols.[12] For example, two-factor digital authentication with biometrics provides a higher level of security than a simple password, which is relatively easier to share or steal. In addition, the trustworthiness of a credential depends on the level of identity proofing or verification that a person underwent *before* it was issued. Using a Google account for authentication, for example, provides a lower

12 See NIST (https://pages.nist.gov/800-63-3/sp800-63-3.html) and eIDAS (https://www.eid.as/home/) for current globally-accepted definitions and standards for levels of assurance in digital authentication.

level of assurance than a digital ID based on a robust government-issued credential, as Google does not require users to provide or substantiate attributes outside of a self-created and asserted e-mail account.[13]

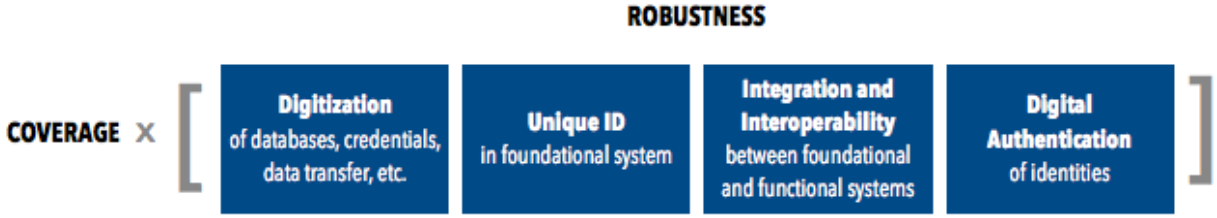
The ability of identification systems to provide the basis for secure digital authentication can directly contribute to cost savings and revenue generation in three distinct ways. First, by reducing the risk of impersonation, digital credentials—such as a biometric-based UIN (India) or a national eID with public key infrastructure (PKI) encryption (Estonia)—can reduce fraud and leakage when used to authenticate beneficiaries for government-to-person (G2P) transfer programs and other transactions (e.g., tax payments). Secondly, digital authentication can simplify and automate procedures for proving one's identity, reducing transaction costs, and enabling more efficient modes of service delivery (e.g., remote payments). Finally, the capacity to digitally authenticate individuals creates opportunities for identity providers to generate revenue by charging third parties for these services.

2.2. Conditions and Constraints

Although the features described above present opportunities for fiscal savings and revenue in the public sector, their efficacy is shaped by a number of factors. Broadly speaking, these can be classified into *endogenous* factors specific to the identification system itself, and *exogenous* constraints that depend on the broader country context.

The first important endogenous condition for savings and revenue is the level of *robustness* in the identification system (see Figure 2). Robustness refers to the accuracy, integrity, and security of system assets and processes, including the four features discussed in this paper. Savings and revenue potential is limited where systems are non-robust, and maximized when systems are statistically error free and highly resistant to fraud or theft. For example, deduplication using only one fingerprint will produce a less robust unique ID than deduplication using ten fingerprints and two iris scans, as the former provides less data to establish uniqueness. Interoperability between databases with inaccurate records will be less useful for identifying ineligible beneficiaries than databases that are relatively complete and error free. Similarly, if

Figure 2: Endogenous Factors That Constrain the Fiscal Benefits of Identification Systems



13 Although the two terms are often used interchangeably in the development context, *authentication* is technically distinct from *verification,* which is the process of determining the *veracity or authenticity* of particular attributes or credentials. When issuing a national ID, for example, identity providers typically undergo a process of "identity proofing," which involves verifying the self-declared attributes and supporting documents that an applicant has provided—e.g., asking for a utility bill as proof of address or checking with the local civil registry office to ensure that a birth certificate is authentic. Similarly, many government agencies require verification of particular attributes or credentials—e.g., name, age, enrollment in a social program, a valid ID card—before allowing a user to access a particular service. Although verification and authentication are related, they are typically distinguished by whether the purpose is to establish or verify particular attributes of an identity (proofing or verification) or to ensure that a person is the "true" owner of an identity or credential (authentication). In some cases, however, authentication procedures go beyond establishing a legitimate claim to an identity and also verify particular attributes (NIST 2013).

digital authentication procedures rely on ID cards with weak security features or identity records that were not thoroughly proofed, the system may be more vulnerable to identity theft and impersonation.

The second important endogenous condition is coverage: the percent of the target population that is enrolled in the identification system and has access to credentials and services. No matter how robust a system is or how many features it implements, fiscal benefits will generally be low where coverage is low. This is true for most of the mechanisms described in Section 3. Gains in administrative and operational efficiencies, for example, will only be possible when coverage is high enough to transition from old procedures and systems to new ones. Similarly, third-party service providers are unlikely to invest in authentication infrastructure that relies on a particular identity credential until a sufficient portion of their client base is covered.

In a few cases, limited benefits may be possible with low coverage, and increase as more people are brought into the identification system. For example, if an identification system covers most civil servants, it can still be used to deduplicate wage payments even if the coverage of the overall population is low. In most cases, however, sufficient coverage is necessary before fiscal benefits are noticeable. One report by the Asian Development Bank, for example, suggests that the identification systems with coverage below 50 percent are of limited use, while benefits for the public and private sector begin to kick in once systems reach 80 percent coverage or more (ADB 2016).

Both coverage and robustness are largely determined by investment in the identification system itself. This means that in order to increase opportunities for savings and revenue, countries must also spend more on their identification systems. Determining the level of investment necessary to achieve sufficient coverage and robustness is outside the scope of this paper; however, some important issues related to cost are discussed in Section 4. The World Bank's Identification for Development (ID4D) initiative has also recently completed a costing database and model that—combined with the Guide in Section 4—can provide the basis for a more complete cost-benefit analysis.[14]

Other important factors that condition savings and revenue opportunities are largely exogenous of investment in the system. These include, for example, the levels of fraud, inefficiency, and tax evasion in the status quo environment. An identification system will only be valuable for eliminating ghost workers, ineligible recipients, and tax evaders to the extent that these problems actually exist or are anticipated to exist in the future. Similarly, countries with relatively streamlined identity management procedures may have less to gain in terms of efficiency and reduced operating costs. In addition, the scope of savings from reducing transaction costs and revenue from charging fees will be limited by the current and anticipated volume of identity-related transactions in the country's ecosystem. If very few residents have access to the Internet, for example, savings opportunities from using digital authentication to facilitate e-Government services will likely be low. Finally, the overall effectiveness of the system will be constrained by resistance to reforms—i.e., agency loss—by those who profit from current inefficiencies. As discussed in the *Guide* in Section 4, practitioners must carefully consider each of these constraints when estimating expected fiscal returns on identification systems.

14 See World Bank (2018d).

3. Evidence of Savings and Revenue

Although there are limited data quantifying the impact of modernized identification systems, we can use existing reports of savings and revenue in particular sectors and ministries to draw some initial conclusions about the source and range of fiscal benefits to the public sector. These cases illustrate a variety of mechanisms through which the features of identification systems elaborated in the previous section can decrease expenditures, increase public revenue, or both.[15]

As shown in Table 2, key mechanisms through which the public sector may decrease expenditures or increase revenue through the implementation of an identification system include (1) reducing fraud in G2P transfers, (2) reducing administrative costs, (3) increasing tax collection, and (4) charging fees for various identity-related services.

Table 2: Mechanisms for Public Sector Savings and Revenue from ID Systems

	A. Decreasing Expenditures		B. Increasing Revenue	
Mechanism	**1. Reducing Fraud in G2P transfers**	**2. Reducing Administrative Costs**	**3. Increasing Tax Collection**	**4. Charging Fees**
Description	reducing ghosts, duplicates, ineligible beneficiaries, and impersonation	eliminating redundant systems and reducing transaction costs	identifying tax evaders and widening the tax base	to individuals for ID services and to third parties for verification/authentication
Location	• Payroll • Pensions • Safety nets • Targeted subsidies • Education • Health insurance, etc.	• Identity providers • Agencies or programs that require identity proofing, verification, authentication, or credentials	• Tax administration	• Identity provider

These mechanisms differ in terms of the nature and location of benefits enabled by identification systems. For the mechanisms that decrease expenditures, cost savings can accrue to a variety of agencies and programs that rely on identification systems to identify, verify, and/or authenticate individuals; those that manage personal data or issue credentials; and the identity providers themselves. For the mechanisms that increase revenue, one (increasing tax collection) is likely to be concentrated within the tax administration, while the other (charging fees) primarily benefits the identity provider. These mechanisms can operate in

15 Naturally, there are likely to be other cases where identification systems *have not* created significant savings or revenue for the public sector. These are not included here as the goal of this paper is to explore *potential* fiscal benefits from these systems; in other words, it focuses on the upper bound of savings and revenue.

isolation or coexist. Naturally, savings and revenue are maximized where multiple mechanisms are enabled; however, not all may be feasible or desirable in a given context (see Section 4).

The remainder of this section describes and illustrates these mechanisms using evidence from a variety of countries that differ in terms of region, income level, and the architecture of their identification systems. As stated in the *Introduction,* the figures cited in this section typically come from government reports, which sometimes involve opaque calculations or unpublished source data. Furthermore, the generalizability of one agency's or country's experience to another's is likely to be limited given the heterogeneity of identification systems and context. As such, the figures below should be taken as indications of the possible location and range of savings rather than as precise estimates. Given the difficulty of generalizing savings from one case to another, readers should use caution when extrapolating these results.

3.1. Reducing Fraud in G2P Transfers

A first group of cases demonstrates how identification systems can generate savings by reducing fraud and inclusion errors in government-to-person (G2P) transfer programs. Governments in developing countries typically spend around 15 percent of GDP on cash or in-kind transfers benefits (Gelb and Diofasi Metz 2018). This includes public wage bills, pensions, and social protection programs, such as food and commodity rations, unemployment benefits, grants for veterans and disabled people, child support, conditional cash transfers, national health insurance, and more. Although high levels of social sector spending may represent a positive commitment to development, budgets can be inflated or wasted by the inclusion of ineligible or fake beneficiaries in program registers (inclusion errors), or by transfers made to the wrong people (authentication errors), as shown in Table 3.[16]

Payrolls and pensions in many countries, for example, are notoriously full of "ghost workers" (fake employees or pensioners for whom someone collects a paycheck) and "double-dippers" (employees or pensioners who receive multiple paychecks under the same or different names). In Tanzania, a 2015 probe estimated that some 1.5 percent of the wage bill in the previous year had been paid to fake workers who were either deceased, retired, or resigned (News24 2015).[17] The same phenomenon exists in social transfers, where some individuals collect multiple benefits and others collect benefits in the name of fictitious or deceased beneficiaries. In India, for example, a 2007/08 audit of the National Rural Employment Guarantee Scheme (NREGS) in Odisha State found that approximately 8.6 percent of registered beneficiaries were ghosts who accounted for some 23.1 percent of person-days worked (NIPFP 2012).

In addition, where targeting systems are weak, many of those included in social program registries may not actually meet eligibility requirements.[18] In Morocco, for example, 2014 estimates suggested that some 60 percent of allocations for the country's main social transfers programs were going to non-poor individuals due to imprecise targeting (Angel-Urdinola, El-Kadiri, and Pillares-Millares 2014). G2P transfers are also subject to fraud at the time benefits are paid and collected. Complex, manual payment and authentication systems offer many opportunities for funds to "leak out" along the way, either due to impersonation of

16 Other types of fraud and leakage include theft of benefits by officials or other individuals during the transfer process and skimming by service providers who keep a portion of the transfers for themselves. These are not included here as they are not directly resolved by identification systems.

17 Out of a total annual payroll of 9,225 trillion shillings (just over US$5 billion at 2015 exchange rates), this represents some US$76.6 million (News24 2015). This number is low compared to estimates from other countries, such as Zimbabwe, where some 40 percent of the wage bill in 2012 was estimated to be lost to ghost workers (Atick 2016a).

18 In some cases, the inclusion of unintended beneficiaries is due to imprecision in the targeting system itself (e.g., geographic vs. household-level eligibility formulas). In this paper, "ineligible" refers instead to inclusion errors due to insufficient or inaccurate information about a beneficiary that—if known—would exclude them from receiving benefits.

Table 3: Identity-Related Fraud in G2P Programs

	Type	Description	Source of Problem	Detection
Inclusion error	Ineligible recipients	A person who collects benefits but does not meet program eligibility requirements	Insufficient information to determine eligibility	Cross-checking identity against eligibility-related records; via a unique ID or some other method
	Double-dippers	A person–eligible or ineligible –who has enrolled multiple times and collects multiple benefits	Lack of unique ID	Creating or integrating a unique ID that uses biometrics or algorithms to detect multiple enrollments
	Ghosts	A fictitious, deceased, or unwitting person under whose name someone collects benefits	Lack of unique ID, no proof of life, insufficient information to determine eligibility	Creating or integrating a unique ID that uses biometrics or algorithms to detect multiple enrollments and deceased identities; cross-checking other identity records
Authentication error	Impersonation	A person who impersonates a genuine beneficiary at the time a benefit is collected	Insecure authentication at the point of service	Increasing the level of assurance for transfers (e.g., using multi-factor digital authentication)

Source: Author's elaboration based on Atick (2016a), DFID (2009) and Muralidharan et al. (2016). Note that in the context of NREGS in India, Muralidharan et al. (2016) distinguish between "ghosts" (workers who do not exist), and "quasi-ghosts" (workers who exist but for whom someone is claiming work and payments against their names, unbeknownst to them).

eligible beneficiaries or theft and corruption by officials and service providers (DFID 2009).[19] With leakage, the intended recipients do not receive their full (or any) allotments; if they pursue their right to restitution, public agencies may end up paying twice (NIST 2013).

Any or all of these problems are likely to be endemic in a system where it is not possible to establish (a) the uniqueness of recipients within a particular program or register, (b) the eligibility of recipients based on accurate and up-to-date information (including that they are not deceased), and (c) that the person receiving a transfer is the intended recipient they claim to be. Strong identification systems can help address these issues through a number of pathways (see Figure 3), with potentially large savings for any department or program that leverages the system for its G2P transfers.[20]

First—and once foundational identification and G2P databases have been digitized—a unique identifier (e.g., a UIN) in the foundational system can be linked to the G2P register in order to deduplicate it, eliminating double-dippers. If the unique ID covers the entire population *and* is updated to include only living persons, this can also eliminate ghosts and deceased beneficiaries by removing identities that exist in the G2P register but not the foundational system. Secondly, where various G2P and other functional databases are interoperable via a unique ID, this can improve targeting by allowing cross-checks across various registers (e.g., payroll, tax register, and social benefits programs). Finally, digital authentication at

19 For example, in the audit of Odisha's NREGA scheme mentioned previously, only 61 percent of wage payments were actually received by workers (NIPFP 2012).

20 It is important to note, however, that while identification systems can help resolve inefficiencies in identifying and authenticating beneficiaries, they are not a panacea for inefficiencies in the targeting system of social programs, including formulas used for targeting and the difficulty of measuring indicators needed to determine eligibility.

Figure 3: Pathways to Savings by Reducing Fraud in G2P Transfers

1. Expenditures: Reducing Fraud in G2P Transfers

Pathways	*Features*			*Conditions*
a. Eliminate ghost, duplicate, deceased enrollees	**Digitization** of foundational and G2P registers	**Unique ID** in foundational system	**Integration/ Interoperability** of UID with G2P registers	• Coverage • Robustness • Level of ghosts, dupes, deceased
b. Identify ineligible enrollees	**Digitization** of foundational and G2P registers	**Unique ID** in foundational system	**Integration/ Interoperability** between G2P and other registers	• Coverage • Robustness • Level of inclusion errors
c. Prevent impersonation and leakage	**Digitization** of foundational and G2P registers	**Unique ID** in foundational system	**Digital authentication** at point of service	• Coverage • Robustness • Level of impersonation

Note: Although some level of digitization may also help eliminate ghosts, ineligible beneficiaries, and fraud and impersonation, its principle role in this mechanism is to enable other features that can reduce fraud on a much larger scale. The same is true for a unique ID in preventing impersonation; although a unique ID may increase the security of digital authentication, it is not a strictly necessary feature.

the point of service—often facilitated by a unique ID—can also reduce fraud and leakage by ensuring that the recipient is who they claim to be, and making it more difficult for officials or payment providers to siphon off funds. Each pathway is discussed below, along with relevant examples from existing cases.

Eliminating Multiple or Ghost Enrollments

A handful of countries have reported significant fiscal savings from linking G2P registers with a *foundational* unique ID to remove ghosts and duplicates in social safety nets (India), emergency assistance programs (Pakistan), and payroll and pensions (Uganda). In general, these savings were possible because these countries have achieved a high level of coverage and robustness and suffered from significant levels of fraud. However, there are other examples of countries that have used biometric-based unique IDs created within *functional* databases—e.g., those managed by human resources and social protection agencies—to reduce fraud in transfer programs even if their foundational identification systems lacked coverage. Despite the smaller scale of these initiatives and their autonomy from foundational IDs, the mechanism at work in these cases is similar, and they are included below in order to widen the evidence base.

India

Many of the most well-publicized—and hotly debated—estimates of savings from the elimination of duplicate and ghost beneficiaries come from India's Aadhaar system (see Box 1). In the past few years,

myriad ministries, states, and union territories have begun to incorporate Aadhaar into their G2P transfer programs, including flagship programs such as the Pratyaksha Hastaantarit Laabh (PAHAL) scheme to provide households with liquefied petroleum gas (LPG), the National Rural Employment Guarantee Scheme (NREGS), the Public Distribution System (PDS) food ration program, various pension schemes (SSP, NSAP), and more. By "seeding"[21] their databases with the unique Aadhaar number, program administrators are able to verify that beneficiaries are "real" people and are only enrolled once. In addition, over 56 ministries and 35 states and union territories have begun to make direct benefits transfers (DBTs) directly to Aadhaar-linked bank accounts via the Aadhaar Payment Bridge System (APBS). Of the approximate INR 4 trillion (US$61.7 billion) that the Government of India spends on core social protection programs and subsidies,[22] approximately INR 1.6 trillion (US$25 billion) now relies on Aadhaar-enabled DBTs.[23]

Box 1: India's Aadhaar System and Direct Benefits Transfers (DBTs)

India's Aadhaar program was launched in 2010 with the mission of providing a biometric-based unique identity number to each of the country's billion plus residents, regardless of nationality. The Aadhaar program collects minimal information, including name, gender, date of birth, address, and a digital photo, along with 10 digital fingerprints and 2 iris scans, which the Unique Identification Authority of India (UIDAI) uses to deduplicate each applicant and ensure their uniqueness. As of February 2018, Aadhaar enrollment covers over 1.2 billion people, or nearly 90 percent of the population. [24]

Rather than relying on a smart card for authentication, enrollees are issued with a simple card (initially a paper receipt) of their 12-digit, randomly generated Aadhaar number. This number can then be used for cloud-based digital authentication in combination with demographic data, a fingerprint, or a one-time password (OTP), depending on the desired level of assurance. Aadhaar authentication queries from third-party users to the central database return a simple "yes/no" response, indicating whether or not the person's asserted identity factors match UIDAI records. "Know your customer" (KYC) authentication using Aadhaar provides some additional information to banks and other financial service providers about an individual, such as address or other demographic attributes.[25]

The Aadhaar platform has been used as a tool to increase financial inclusion and curb fraud and leakage in the government's extensive subsidy programs—a central motivation for its creation. In addition to seeding their databases with the Aadhaar number to reduce ghosts and duplicates, social transfer programs have begun using the Aadhaar Payment Bridge System (APBS) to link beneficiaries' bank accounts with their Aadhaar number. This allows the government to make Direct Benefits Transfers (DBTs) to these accounts, which has the potential to reduce leakage, improve user experience, and reduce payment delays[26]

---

21 Seeding refers to the process of incorporating a unique ID number into program registers and databases.

22 For FY 2018/19 the Government of India plans expenditures of nearly INR 3 trillion for subsidies and an additional INR 1 trillion for other social protection programs including NREGA, health care, maternity benefits, and more (Ministry of Finance 2018; DBT Mission 2018).

23 As of March 2018, the DBT portal reported that INR 1.59 trillion in transfers was made through the system in FY 2017/18. See https://www.dbtbharat.gov.in/ for updated figures.

24 See https://uidai.gov.in/aadhaar_dashboard/india.php for most recent numbers.

25 As of early 2018, UIDAI also introduced "limited KYC," which will provide a reduced set of attributes to certain Authentication User Agencies (AUAs) in order to enhance privacy. See https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf for more information.

26 For more general information about Aadhaar, consult https://uidai.gov.in/. An excellent introduction to the overall Aadhaar system and DBT transfers is also provided in Abraham et al. (2017). For a brief introduction to the various layers of Aadhaar (called the "India Stack"), see https://medium.com/wharton-fintech/the-bedrock-of-a-digital-india-3e96240b3718.

As of early 2018, the Government of India reports estimated fiscal gains of more than INR 82,500 crore (some US$12.7 billion at current exchange rates) since 2013 from Aadhaar-enabled DBTs and related reforms to improve beneficiary identification and targeting of social programs and subsidies—around nine times the cost of Aadhaar implementation to date (DBT Mission 2018).[27] However, the full methods and data for calculating these figures have not been made public, and there have been many high-profile debates that dispute the government's claims of overall and program-specific savings from Aadhaar.[28] Although it seems highly likely that Aadhaar has had a positive impact on government finances, we do not yet have enough information to precisely quantify the amount of fiscal savings or to separate Aadhaar-related savings from those generated by digitizing beneficiary lists, implementing DBT payment mechanisms, or potentially falsely excluding deserving beneficiaries. These issues are not unique to India, and apply to many of the other cases discussed below.

One of the most cited cases of fiscal savings from Aadhaar comes from the PAHAL scheme, which replaced a subsidy for LPG cylinders sold to households with a DBT-based reimbursement for consumption.[29] As part of these reforms, the public Oil Marketing Companies (OMCs) that administer LPG distribution seeded their databases with Aadhaar by requiring consumers to provide their Aadhaar-linked bank account information. Customers now purchase LPG cylinders from the distributor at full cost, and the subsidy amount is transferred directly to their bank accounts. In addition to enabling the DBT mechanism that allowed the government to move away from an inefficient dual price system for LPG,[30] the Aadhaar linkage was also intended to clean up customer lists by removing fraudulent accounts.[31]

Estimates of savings from the PAHAL-Aadhaar linkage have varied greatly over time and based on the method of calculation (Mittal et al. 2017). For FY 2013/14, estimates of the reduction of LPG cylinder sales due to Aadhaar-linked DBT reforms range from 11–14 percent (Barnwal 2016) to 24 percent (Subramanian and George 2016). However, translating this reduction into a clear estimate of fiscal savings through fraud reduction has not been straightforward; more recent estimates have focused instead on the total number of beneficiaries removed from the system, multiplied by the assumed cost of the transfers. For the nine-month period between 2014/15 and 2015/16, for example, the Comptroller and Auditor General of India reported a savings of INR 1,764 crore (approximately US$270 million), which has been on the low end of official estimates (CAG 2016).[32] Currently, the DBT Mission reports fiscal gains of INR 9,108 crore (US$1.4 billion) from the reduced number of beneficiaries for the 2017/18 fiscal year, and a cumulative savings of INR 38,877 (US$5.9 billion) since the program's inception (DBT Mission 2018).

However, we do not know exactly how much of this savings can be attributed to Aadhaar alone. Although the government reports that some 38.5 million duplicates and ghosts have been blocked through the transition to Aadhaar-enabled payments (DBT Mission 2018), it is possible that some portion of these were false exclusions—genuine beneficiaries who were unable to transition to DBT because they lacked Aadhaar

27 From inception until 2017, the total cost of Aadhaar implementation has been approximately US$1.4 billion dollars, and steady-state costs are likely to converge at around US$150 million per year. As a result, the program costs a little over US$1 per person (World Bank 2018b).

28 See, for example, an excellent review by IDinsight at http://stateofaadhaar.in/did-aadhaar-really-save-rs-57000-crores-simply-put-no/.

29 For more on India's LPG subsidy reform, see Mittal et al. (2017).

30 Cylinders purchased by businesses were not subsidized, incentivizing fraud and creating a black market for LPG.

31 For more information about the PAHAL scheme and controversy surrounding savings estimates, see Barnwal (2016) and Lahoti (2016).

32 The CAG estimates, for example, assume that removed beneficiaries would have claimed the average number of cylinders consumed in a year (a little under 7), while other government estimates have assumed that they would have claimed the maximum of 12 cylinders (Mittal et a. 2017).

numbers or linked bank accounts (Lahoti 2016).[33] Similarly, an estimated 2.29 million nonsubsidized consumers who *voluntarily* left the program due to a simultaneous "Give It Up" campaign are included in the savings calculations (DBT Mission 2018). Another criticism of the official numbers is that some duplicate and ghost beneficiaries were removed from LPG client lists *before* Aadhaar, when oil companies reconciled their databases using name- and address-matching algorithms to delete multiple connections at the same household address. Mittal et al. (2017), for example, estimate that some 13.3 million beneficiaries were removed through this process by the end of 2012, before Aadhaar seeding had begun. Another report estimates that the true number of beneficiaries removed by Aadhaar seeding was actually around 800,000, or only 2 percent of the total 35 million removals claimed by the Indian government in 2016 (Clarke 2016).

In addition to PAHAL, the Indian government has also reported significant savings from removing ghosts, duplicates, and fakes from a variety of social protection and other programs.[34] For the PDS scheme, for example, the government reported a cumulative savings of INR 14,000 crore (US$2.1 billion) through mid-2017, due to the removal of some 23.3 million fake beneficiaries (Abraham et al. 2017). As of FY 2017/18, the number of "fake" or duplicate ration cards eliminated has reportedly reached 27.5 million, with a cumulative savings of INR 26,792 crore (US$4.1 billion) (DBT Mission 2018). For NREGS, the government estimates a 10 percent average reduction in expenditure on wages per year due to a reduction in duplicate and ghost workers, with associated cumulative gains of INR 15,374 crore (US$2.3 billion) to date (DBT Mission 2018). Other reported gains from removing fake beneficiaries through Aadhaar-linkages include INR 425.57 crore for the NSAP pension schemes, and 181.54 crore from scholarships managed by the Ministry of Minority Affairs and the Ministry Social Justice and Empowerment (DBT Mission 2018). As with PAHAL, however, it remains unclear what percentage of savings can be attributed to Aadhaar alone and what percentage of removed beneficiaries were truly fakes or duplicates versus false exclusions. As Aadhaar seeding increases across a variety of programs and agencies, we are likely to see more savings estimates, which will hopefully add clarity to the debate over the program's impact.[35]

Pakistan

Pakistan's National Database and Registration Authority (NADRA) has also reported significant savings in G2P transfer programs by using its unique identity database to weed out multiple registrations. In particular, the NADRA example shows how a robust identification system can be used to quickly deploy emergency assistance while limiting fraud. In 2010, for example, the government launched the Watan Card program in response to devastating floods that displaced some 20 million people, or over 10 percent of the country's population (BBC 2010). The program rapidly disbursed cash grants—initially PKR 20,000

33 The government argues that the false exclusion rate is likely to be low because the drop-off was highest among customers who bought the largest amount of LPG before DBT was implemented, suggesting that they were likely to be rich households or ghost accounts (Subramanian and George 2016).

34 Beyond social protection programs, selected agencies and local governments have also begun to use Aadhaar to eliminate fraud in wage payments. Although many municipal corporations in India have experimented with biometric attendance machines for staff, the Greater Hyderabad Municipal Corporation (GHMC) is among the first to use an Aadhaar-Enabled Biometric Attendance System (AEBAS). In mid-2017, the GHMC implemented this system for the approximately 21,500 workers in health facilities, including health care staff and sanitation workers. Rather than manual tracking of hours worked, employees must verify their daily attendance by authenticating their Aadhaar number against one of some 1,200 handheld biometric devices at the health facilities. According to the Corporation, this system has reportedly led to a monthly savings of INR 2.86 crore (a little under US$445,000, or US$20.7 per worker) by identifying fake and duplicate sanitation staff and eliminating worker absences (New Indian Express 2017).

35 Another emerging example comes from the mid-day meal scheme (MDM), a program that provides free lunches to school children. During 2017, Aadhaar seeding reportedly identified around 272,000 fake or ghost beneficiaries, including over 215,000 in Andhra Pradesh, over 42,400 in Arunachal Pradesh, and nearly 14,000 in Manipur. These reports have not yet included savings estimates; however, a reduction in fake students of only 1 percent could lead to an annual savings to the Union government of some 1 billion rupees (around US$15.4 million) per year, assuming an annual expenditure of INR 10,000 crore (Nanda 2017). This estimate does not take into account potential savings to States, who co-finance the MDM scheme.

per household, or around US$235 in 2010—to households in affected regions using the NADRA database and Visa-enabled payment cards. Individuals registered using their Computerized National Identity Cards (CNICs) at centers across the country, and NADRA then cross-checked these applications to verify the validity of the CNICs, whether other family members had enrolled, and whether the address of residence was in a flood-affected area. Initially, some 2.7 million people applied to claim the flood grants. Of this total, around 1.1 million (nearly 40 percent) were found to be ineligible or were duplicate family members (Hakeem 2010). Compared with the cost of paying grants to all 2.7 million individuals who applied, this translates to an estimated savings of some PKR 21 billion (US$248 million in 2010) in the first phase of the program.

The success of the Watan program built on NADRA's 2009 experience registering internally displaced persons (IDPs) to distribute cash grants to households affected by military operations against the Taliban in the Swat Valley. Of the 755,464 families who initially registered, nearly 30 percent were found to be multiple registrations of the same person, around 12 percent were found to have invalid or no CNIC cards, and nearly 10 percent were cases where multiple family members from the same household had attempted to register. Additionally, some 5 percent were determined to be ineligible based on residence outside the affected areas. In total, this validation process eliminated around 56 percent of applications, leaving a final list of approximately 330,000 beneficiary families (Hakeem 2010). Based on a grant amount of PKR 25,000 per household, this exercise yielded a savings of approximately PKR 10.6 billion (around US$130 million in 2009), compared with the cost of distributing the grant to every applicant. As with the Indian cases, however, some percentage of rejected applicants for both the Watan and IDPs programs may have been false exclusions, including some of the 12 percent of IDPs who were removed from the beneficiary list for not having a valid CNIC card.

In addition to safety nets, NADRA has also taken steps to use its database to eliminate fraud in the public payroll and pension systems. Without a unified civil servant database, it was relatively easy for individuals to collect salaries for multiple departments; in one case, for example, a person was registered both as a doctor and as a police officer, drawing two full-time salaries. By reconciling these records against the unique CNIC number, NADRA was able to identify ghosts and double-dippers, including 20,000 in Sindh province alone. The agency also found fraud in the pension system, as well as some cases where those who should have been receiving pensions (due to age and previous employment in the public sector) had been falsely excluded. This project, however, was not fully completed, and we do not have estimates on total savings (Malik 2014, 2017b).

Uganda

Like India and Pakistan, Uganda has recently rolled out a robust national ID program with a UIN, which now covers some 18.4 million Ugandans over age 16 and 10.5 million children aged 5–16—nearly 70 percent of the total population.[36] The government has plans to integrate the UIN with a variety of databases, including the Uganda Revenue Authority (URA), the Uganda Bankers Association, mobile network operators, and credit reference bureaus. One of the early uses of the national ID database, however, has been to help eliminate payroll fraud.

Beginning in 2014, the Office of the Auditor General began collecting the biometrics of civil servants as part of a payroll audit to address irregularities uncovered by a forensic report. This effort was later continued by the Ministry of Public Service (MPS), which incorporated this biometric data into its Integrated Personnel and Payroll system (OAG 2014). Once the NIN reached a sufficient level of coverage, MPS was then able to cross-check its existing biometric records against the national ID database. Between September 2016 and June 2017, the identity of some 307,916 public officers were verified using biometric matching. Of these,

36 Figures reported to the World Bank by the National Identification and Registration Authority (NIRA) in late 2017.

the identity of some 4,664 officers could not be verified, either because they failed to register for the NIN (and were thus considered to be ghosts) or because their names differed from the information in the national ID database. These identities were submitted to the Inspectorate General of Government (IGG) for investigation, and were removed from the payroll. Of the 4,664, some 2,477 had irreconcilable information, and the remainder are still under investigation. As a result of these removals, the government was able to save over UGX 24.6 billion (approximately US$6.9 million) in less than a year (MPS 2018).

Examples from Functional Registers

In addition to the above examples, there are a number of cases where G2P programs have created functional identification systems or used biometric deduplication within their own databases to eliminate multiple and fraudulent enrollees within their registers. Despite their limited scale and autonomy from foundational systems, these examples illustrate similar cost-savings mechanisms as cases where G2P administrators leverage a foundational unique ID.

One often cited case is that of Nigeria, which implemented an eID system called the Integrated Payroll and Personnel Information System (IPPIS) for its civil servants. Beginning with a pilot in 2007, the IPPIS biometrically enrolled employees in a limited number of federal agencies. Through registration and deduplication, this process uncovered approximately 60,000 fictitious employees (some 20 percent of these agencies' payrolls), reportedly saving the government US$1.12 billion dollars over the 2007–2014 period (Gelb and Diofasi Metz 2018). Ghana has also been able to reduce payroll fraud using the unique identifier in its e-Zwich payment system. Among other applications, the e-Zwich system—which relies on fingerprints for enrollment and authentication—was used to verify the identities of National Service System employees when receiving wage payments. The government reports that this process allowed them to eliminate some 35,000 fictitious employees from the initial agency payroll of 75,000, leading to a savings of US$35 million per year (Yeboah 2016).

Another example comes from India where—before implementing the Aadhaar program—a number of states experimented with biometric registration and smart cards to reduce fraud in social programs, including PDS, NREGS, pensions, and others. The most advanced case comes from Andhra Pradesh (AP), where a 2008 initiative used iris-scan technology to deduplicate the state's PDS beneficiary database, which contained 86 million records in a state with 83 million people. At only 60 percent complete, the exercise had already identified some 7 million duplicate ration cards (around 8 percent of all cards). Because these cards were commonly used as proof of ID for other social programs, the project was also able to eliminate some 255,000 duplicate pensioners and 347,000 duplicate housing beneficiaries. The result was a reported savings of US$6 million per month for PDS, US$1.6 million per month for pensions, and a one-time savings of US$5 million in housing grants. At this rate, AP's investment of US$10 million in backend software was recovered in less than a month (Zelazny 2012).

Identifying Ineligible Beneficiaries

In addition to identifying duplicates and ghosts, some government agencies have used identification systems to improve the targeting of social programs, saving money by removing beneficiaries who do not meet eligibility criteria. Where foundational identification databases themselves have sufficient information for targeting, simply linking a single G2P register with the foundational system can achieve this goal. This is the case in the Pakistan example described below, where eligibility was based on attributes already held by NADRA (e.g., address, household, and occupation).[37] Typically, however, assessing eligibility for social

37 The same is true for the Watan and IDP programs in Pakistan discussed in the previous section. Because eligibility for these programs was based on household and address information that the NADRA database already contained, the agency was able to check for eligibility at the same time that it screened for duplicates.

programs requires broader information on income levels and other individual or household characteristics that may be held in a variety of databases (e.g., tax and property records). In such cases (e.g., Argentina and Thailand), integration between a foundational unique identifier (e.g., a UIN), the G2P register, *and* other relevant databases can facilitate data exchange or queries that allow administrators to verify relevant identity attributes from multiple sources.

Argentina

Argentina is one of the first countries to use a digital identification system to improve the targeting of its social programs by electronically cross-checking eligibility indicators across a variety of databases. In 1998, the federal government began developing the *Sistema Nacional de Identificación Tributaria y Social* (SINTyS), which allows for communication and data exchange across multiple databases at the federal, provincial, and municipal levels (World Bank 2008). The first phase of the project involved integrating a subset of core databases, including registers of formal sector workers and pensioners, the electoral roll, beneficiary lists for 34 social programs, health insurance for public sector employees, a list of the deceased, real estate records for some provinces and cities, the vehicle register, the tax register, a list of poor households (SISFAM), and the national ID number (DNI).

After being cleaned and standardized, these databases were linked by seeding each one with the most reliable and unique of the country's existing identifiers, the unique taxpayer ID number (CUIT) (Pessino and Fenochietto 2007). This allowed the government to identify inclusion errors across pensions and social programs, with an estimated savings of approximately US$143 million between the 1999–2007 (World Bank 2008). By 2008, the SINTyS system had been expanded to cover over 200 agencies and 500-some databases across all levels of government, providing additional opportunities for savings. During the later phases of the project, the system continued to help rationalize social spending. In 2013 for example, the government estimated that the system saved over US$160 simply from removing deceased individuals from social benefits registries that year.[38] Combining this conservative estimate with the savings from 1999–2007, this yields a combined savings in G2P programs of some US$303 million, which is roughly eight times the US$38 million in World Bank funds used to implement the project (World Bank 2014b).

Thailand

Another example comes from Thailand, where the Ministry of Finance implemented a program in 2016 to give subsidies of 1,500–3,000 baht (US$45–90) to individuals who make less than 100,000 baht (US$3,000) per year. In order to register for the scheme, beneficiaries were required to present their national ID cards, and the national ID number was then checked against a number of databases to determine eligibility, including the identity database maintained by the Ministry of the Interior (to verify that beneficiaries were still alive at the time the transfer was made), the Revenue Department database (to check for earnings), and the list of agriculturalists held by the Ministry of Agriculture and Cooperatives (MOAC) (to verify occupation). In total, these checks eliminated approximately 660,000 (7.9 percent) of the 8,375,383 people who applied. Most of these (around 600,000) were individuals who claimed to be agriculturalists on their applications, but who could not be found in the MOAC database. This translates into a potential savings to the government of between US$29.7–59.4 million in transfers, compared to a process without this vetting. The Ministry of Finance renewed this program in 2017, and will increase the number of databases against which applicants are verified, including the Bank of Thailand, land department records, the social security office, and the statistical office (Ministry of Finance 2017).

---

38 This calculation used the average value of benefits within each registry and assumed that deceased individuals were dropped from the registries one month after identification. This is a relatively conservative estimate of total impact as it includes only one year of the program and does not measure the effect of removing other types of fraudulent or ineligible beneficiaries (World Bank 2014b).

Pakistan

Beyond the emergency assistance programs described above, Pakistan has also reported savings from identifying ineligible beneficiaries in G2P programs through integration with the NADRA system. One such linkage was with the Benazir Income Support Program (BISP)—the country's largest social safety net—which distributes unconditional cash transfers to women in poor households each month. When the program was initially launched in 2008, targeting was done by parliamentarians, who were each issued with nomination forms used to solicit recommendations for beneficiaries in their communities. This process generated an initial list of 3.3 million people based on completed forms, which was given to NADRA for screening (Masood 2017). After using information in the NADRA database—e.g., checking whether or not applicants were Pakistanis living abroad or civil servants, or if they had filed taxes or applied for a passport, etc.—to generate a poverty score, NADRA determined that only 2.24 million were eligible for assistance (Masood 2017; Malik 2014, 2017b). Based on the initial monthly payment amounts of PKR 1,000 per family, this would have saved an estimated 1 billion rupees (around US$13.9 million at the time) in the first year of the program, compared with making payments to the initial list of 3.3 million.

NADRA also provided eligibility checks for beneficiaries of the government's program to redistribute zakat[39] funds collected by banks to those living in extreme poverty. Using algorithms similar to the BISP program to give beneficiaries a poverty score, NADRA found that some 3 billion rupees, approximately US$39 million, were being directed to those who did not meet the program criteria. This savings amount was large enough that the government was able to create additional zakat-funded programs, including providing wheelchairs to the disabled and supporting orphans (Malik 2017b).

Preventing Impersonation and Leakage

By ensuring that a person is who they claim to be, robust digital authentication can help curb fraud and leakage by reducing beneficiary impersonation. When combined with digital payment mechanisms, it can also help create an electronic trail of transactions that makes it more difficult for intermediaries to siphon off funds (Abraham et al. 2017). Digital authentication therefore has the potential to increase the efficiency of government spending by ensuring that a higher proportion of transfers go to the intended recipients, and/or create fiscal savings by preventing previously leaked funds from leaving government coffers. Despite the promise of this technology, however, there are few examples of quantified reductions in fraud due to the secure authentication of G2P transactions.

In part, this is because digital authentication for G2P payments is rather new and remains relatively rare, particularly in developing countries. In addition, measurement is complicated by the fact that it is difficult to observe the rate at which authentication prevents fraud. In the case of biometric authentication, for example, the failure to match fingerprints could either indicate success in curbing impersonation or failure to correctly identify legitimate beneficiaries (also known as a "false rejection," as discussed in more depth in Section 4). One limited example that comes from a functional identification system in India is described below; however, we are likely to see more evidence of the impact of digital authentication on efficiency and fiscal savings as this technology becomes more widespread.[40]

India

In parallel to its program to use iris scans to deduplicate the PDS registry in 2008 (described above), Andhra Pradesh attempted to reduce leakage in NREGS and Social Security Pension (SSP) transfers by switching

39 Zakat is one of the pillars of Islam, and requires individuals to give 2.5 percent of their assets to charity.

40 In Pakistan, the government has also reported that biometric authentication of Watan card beneficiaries helped save approximately PKR 639 million by preventing 31,947 attempts at impersonation (Hakeem 2010).

to a new payment system that used biometric authentication. Under the biometric system, beneficiaries were enrolled using fingerprints and (in most cases) issued with smart cards linked to newly created bank accounts. Pensions and NREGS wages could then be collected by inserting the cards into point-of-service (POS) devices that would authenticate the user's fingerprint against a template stored on the card (or in a few cases, on the POS machines themselves).

In a randomized evaluation of the program during 2010–2012, Muralidharan et al. (2016) found that the proportion of households who reported working through the NREGS program was 7.1 percentage points higher in sub-districts with biometric cards, compared with sub-districts that used traditional payment processes. Furthermore, although the government outlays for NREGS were held constant, household income from NREGS increased by 24 percent, a substantial increase in efficiency. This suggests that the payment and authentication process made it more difficult for officials to overreport the amount of work that beneficiaries had done and then siphon off a portion of their wages. Overall, Muralidharan et al. (2016) estimate that the biometric cards resulted in a 12.7 percentage point decrease in leakage in the areas where they were deployed for NREGS. For SSP payments, they find a smaller but still statistically significant 2.8 percentage point reduction in leakage. As a percent of outlays, this implies an annual savings of approximately US$38.5 million for NREGS and US$3.2 million for SSP (Muralidharan et al. 2016).

Although the system did not reach full-scale implementation and the government's outlays remained the same—as payments now reached the intended beneficiaries rather than being siphoned off—this case illustrates the potential of secure authentication mechanisms to curb leakage and improve the efficiency of service delivery. However, it remains unclear how much of the reduction in leakage can be attributed to stronger authentication alone, and how much was due to the change in payment mechanisms,[41] or to the biometric registration of beneficiaries that may also have eliminated duplicates or ghosts. With AP and other states now seeding databases like NREGS, SSP and PDS with Aadhaar numbers on a large scale, we are likely to see more estimates of the effect of Aadhaar authentication on reductions of impersonation and payment fraud in the future.[42]

3.2. Reducing Administrative Costs

A second opportunity for decreasing government expenditures comes from the ability of digitization, unique IDs, interoperability, integration, and digital authentication to reduce operating costs within a country's identity ecosystem. The collection, management, and use of personal data is a central theme of government administration (Scott 1998). This requires a variety of identification systems and transactions within and across many departments beyond those that manage G2P transfers—which as described above, must identify potential beneficiaries, collect enough data to ensure eligibility, and authenticate or verify users at the point of transaction.

Conducting elections, for example, requires creating and maintaining lists of eligible voters and checking voters' identities at polling stations. Border control requires a system of issuing and checking passports. Transportation safety requires a system to register eligible drivers and their cars and issue them with licenses. Development planning requires aggregating or estimating demographic characteristics for the

41 In addition to biometric authentication, the new payment system avoided multiple transfers between government layers, as funds were transferred electronically from the State to a technology provider, and then to the customer service providers (CSPs), who issued cash payments directly to beneficiaries. Under the old system, funds had been transferred electronically from states to districts to *mandals,* who then transferred cash to gram panchayats (local governments) for distribution (Muralidharan, Niehaus, and Sukhtankar 2016).

42 In AP's Krishna district, for example, there are reports that Aadhaar-based POS authentication of PDS beneficiaries has helped prevent shop owners from diverting rations that are not picked up (World Bank 2018a). However, we do not yet have concrete estimates of savings from this case.

entire population, which begins with the collection of individual and household data on occupation, migration, income levels, etc. Taxation requires knowing who potential taxpayers are, determining the size of their tax obligation based on factors such as income, investments, and property, and then crediting payments and issuing refunds to the correct individuals.

Operating all of these identification-related systems can be expensive. This is particularly true in paper-based systems, which as discussed above, require labor intensive, manual administration throughout the identity lifecycle. These inefficiencies are multiplied in fractured ecosystems where each register is maintained by a separate agency with little or no communication between them. Because they have no economies of scale in terms of data collection or management, the operation and maintenance of fractured systems can be quite costly. In Nigeria, for example, a World Bank assessment estimated that the fiscal burden of maintaining the country's various overlapping foundational and functional identification systems will amount to US$4.3 billion, including the US$1.2 billion spent between 2011 and 2015 and the US$3.1 billion needed to continue these programs over the medium term (World Bank 2015).

Figure 4: Pathways to Savings by Reducing Administrative Costs

2. Expenditures: Reducing Administrative Costs

Pathways	*Features*	*Conditions*
a. Reduce staff time and transaction costs	**Digitization** of foundational system; **Unique ID** in foundational system; **Integration/ Interoperability** of various registers; **Digital authentication** at point of service	• Coverage • Robustness • Level of inefficiency
b. Eliminate redundant systems	**Digitization** of foundational and functional registers; **Unique ID** in foundational system; **Integration/ Interoperability** of various registers	• Coverage • Robustness • Level of redundancy

Note: Digitization alone is unlikely to have large effects on allowing governments to eliminate or reduce the size of redundant systems. However, it does play a supporting role in facilitating the development of a unique ID which can be integrated into a variety of registers.

As shown in Figure 4, there are two primary pathways through which features of modern identification systems can reduce some of these operating costs. The first is through decreasing the per capita cost of identity-related transactions for both foundational identity providers and the functional agencies that rely on their systems. Strong identification systems can decrease transaction costs directly by reducing the staff time and resources needed for identity verification, authentication, and management processes, and indirectly by enabling cost-saving services such as e-Government portals and remote payment systems. The second path to administrative savings occurs when countries are able to create a foundational identification system with enough coverage and interoperability or integration to rationalize duplicative functional systems. Although different agencies often require separate data systems given their different purposes, attributes, and target populations—and the need to protect personal data and privacy—there may be opportunities to downsize in certain areas, such as the number of credentials issued. Country examples are presented below for each of these pathways.

Reducing Transaction Costs

Creating, verifying, and authenticating identities entails a variety of transactions between individuals and governments and between government agencies themselves. Transitioning from a paper-based system to a digital one, creating a unique ID, increasing interoperability and integration, and building digital authentication capacity each have the potential to directly reduce the cost of many of these transactions, as shown in Table 4. Direct savings come primarily from reducing staff time and resources—such as the cost of printing, postage, and telephone calls—needed for identity-related transactions. In addition to identity providers themselves, these benefits can accrue to G2P providers (as in Slovenia), as well as entities in charge of immigration and border control,[43] taxation (as in the United States), justice departments, housing and census agencies, departments in charge of property and land records, and business registers, etc.

Table 4: Role of Identification Systems in Reducing Transaction Costs

	Savings Effect	Location
Direct	Reduce costs of identity creation/verification/ authentication	Foundational ID providers + other agencies
Indirect	Facilitate e-Gov services	Foundational ID providers + other agencies
	Facilitate electronic and direct payments	G2P providers

In addition, identification systems that provide secure authentication mechanisms (e.g., an ePKI system based on a unique ID) can also indirectly reduce transaction costs for a variety of agencies by enabling e-Government or "self-service" portals, e-invoices, and digital payments. E-Government portals can decrease operating costs by allowing individuals to complete transactions—e.g., requesting ID cards, filling out benefits applications, requesting building permits, etc.—online rather than in person or over the phone (as in the U.S. and Estonia examples discussed below). In the UK for example, one report estimated that the country would save between GBP 1.7 and 1.8 billion (US$2.3 to 2.4 billion) per year if 82 percent of the services that process over 10,000 transactions were moved online.[44] Similarly, secure authentication mechanisms can also enable electronic payments directly to beneficiaries, which has the potential to increase the efficiency of G2P transfers by eliminating cash or check-based systems. Before Aadhaar implementation began, for example, one study estimated that the Indian government could save some US$4.4 billion per year in reduced transaction costs by connecting every household to a digital automated payment system (Gelb and Decker 2011).[45]

43 In Pakistan, for example authentication of an applicant's biometrics and verification of their CNIC card against the NADRA database has allowed the passport agency to simplify its identity proofing process. Previously, they conducted labor-intensive data collection for each applicant from the local police and other departments; now, the agency simply pays a fee of PKR 35 (currently around US$0. 35) for near instant verification (Malik 2017b).

44 On average, this represents an approximate 25 percent reduction in administrative costs for these services, not taking into account adoption costs. A majority of these savings would come from decreases in full-time employees (78 percent), estates and accommodation (12 percent), printing and postage (7 percent), and IT systems and equipment (4 percent). Overall, evidence suggests that transactions done face-to-face, via post, or over the phone are 50, 30, and 20 times more expensive than digital transactions, respectively (UK Cabinet Office 2012).

45 Although official savings figures from Aadhaar-enabled payment transactions have not yet been made public, some claim that the per-transaction cost of a payment to an Aadhaar-linked account would be close to zero, compared with transaction costs for payments made by credit cards (around 3.5 percent) or debit cards (between 1.25 to 1.5 percent) (ET 2017). Another estimate suggests that using Aadhaar would reduce KYC costs from approximately US$15 to US$0.50 per transaction (BusinessLine 2016). Estimations from the private sector also give some indication of potential benefits for the government: according to one, Aadhaar may reduce an average firm's onboarding cost of obtaining and validating client data from US$23 to US$0.15 per person (World Bank 2018c).

Slovenia

Slovenia operates a number of social security programs, including child benefits, cash grants and income support, rent subsidies, education benefits, and support for health services and insurance. After the financial crisis in 2009, demand for these services was high, and the government needed to improve the efficiency and transparency of eligibility determinations and ensure that limited resources reached those who needed it most. At the time, however, the Ministry of Social Affairs used a legacy IT system that was fragmented among various programs. Furthermore, it had limited connections to the 50-plus institutions that held information necessary to verify program eligibility, including the population register, households register, tax records, property, vehicle and land registers, educational enrollment, health and insurance enrollment, employment status, and financial investments. As a result, the Ministry relied mostly on labor-intensive methods for the verification of identity attributes, including sending and receiving official requests for information on each applicant to disparate data-holders via the postal service (Gabrijel 2013).

To overcome these inefficiencies, the government began developing an "e-Social Security Interoperability platform" in 2011, which became operational in 2012. This platform allows for queries across social security and other databases and administrative agencies, including systems for e-Procurement, e-Higher Education, and the government certification authority (Gabrijel 2013; European Commission 2016). On average, the system manages 16,587 queries per day, or approximately 6,000,000 per year for a population of around 274,000 beneficiaries. By eliminating paper-based queries, the European Commission estimates that this system has saved the Ministry of Social Affairs some EUR 12.3 million (approximately US$14.5 million) per year.[46] This *yearly* savings is almost nine times the initial investment of EUR 1.4 million for the system in 2011, and 23 times its average operational costs of EUR 516,660 per year (European Commission 2016).

United States

The U.S. Internal Revenue Service (IRS) also spends significant resources on transactions with taxpayers, particularly during the annual tax filing period. In 2012, this included processing over 30 million paper-based tax returns, sending over 220 million pieces of mail, and fielding some 90 million phone calls. In total, phone and mail correspondence with taxpayers cost the IRS an estimated US$1 billion in 2012 (NIST 2013). A report by the National Institute of Standards and Technology (NIST) argues that creating a secure credential for authentication could drastically reduce the agency's operating costs by enabling it to move more of its services online (NIST 2013). Although the IRS currently offers e-filing options that are US$3.41 cheaper per transaction than paper-based filing, the lack of a secure digital authentication mechanism has deterred users who worry about identity theft and the security of their information when filing online. By increasing the level of assurance, NIST argues that a trusted digital credential would increase the adoption of online services, saving between US$91 million and US$318 million annually, depending on the demand for the service and whether the credential was provided in-house or by a third party. Taking into account the cost of implementation, they estimate that the net benefit would be between US$74 million to US$305 million per year (NIST 2013).

The report argues that cost savings would be maximized if the agency were to adopt a third-party credential provided by trusted private sector entities, rather than developing a proprietary system. This is due to the fact that a significant portion of the IRS's mail and phone communications are currently devoted

46 This figure is based on an estimated cost of EUR 45.45 for 50 queries per beneficiary per year, multiplied by the number of beneficiaries in 2011 (n = 274,000). The estimate of EUR 45.45 per person assumes a cost of approximately EUR 36.83 per person for outbound queries from the Ministry of Social Affairs (assuming 50 queries of 0.7366 each), and approximately EUR 8.62 to process the responses to the queries (e.g., receiving and opening envelopes, and scanning and archiving them). These per-query rates assume that processing each inbound query will take three minutes of staff time under a minimum monthly wage of EUR 1,200, along with the cost of paper, printing, envelopes, and postal service, while processing a query response will take approximately 1.5 minutes of staff time (European Commission 2016).

to assisting users with authentication (e.g., taxpayers and tax preparers calling to retrieve forgotten PINs). By relying on a third-party credential, the agency could outsource both the cost of identity proofing and authentication-related customer service. Furthermore, because the third-party credential could grow into a foundational credential used by a wide variety of e-Government services, this would reduce the overall transaction costs charged by the provider by increasing economies of scale. According to NIST, the reduction in these expenses alone would save the IRS between US$556,000 and US$1.9 million annually, compared with developing a proprietary credential. Overall, the report estimates that the initial cost of implementing digital authentication would be US$40 to US$111 million less—and ongoing operational costs would be US$2 to US$19 million less per year—if the IRS were to adopt a foundational credential rather than an IRS-only system (NIST 2013).

Estonia

Estonia has one of the world's oldest and most advanced foundational eID systems. The system is underpinned by a national population register and a smart eID card, issued since 2002. In a population of some 1.3 million people, more than 1.2 million eID cards have been issued (Vassil 2015). The smart cards, along with mobile-based eID applications offered since 2007, use PKI technology based on secure certificates and PINs to provide digital authentication and digital signatures for thousands of online services, including banking, tax filing, medical prescriptions, and even voting in national and European elections. In addition, the Estonian X-Road system provides an interoperability layer for the country's many identity databases, both private and public. Relying primarily on the National Personal Identification Code—a unique identifier issued by the Citizenship and Migration Board—as a key, X-Road allows for queries and information exchange between disparate databases. This provides for seamless identity verification, significantly decreasing transaction costs for government agencies as well as users, and reducing the amount of data collected by mandating that government identity providers only collect information that is not already available from an X-Road-linked provider. As of 2017, X-Road processes some 500 million queries annually, over 400 per eID-holder.[47]

There are a number of estimates of the fiscal impact of Estonia's eID system. One often-cited figure is that the eID has increased GDP by some 2 percent annually (around US$500 million), as a result of improving the efficiency of identity-related transactions and bringing 99 percent of services online (Gelb and Diofasi Metz 2018). According to a cost-benefit analysis by the Estonian Certification Centre, digital signatures alone have saved over EUR 200 million (e-Governance Academy 2016). Another study by Vassil (2015) estimates the benefits of X-Road in terms of time saved. Conservatively assuming that each of the 113 million X-Road transactions in 2014 saved approximately 15 minutes, this results in a savings of some 3,225 years of time.[48] Further assuming that government staff work eight hours a day for 260 days a year, this is the equivalent workload of approximately 13,460 full-time employees for one year (Vassil 2015). If these staff were paid an average of EUR 15,000 per year,[49] this would amount to over 200 million euros in yearly salary, assuming fewer staff hours were allocated. Together, this savings represents a combination of efficiencies provided by secure authentication, as well as the ability to move transactions online; however, it remains difficult to isolate the former from the latter.

Eliminating Redundancy in Identification Systems

In addition to improving the overall efficiency of identity-related transactions, interoperability or integration between identification systems with sufficient coverage and robustness can create the opportunity to

47 See https://e-estonia.com/solutions/interoperability-services/x-road/ for updated estimates.

48 These calculations are framed as cost savings to *individual customers/users* interacting with the government; however, we might also assume that 15 minutes per transaction is a conservative estimate for the staff time required for identity-related or other service transactions.

49 This is close to the average gross annual wage in Estonia, as of 2017 (see https://www.stat.ee/news-release-2017-091).

reduce or eliminate some redundant aspects of the identity ecosystem. In theory, this could apply to a number of sectors. For example, countries that create unified social registers to underpin the delivery of multiple safety nets may be able to eliminate some or all of the legacy systems previously used to manage each transfer in isolation. Similarly, an up-to-date-population register linked with a variety of social and economic databases could eliminate the need for some periodic censuses.

Most of the cases with data on cost savings, however, come from countries (e.g., South Africa and Malawi) that have used foundational registers and credentials to underpin voter lists, thereby reducing the costs of voter registration and/or eliminating the need for separate voter ID cards.[50] Stand-alone costs for one-off voter registration campaigns can be quite high, particularly when they use biometric technology to deduplicate voter lists or authenticate voters. Gelb and Diofasi (2016), for example, look at 12 Sub-Saharan African countries and find that the typical overall costs for an election range from US$5 to US$20 per person, and approximately one-third of this—frequently tens of millions of dollars—is for biometric technology. The gains from linking foundational identification systems and credentials to electoral systems are thus potentially large in scope if countries are able to avoid duplicate data collection or separate credentials.

South Africa

South Africa has been able to significantly reduce its expenditure on electoral administration over the past two decades, in part by linking voter registration with the national ID. Beginning in 1999, the Independent Electoral Commission (IEC) began using the national ID booklet and UIN as the basis for continuous (rather than mass) voter registration. Citizens register to vote by filling out paper applications with address information, and election officials then scan the bar code in their ID booklets with handheld "zip-zip" readers. Using the UIN as a key, this data is checked against the National Population Register maintained by the Department of Home Affairs (DHA). The zip-zip readers also print receipts confirming registration that are affixed to the ID booklets. This system has been used since 2009 to confirm eligibility on election day by scanning the receipts with zip-zip readers loaded with the entire voter list (Evrensel 2010).

The integration between the national ID system and voter registration and identification has been relatively cost effective. The first post-apartheid elections in 1994 were conducted before the integration and cost approximately US$250 million, part of which included the cost of printing temporary voter cards for those who lacked national identity documents. In 1999, the cost was approximately US$170 million, a 30 percent cost reduction. By 2009, this cost had fallen to ZAR 240 million (US$32 million, or ZAR 10.4/US$1.4 per capita in 2013 prices). A majority of the country's expenses for the 2009 elections were for 30 thousand new zip-zip readers, which were purchased for ZAR 160 million (US$21.4 million) (Evrensel 2010).

Not all of these savings can be attributed to the identification system itself. For example, some of the decreases in cost are likely due to the move from mass to continuous registration, and the decline in the number of voters by around 20 percent between 1994 and 1999 (World Bank Forthcoming). However, integration and cooperation between the DHA and IEC systems have clearly streamlined the enrollment process and averted the need to issue separate voter ID cards. Indeed, despite the higher cost of labor in South Africa (around 50 percent of the IEC's expenditures) the per-elector cost of elections in South Africa *declined* by 9 percent in real dollar terms between 1999 and 2014, but increased by 167 percent for the average Sub-Saharan African (SSA) country in real dollar terms. Given the relative efficiency of ID-enabled voter registration and identification in South Africa—and the significant investments many other SSA countries have made on biometrics and other high-tech equipment for election administration—it is likely

50 Foundational identity credentials can only feasibly replace voter ID cards to the extent that they can be used to verify the right to vote (normally citizenship and age), and potentially also a person's address, depending on the election. This may not be desirable or feasible in all cases.

that part of this discrepancy can be attributed to the IEC's ability to leverage the national ID system (World Bank Forthcoming).

Malawi

A more recent example of eliminating redundant systems in electoral administration comes from Malawi, which is in the process of building a new eID system to improve identification within the country and underpin a variety of services. A rapid enrollment campaign began in 2017, and the system covered around 7.7 million people as of October, with plans to cover the population of over 9 million adults by the end of the 2017 (Malik 2017b). One of the first third-party users of the ID is the Malawi Electoral Commission (MEC), which will integrate the eID into voter identification and authentication ahead of the upcoming 2019 elections. Rather than reregistering voters by collecting extensive personal information, MEC will generate the voter list through a door-to-door campaign where enumerators will scan the quick response (QR) codes of registrants' cards and verify these against the eID database, extracting the individual's photo.

Although this does not eliminate the registration campaign entirely, the process is anticipated to be much less labor intensive, reducing the need to collect duplicate information. In addition, the integration between the eID and MEC will allow Malawi to eliminate the need for a separate voter card. Instead, the eID cards will be used as proof of identity for voting and compared to the photo obtained from the database during registration. During the previous election in 2014, MEC reportedly spent US$44 million on voter ID cards alone. Assuming a similar price in 2019 adjusted for inflation, this represents a huge potential savings to the government equal to approximately 90 percent of the initial investment in the eID project (US$49 million) and far greater than the cost of adapting the MEC system to leverage the eID (Malik 2017a).[51]

3.3. Increasing Tax Collection

In addition to reducing program and operational costs, identification systems can also help governments raise additional revenue through two key mechanisms, the first of which is increasing tax collection. Low levels of tax revenue are a chronic problem in many developing countries (and also some wealthy ones). In Tanzania, for example, the National Identification Authority (NIDA) estimates that of those 14 million people capable of paying taxes, only 1.5 million do (around 10 percent). In India, the Ministry of Finance estimates that only 35 million people—fewer than 3 percent of the total population—regularly pay taxes (Atick 2016a). Across Latin American countries, approximately half (52 percent) of potential tax revenues are lost to tax evasion (Cavallo and Serebrisky 2016).

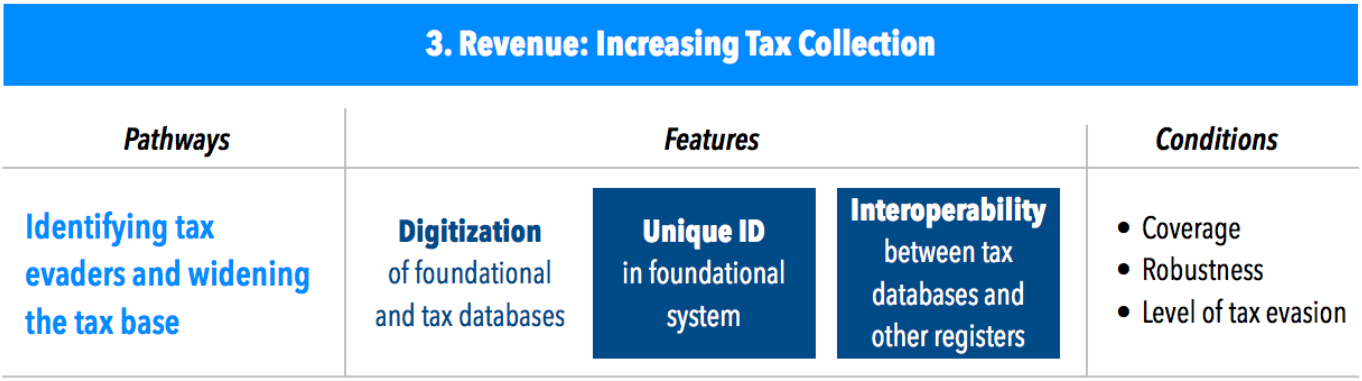
Low tax collection stems from a number of issues, including tax evasion.[52] The task of finding tax evaders—those who are liable but are not paying taxes at all, or those who are underpaying relative to what they owe—is a complex information problem. The government must know who does and does not pay taxes, be able to assess each individual or business' tax liability based on their income, properties, investments, etc., and have the capacity to enforce tax collection. When earnings and assets cannot be verified by third party sources (e.g., property registers, declarations of salary from employers, etc.), taxpayers have an incentive to underreport their liability or forego paying taxes all together. The lack of accurate and reliable identification systems for taxpayers therefore weakens tax collection and enforcement and increases administrative costs related to compliance and tax arrears management.

---

51 Although the full cost of adaptation is difficult to estimate, the largest ticket item is likely to be the QR readers purchased by MEC in order to read the info from the ID cards. A total of 5,000 machines were needed for the 2019 elections. At a cost of approximately US$350 each, this totals around US$1.75 million dollars, or 3.9 percent of the cost of voter ID cards in 2014 (Malik 2017b).

52 Overall, increased revenue collection is a product of both tax policy changes and administrative reforms, including identification.

Figure 5: Pathways to Generating Revenue by Increasing Tax Collection



Note: Digitization alone is unlikely to have large effects on increasing tax revenue. However, it does play a supporting role in facilitating the development of a unique ID that can be integrated into tax registries and other databases to identify tax evaders.

In order to address these issues, many countries adopt taxpayer identification numbers (TIN). TINs are widely regarded as best practice in tax administration and can help increase compliance and reduce fraud (e.g., particularly for value-added taxes, or VAT) by ensuring the uniqueness of individuals and businesses and facilitating longitudinal recordkeeping. If other agencies also collect or record the TIN, this can facilitate interoperability between revenue agencies and other areas of government that allows for the exchange of key information needed to verify tax liabilities.

However, where a unique TIN does not exist or where the tax register has low coverage, a foundational unique ID linked with the tax database can help improve taxpayer identification, potentially broadening the tax base and improving compliance (see Figure 5). First, a unique population register can provide the denominator for assessing the rate of individual tax payment and identifying the total base of potential taxpayers who may not yet be registered by the tax administration. Furthermore, when integrated into the tax database, a unique ID can be used to deduplicate tax records, identifying individuals who use multiple tax IDs to decrease their liabilities (e.g., as India plans to do).

Additionally, identification systems that link the tax administration with other government agencies, databases, and big data sources—e.g., land records, vehicle registers, customs databases, and social benefits registers—can better identify businesses or individuals who are underreporting their earnings or assets and generate risk scores to better target audits (e.g., in Argentina, Pakistan).[53] As discussed above, potential increases in revenue may also be complemented by reduced expenditures on tax administration to the extent identification systems can streamline and automate core business processes (e.g., the U.S. IRS). Although a strong identification system is insufficient to solve all the problems of tax administration, it can increase revenues at the margin and serve as a necessary foundation for broader tax reform.

53 There are other types of tax-related fraud that may also be reduced through stronger identification systems, but for which we do not yet have clear estimates. In the U.S., for example, the IRS loses over US$5 billion per year due to tax refunds erroneously made to identity thieves and impersonators, an amount that could be decreased with the implementation of secure online authentication mechanisms (NIST 2013).

Another example is the multiple claiming of individuals (e.g., children, others) in systems that offer tax deductions. In Thailand, for example, the government gives tax incentives to companies that employ disabled people. In some cases, the Revenue Department found that multiple companies were claiming the same person in order to qualify for the deduction. By linking the business' registration numbers with the national tax ID numbers of these employees, the Department has been able to ensure that they are not claimed by multiple companies. To date, however, there have been no estimates of the scale of revenue recovered from this initiative (Revenue Department 2017).

Argentina

In addition to the initial US$143 million in savings from better-targeted social programs discussed above, Argentina's SINTyS system has also been used to increase tax revenue. By linking tax databases together with other registers (including property and vehicles), the system enabled authorities to improve audit targeting and uncover more instances of tax fraud, evasion, and arrears. This integration is estimated to have generated approximately US$44 million in additional revenue during the initial phases of the project between 1999 and 2007 (World Bank 2008). The overall effect of SINTyS on tax collection is likely to be higher, as this figure does not take into account the potential for higher levels of compliance among individuals who—though they were not audited themselves—may have paid more taxes in anticipation of the higher probability of being audited under the SINTyS system (Pessino and Fenochietto 2007).[54] As the system has developed further over the past 10 years, it is likely that it has continued to contribute to higher rates of tax collection; however, the revenue impacts for later phases of the project are not available (World Bank 2014b).

Pakistan

In 2012, Pakistan also experimented with using NADRA's capabilities to identify tax fraud through links between various databases. Out of a population of around 190 million, there were fewer than 800,000 taxpayers. Under an agreement with the Federal Bank of Pakistan, NADRA was able to query a variety of databases to determine frequent travelers, individuals with multiple bank accounts, residents of wealthy neighborhoods, owners of expensive cars, high utility users, arms owners, and white-collar employees. This data mining allowed NADRA to identify some 2.4 million wealthy individuals who did not yet have national tax numbers, as well as 1.2 million who had tax numbers but were not filing. At the time, NADRA estimated that an additional 100 billion rupees (about US$1 billion) in revenue could be generated within three months if a fraction of these 3.6 million were to begin paying some of the taxes they owed (Malik 2014).[55] Simply adding the 2.4 million previously unidentified tax payers into the system would have increased the potential tax base by 300 percent.

India

The Indian government plans to use Aadhaar to address tax fraud perpetrated by individuals who use multiple or fake tax IDs (Permanent Account Numbers, or PANs). PAN cards are required for filing income tax returns along with a variety of other transactions, including purchasing property and bank deposits of over 50 thousand Rupees (Dhoot 2017). As of 1 July 2017, existing PAN card holders will be required to submit their Aadhaar number when filing taxes, and Aadhaar numbers will also be required for those applying for a new PAN card. The government hopes this linkage will weed out duplicate or fake PANs, which are commonly used for money laundering, and tax evasion. In a recent exercise, for example, the Income Tax Department deleted or deactivated over 1.14 million duplicate cards, as well as 1,566 fakes (Falak 2017; Times of India 2017). Linking the PAN system with Aadhaar has the potential to identify even more fraud. Estimates of recovered revenue from this program are likely to be forthcoming by the end of the 2017/18 fiscal year.

---

54 Italy's National Revenue Agency also uses a system of linking disparate information in order to detect tax fraud, relying on big data from both the public and private sector. The *redditometro* (or "income measurer") system analyzes over 100 life-style indicators, including things like car ownership, vacations, gym memberships, cellphone usage, clothing, and payment of private tuition to estimate expenditures. If expenditure is 20 percent higher than a person's declared income, the account is flagged and an explanation is required (Povoledo 2013). The result is better targeted audits, which has reportedly helped the country recover significant tax revenue (Boston Consulting Group 2012).

55 For example, if 1 million of these individuals (less than a third) paid a minimum amount of PKR 100,000 (around US$1,000 at the time), this would yield 100 billion.

3.4. Charging User Fees

The final mechanism through which identification systems can raise revenue for governments is the opportunity for identity providers to charge fees for various services. Unlike the other three mechanisms, these benefits accrue only to the foundational identity agency itself. And although any identity provider can levy fees for its services, fee-charging models are typically found in fiscally autonomous agencies empowered to raise and manage their own revenue.

Identity providers can charge fees both to individuals and to third party entities for identity-related services, as shown in Figure 6. Charging individuals for identity services is common in foundational systems, whether digital or paper based, and typically includes fees for obtaining credentials and for expedited application processing. Some countries have reported significant savings from this model. For example, Rwanda's National Identity Agency (NIDA), charges US$0.72 for the basic national ID card, except to those who are unable to pay and receive the card for free. In addition, it charges much larger fees for expedited processing, passports, and driver's licenses, which together reportedly generate enough revenue to cover the agency's full operating costs (Atick 2016b; Gelb and Diofasi Metz 2018).[56] In Pakistan, NADRA also helps subsidize free cards by charging expedited processing fees for those who wish to pay a small fee.[57] Digitization brings the opportunity to charge for additional value-added services. For example, countries can have a tiered pricing model, providing basic ID cards for free but charging extra for advanced eID cards. In Peru, for example, citizens—with the exception of vulnerable populations, who are exempt—pay around 29 Nuevo Soles (US$10) for a basic adult ID and 40 Nuevo Soles (US$14) for the eID (World Bank 2014a). Other examples include allowing users to opt in to an SMS or e-mail service that alerts them when their application is ready, for a small additional fee.

Figure 6: Pathways to Generating Revenue by Charging Fees for Identity Services

4. Revenue: Charging Fees

Pathways	*Features*				*Conditions*
a. To individuals for ID services	**Digitization** of foundational and third party registers				• Coverage • Robustness • Prices
b. To third parties for authentication services	**Digitization** of foundational and third party registers	**Unique ID** in foundational system	**Integration/ Interoperability** with third parties	**Digital authentication** of individuals	• Coverage • Robustness • Prices • Number of transactions

Note: In principle, identity providers can charge fees to users (e.g., for expedited services) regardless of the type of identity system or its level of modernization. However, some opportunities for services (e.g., charging for an optional smart card, automatic notifications when applications have been processed, etc.) require the digitization of databases and/or credentials. Similarly, identity providers *could* charge fees to third parties in systems without digitization, comparing lists of registers by hand, however this is likely to be highly inefficient and not a reliable source of revenue.

56 NIDA does not currently charge third parties for verification or authentication, but may roll out fees for issuing other credentials, such as diplomas or professional certificates (Gelb and Diofasi Metz 2018).

57 As of October 2017, the maximum fee for expedited processing was PKR 1,000 (around US$10) for the basic CNIC and PKR 1600 (around US$16) for the new smart card. See https://www.nadra.gov.pk/fee-structure/ for a current list of fees.

A second fee-based model involves charging fees to third parties—including public agencies, banks, mobile operators, and other private companies—for identity verification or authentication services. This requires digital credentials such as a unique ID, along with some form of integration or interoperability platform with the third parties. For example, an identity agency could create a platform for banks to digitally verify the name and address of a new applicant in order to meet KYC requirements, charging a small fee for each transaction (e.g., as in the Peru and Pakistan cases discussed below).

On the whole, this pathway may offer greater potential for revenue generation than individual fees, given the volume of identity-related transactions with third parties. However, although this revenue stream can allow identity providers to invest in their systems and reduce dependence on government budgets, there is also a risk that such fees can place a burden on users by driving up their operating costs or can create barriers for the population to access services if users pass on the costs to the population. In addition, charging fees to individuals—particularly for obtaining basic credentials—can work against the principle that identification is a public good and should be accessible to all individuals, regardless of ability to pay.[58] Setting fees therefore requires finding a balance between earning revenue and ensuring that services are inclusive and in demand. In addition to a strong regulatory framework, this has been accomplished by varying fees for different users or types of services. These issues are discussed more thoroughly in Section 4.

Peru

Peru's *Registro Nacional de Identificación* (RENIEC) has provided online identity verification services using biometrics since 2009. Initially, the service was provided to allow notaries to verify the identity of individuals for transactions such as property sales. Since then, it has been expanded to cover many public and private entities, including social welfare agencies, the justice department, police, banks, commercial centers, and telecom companies. In general, private entities are required to pay a fee for verification or authentication services, while public agencies receive these services free of charge. However, in certain cases—such as government-mandated biometric authentication checks for the onboarding of mobile customers—private-sector third parties may also be exempt from certain fees (RENIEC 2018). [59]

Prices for fee-paying third parties are based on (a) the type of information requested, (b) the number of queries, and (c) whether verification relies on wired connections or the agency's website. *For non-biometric attributes,* a variety of authorized users—e.g., small banks, commercial centers, etc.—can query the RENIEC database via the *website* at a per-transaction cost of PEN 0.9 (US$0.28) for basic information such as name or date of birth; PEN 1.2 (US$0.37) for additional information such as photo or address, and PEN 1.6 (US$0.49) for higher-level data such as a signature. For third parties such as banks that have a *wired connection* to the RENIEC database, similar non-biometric queries are priced by bulk and cost between PEN 0.6 (US$0.18) for 0–400,000 queries to PEN 0.11 (US$0.03) for 1,600,000+ queries. *Biometric queries* that match individuals' fingerprints against the RENIEC database in order to establish identity or uniqueness are mainly used by notaries, telecoms, the police, and social programs. These queries return a "yes/no" response from RENIEC and are priced between PEN 1.5 (US$0.46) for 0–30,000 queries to PEN 0.14 (US$0.04) for 1,200,000 or more queries (RENIEC 2017a).[60]

RENIEC processes around 250 million verification queries per year. Of these, approximately 70 percent are performed free of charge for public agencies, while 30 percent are for private entities. In total, this yields

58 See, for example, the *Principles on Identification for Sustainable Development* (World Bank 2017b).

59 Before 2017, a few public services that charged end users—e.g., driver's licenses and passports—payed fees to RENIEC for authentication and verification. As of 2017, however, all public entities are no longer required to pay fees as part of an effort to promote interoperability (RENIEC 2008).

60 An updated list of services and fees can be found on the RENIEC website at http://www.reniec.gob.pe/portal/Tinstitucional.htm.

approximately US$45 million in revenue annually (RENIEC 2017b, 2018). The agency also receives fees from charging for ID cards. For example, some 500,000 new eID cards have been issued to date. At a cost of PEN 40 (US$14) per card, this has generated some US$7 million in revenue (RENIEC 2018). Together, these revenue streams cover approximately 70 percent of the agency's budget (Gelb and Diofasi Metz 2018).

Importantly, RENIEC's policies and oversight mechanisms help ensure that charging for services does not become a barrier for inclusion. The price of each service is set *equal to the cost* that RENIEC incurs for providing that service, as determined through periodic assessments of its business processes conducted by the Manager of Administration and Budget. Fees for services to poor individuals are also free of charge and are subsidized by the central government (RENIEC 2018).[61]

Pakistan

Another example of a fee-charging model comes from Pakistan's NADRA. The agency provides verification and authentication services to a number of public agencies, including the election commission, social protection agencies (e.g., BISP, the disaster management authority, and the Zakat and Bait-ul-Mal departments), microfinance institutions, the Federal Bureau of Revenue, the courts, provincial and local governments, and the passport and immigration department. It also facilitates authentication services for private firms, including banks, other financial institutions, and telecom companies. Some of these transactions are done online in real time, while others are performed in batches for specific needs.

In general, public sector agencies are charged PKR 15 (currently US$0.14) per transaction, while private firms are charged PKR 35 (around US$0.33) per transaction. For example, NADRA verified 100 million SIM card identities for the Pakistan Telecomm Authority in 2014, which at a per-unit fee of PKR 15 would have netted approximately PKR 1.5 billion (some US$14.7 million at the time). Each month, approximately 5.4 million BISP beneficiaries have their credentials verified to receive their cash transfers, yielding approximately PKR 972 million (around US$9.3 million in current rates) in revenue annually. NADRA also verifies voter identities; for the 2013 election, this consisted of 86 million queries, which would have translated into approximately PKR 1.2 billion (US$12.2 million) in revenue (Malik 2016). Together with external contracts—e.g., to supply driver's licenses in Bangladesh—and charging for certain services such as expedited processing and other premium products (e.g., smart ID cards), these fees are sufficient to fully cover NADRA's operating costs.

3.5. Additional Sources of Savings

Beyond the main mechanisms considered above, identification systems may have additional fiscal benefits for the public sector that are either indirect or difficult to measure. Furthermore, there are a number of ways in which these systems may generate savings for individuals and donors, as well as savings, revenue, and a business-friendly climate for the private sector. Although a full analysis of these potential benefits to the economy as a whole is outside the scope of this paper, each is discussed briefly below.

Governments

The savings opportunities provided by robust and inclusive foundational systems may extend beyond the mechanisms described above. Generally, well-run identification systems that protect privacy while offering clear benefits may be able to increase trust in government, with a variety of difficult-to-measure benefits. For example, a trusted identification system may reduce the likelihood that election results are disputed, thereby decreasing risk of election violence and its associated human and financial costs.[62] Post-election

61 For more information on the methodology for setting costs and prices, see Government of Peru (2012) (in Spanish).

62 In Kenya, for example, post-election violence in 2007–08 cost over 1,200 lives and displaced some 500,000 people. The associated economic cost was an estimated loss of US$8 billion over the 2007–2011 period (Gelb and Diofasi 2016).

violence is strongly correlated with disputed election results, which are frequently caused by controversies over the composition of voter lists or accusations of voter fraud. In a 2016 paper, Gelb and Diofasi argue that an investment in biometric technology for voter registration and/or authentication is likely to be worth the cost if it is able reduce the probability of election violence by only a few percentage points.[63] Although the benefits of reduced election violence may be difficult to quantify, they can be large. Other examples could include efficiencies created by having more data available for long-term development planning, more responsive service delivery, improvements to security and border control, and more. Given these additional potential sources of savings, the model developed above is likely to underestimate the effects of identification systems on the public purse and on overall government capacity.

Individuals

Identification systems that reduce fraud and increase the efficiency of transactions can also produce substantial savings for individuals. By virtue of reducing leakage and impersonation, households will receive a greater portion of G2P transfers to which they were entitled. This was the case with Andhra Pradesh's biometric payment cards, which increased household income from NREGS wages by approximately 24 percent (Muralidharan, Niehaus, and Sukhtankar 2016). In addition, strong identification systems can save significant time for individuals by reducing transaction costs, for example by streamlining identity-related transactions and facilitating digital payments and e-Government services.[64] For example, Muralidharan et al. (2016) also find that NREGS workers with biometric payment cards spent 19 percent less time collecting wage payments and experienced 39 percent fewer payment delays. Similar benefits have been reported during the implementation of Aadhaar-based payments in Andhra's Krishna District, including an increase in user satisfaction among PDS beneficiaries and fewer complaints registered at fair price shop (FPS) dealers (World Bank 2018a).

In Morocco, a World Bank study estimates that creating a unified register to streamline beneficiary identification for the country's main social programs would save each household an estimated two hours of work at minimum wage per year (Angel-Urdinola, El-Kadiri, and Pillares-Millares 2014). In Korea, a cost-benefit analysis of an early e-Government portal estimated that direct and indirect benefits to individuals would reach some KRW 1,113.6 billion (US$890 million in 2002) from a reduction paper documentation and lower transportation and time costs. This is over 300 times the cost of KRW 3.3 billion needed to create the portal (Joon Song et al. 2016).

Donors

Donors and development partners—including multilateral and bilateral agencies and many international NGOs—often require some means of identifying beneficiaries in order to target or distribute aid and other goods. In many cases, donors have ended up creating one-off systems specific to a particular project, which can be expensive and wasteful. The ability to leverage preexisting identification systems within a country therefore has the potential to save significant portions of assistance budgets. In Pakistan, for example, the World Bank, DFID, USAID and other donors provided approximately US$580 million in financing for the Watan emergency transfer program for flood victims. By using NADRA's preexisting database and infrastructure to manage enrollment and eligibility determinations, implementers were able to keep administrative costs to around 2 percent of the total budget (some US$10 million), freeing up the vast majority of funds for direct distribution to beneficiaries (Malik 2017b).

---

63 The technology, of course, is not a panacea. Its ability to reduce the probability of violence depends on the degree to which the technology is able to improve the public perceptions of credibility (Gelb and Diofasi 2016).

64 Gelb and Decker (2011), for example, find that traditional payment methods can cost up to 20 percent of the grant amount for individuals to collect, and can take up to a day in terms of travel time to local offices or distribution points. Identification systems that facilitate digital payments therefore have the potential to produce large savings for recipients.

Private Sector and Economy as a Whole

Finally, identification systems can have positive fiscal impacts for businesses and the economy as a whole. In a companion piece to this paper, the World Bank (2018c) demonstrates that many of the same mechanisms through which identification systems save money for public sector also apply in the private sector. A strong identification system provided by the government can decrease firms' expenditures by reducing (a) administrative and transaction costs associated with customer onboarding and identity management, (b) fraud and theft by improving identify verification and preventing impersonation, (c) compliance costs with KYC, consumer due diligence, and anti-money laundering regulations, and (d) liability costs associated with holding personal data. In addition, such systems can boost firms' revenues by (a) increasing customer bases by removing a barrier to access for consumers (e.g., for financial services), (b) decreasing customer abandonment and rejection due to improving verification and authentication, (c) and allowing companies to charge fees for identification services (World Bank 2018c).

Identification systems may also have broader impacts on the economy similar to that of other ICT infrastructure. This could include job creation in sectors related to developing authentication software and infrastructure, as well as e-Government services. As with broadband, it is possible that the creation of a digital identification system could act as a multiplier in other sectors to increase overall economic productivity (Min and Rossotto 2012; Qiang and Rossotto 2009). Where such systems develop cross-border linkages—e.g., interoperability that allows a government to verify attributes of ID holders from other countries—they may also facilitate trade. However, these wider impacts are difficult to identify and measure.

4. Guide for Practitioners: Toward a Savings Model

The above cases provide preliminary evidence that strong identification systems can generate savings and revenue opportunities across a variety of public agencies and through diverse mechanisms (see the Appendix for a summary of cases). Through the adoption of digitized systems that provide unique IDs, interoperate or integrate with functional registers, and offer digital authentication infrastructure, countries can decrease fraud in transfer programs, reduce the cost of administration across a variety of ministries, increase tax collection, and charge fees for identity services to create additional revenue streams.

At the same time, it remains difficult to develop a general estimate of the fiscal impact expected from these systems overall. A lack of reliable data limits our ability to make valid cross-country comparisons, particularly given the number of variables that can affect savings and revenue in a particular country—e.g., the precise features of the identification systems, how they are used and in which sectors, levels of coverage and robustness, prices set in fee-charging models, and exogenous factors such as the levels of fraud and inefficiency. However, using the framework of features and mechanisms developed in Sections 2 and 3, Section 4 offers an initial Guide for Practitioners to estimate context-specific sources of savings and revenue for current or future projects. This Guide proposes a set of concrete steps to explore the viability of different mechanisms in a specific context and highlights important issues to consider during planning and implementation.

4.1. Assessing Savings and Revenue Opportunities

This Guide provides an overview of key questions and information necessary to explore avenues for savings and revenue generation through investment in identification systems. It is intended to be a first step toward a more systematic assessment of the benefits of these systems, and is not a definitive checklist.[65] In addition to policy makers and practitioners planning new identity-related investments, this Guide should also be useful to researchers attempting to further evaluate the fiscal impacts of identification systems.

Reducing Fraud Targeting in G2P Transfers

For many countries, a primary motivation for adopting modern identification systems is their ability to reduce fraud and leakage in transfer programs. In order to evaluate the potential scope of savings from this mechanism, it is necessary to first take stock of existing G2P transfer programs that could potentially be linked to a foundational identification system.

65 Any assessment of the fiscal impact of an identification system should be adapted to suit the country context. A recent cost-benefit analysis of options for implementing a national identification strategy in Zambia, for example, focused on assessing financial benefits in four areas: (1) linking social welfare programs to the ID system, (2) streamlining election administration, (3) facilitating easier KYC for banks, the financial sector, and telecom companies, and (4) preventing money laundering (World Bank 2017a).

STEP 1. Inventory of existing G2P programs

Primary examples of G2P programs that may benefit a strong identification system to reduce fraud typically include:

- Payroll
- Pensions
- Cash transfer programs
- Emergency assistance programs
- Subsidy and ration programs
- Health insurance
- Educational benefits

However, not all programs will benefit equally from integration or interoperability with unique IDs or databases. Some may already have robust ways of detecting and preventing fraud and accurate methods of targeting intended recipients. For example, many countries already use biometrics to weed out duplicates in social transfers and have advanced targeting protocols to reduce inclusion errors. Conversely, leveraging foundational identification systems is likely to have the greatest marginal benefits in cases where there are serious concerns about the prevalence of ghosts, duplicates, and ineligible beneficiaries. Similarly, the impact of digital authentication on savings is likely to be highest in programs where there are serious concerns about leakage due to identity theft or the impersonation of recipients.

STEP 2. Calculate expected savings from fraud reduction

For each relevant program, a preliminary estimate of potential savings can be calculated with the following information:

- Number of beneficiaries (current and projected)
- Average value of transfers (current and projected)
- Estimated percent of duplicates and ghost beneficiaries
- Estimated percent of ineligible beneficiaries
- Estimated rate of impersonation

For example, imagine a country with 20 million people (the average size of a country in Africa) that employs 1 percent of its population (200,000 civil servants) and pays them an average salary of US$12,000 per year (Table 5, Panel 1). The government estimates that some 15 percent of these employees are duplicate or ghost beneficiaries, and 1 percent of payroll transactions involve identity fraud (i.e., impersonation). In addition, it has a cash transfer program that pays US$300 per year to ten percent of its population (1 million people), with an estimated 10 percent ghosts or duplicates, 5 percent impersonation during payment transactions, and 30 percent inclusion errors of ineligible beneficiaries. The government plans to weed out ghosts and duplicates in both programs by integrating a foundational unique ID number into their databases. Furthermore, it hopes to eliminate impersonation by implementing digital authentication for transfers, and to eliminate the large number of estimated ineligible beneficiaries in the cash transfer program by linking these databases with property, tax, and utility registers via common adoption of the unique ID.

Table 5: Stylized Example of Reduced Fraud from Identification Systems

Panel 1. Current estimates

Department/ Program	Payroll	Cash Transfer
(A) Total recipients	200,000	1,000,000
(B) Average transfer value (USD/year)	12,000	300
(C) Estimated ghosts or duplicates	15%	10%
(D) Estimated impersonation	1%	5%
(E) Estimated ineligible	0%	30%

Panel 2. Reduction in fraud and leakage (robustness x coverage = 100%)

Fraud Reduction	Formula	Payroll	Cash Transfer	Total ($ millions)
Removing ghosts/duplicates	A x B x C x 100%	360	30	390
Reducing impersonation	A x B x D x 100%	24	15	39
Removing ineligible	A x B x E x 100%	-	90	90
Total ($ millions)		384	135	519

Panel 3. Reduction in fraud and leakage (robustness x coverage = 50%)

Fraud Reduction	Formula	Payroll	Cash Transfer	Total ($ millions)
Removing ghosts/duplicates	A x B x C x 50%	180	15	195
Reducing impersonation	A x B x D x 50%	12	8	20
Removing ineligible	A x B x E x 50%	-	45	45
Total ($ millions)		192	68	260

The effectiveness of the system in reducing fraud will depend on the features implemented—in this case, integration with a unique ID, digitally enabled authentication, and interoperability with other databases—as well as the level of coverage and robustness (accuracy) in the system.[66] In this example, the upper bound of savings would be US$519 million per year for these two programs if the system had 100 percent coverage and accuracy (i.e., all fraud is eliminated) (Table 5, Panel 2). However, under a more realistic assumption

66 Coverage and robustness rates are combined here as a deflator for the upper bound of savings (which assumes that 100 percent of fraud is removed). For example, a system with 100 percent coverage but only a 50/50 chance at eliminating fraud would suggest a multiplier of 0.5. Similarly, a system with 80 percent coverage and 90 percent accuracy would suggest a multiplier of 0.72.

of 50 coverage and robustness (i.e., where fraud is reduced by only 50 percent), annual savings would be around US$260 million (Table 5, Panel 3).[67]

This basic exercise will give a rough estimate of the order of magnitude of expected benefits from implementing various features of identification systems. As is evident, the largest savings come from those programs with the highest levels of fraud *and* the largest transfer amounts (in this invented example, this is payroll). Estimates can be made more precise by varying the level of coverage and robustness by program or system features[68] and adjusting for inflation and expected growth rates in the population size, recipients, and transfer amounts.[69]

STEP 3. Address measurement challenges

Once a project has been implemented, actually *attributing* a reduction in fraud and leakage to the identification systems poses a few challenges. The first are standard issues with identifying cause and effect. In order to say definitively that an identification system was responsible for an observed decrease in fraud and leakage, we would need to be able to hold all other factors constant.[70] Beyond this, however, is the difficultly in observing—and thus measuring—fraud in the first place. Rather than direct measures, most estimates have relied on proxies for fraud reduction, including looking at changes in expenditure or in the number of beneficiaries enrolled and receiving transfers before and after identification programs were implemented.

In some cases, the change in enrollment may be a good proxy for removal of ghosts and duplicates. In many other cases, however, it can be highly inaccurate (see Figure 7 for an illustrated example). It may be the case, for example, that some eligible beneficiaries were removed from the database in error. Similarly—and particularly where the implementation of identification systems involves the reenrollment of the population—it may be the case that eligible individuals who were previously excluded from the database have now enrolled, increasing the overall number of records. A more conservative option is to track and measure the precise number of identities removed from the database during the identification process. However, this number may still overestimate fraud reduction if it includes false removals of eligible beneficiaries, or underestimate fraud reduction by excluding the number of fake beneficiaries who do not attempt to reenroll.

---

67 In Zambia, for example, some studies have suggested that leakage in social transfer programs may be between 25 and 35 percent (World Bank 2017a). However, a recent cost-benefit analysis estimates that using the national ID to clean beneficiary lists and facilitate secure direct benefits transfers in four programs—the Public Service Pension Fund, the food security program, social cash transfers to households, and the Farmer Income Support Program—could save between US$604 million and US$2.04 billion. This calculation conservatively assumes that the identification program will reduce only a fraction of this leakage, or around 5 percent (World Bank 2017a).

68 For example, a biometric-based unique ID linked to a transfer program may have a higher success rate in removing ghosts or duplicates than interoperability between G2P databases may have in identifying ineligible beneficiaries.

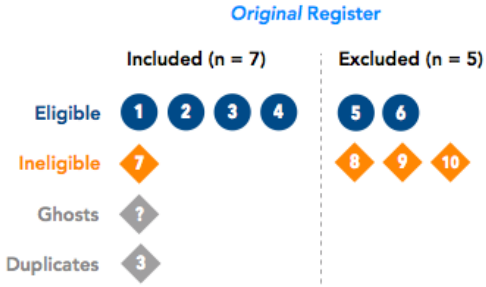
69 Note, also, that these calculations assume that ghosts, duplicates, impersonation, and ineligibility are mutually exclusive categories of fraud. In reality, the situation may be more complex.

70 It may be the case that other variables that affect fraud—and the enrollment and expenditure levels used to proxy fraud—have also changed during the implementation period. This has been an issue for estimating savings from India's PAHAL program, for example. Initial figures cited by the government wildly overestimated the impact of Aadhaar because they calculated savings as the difference in transfer amounts before and after Aadhaar without accounting for a substantial decrease in fuel prices that had occurred at the same time and accounted for a majority of the change in expenditure (Abraham et al. 2017; Gelb and Diofasi Metz 2018).

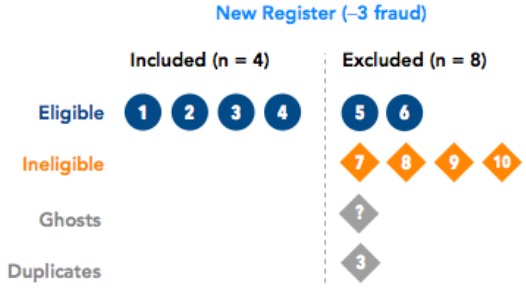
Figure 7: Illustration of the Difficulties in Measuring Fraud Reduction in G2P Registers

1. Assume a population of 10 people, six of whom are eligible for a cash transfer program and four of whom are ineligible:

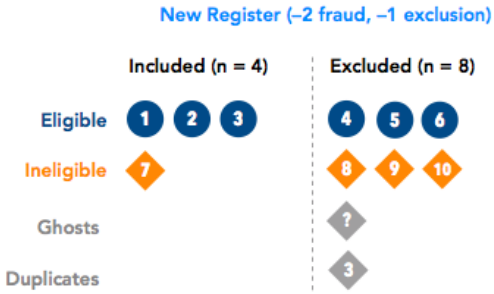
2. Before implementing a unique ID, the G2P program database is exclusive and non-robust. Some eligible beneficiaries are excluded, some ineligible are included, and there are some ghosts and duplicates:



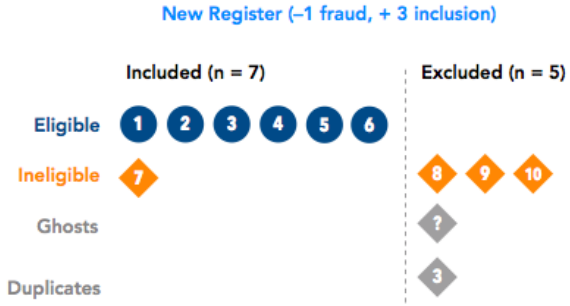
3. Ideally, integrating a unique ID with the G2P register and cross-checking eligibility with other registers will remove all ineligible, ghost, and duplicate recipients. In this case, the change in the database (–3) is equal to the reduction in fraud.



4. However, it is unlikely that the system will completely eliminate fraud, and also possible that some *previously included* eligible individuals would be *excluded by error*. In this case, the change in the database (–3) is NOT equal to the reduction in fraud.



5. It is also possible that some fraud is eliminated, but the ID program also encourages previously excluded but eligible beneficiaries to enroll. In this case, the total number of enrollees stays the same (7), but there has been both a reduction in fraud *and* an increase in inclusion.



The challenges of measuring reductions in impersonation via digital authentication are even greater than that of measuring reductions in ghosts or duplicates, as discussed in Section 3. This is particularly true when it comes to biometric authentication. In a hypothetical world with a zero percent false rejection rate (FRR)—i.e., where any rejected attempts at authentication were not in error—the number of rejections would provide an indication of the quantity of fraudulent transactions prevented.[71] However, the FRR rate in the real world is significantly above zero percent, meaning that many rejections may not be instances of fraud, but rather the failures to correctly identify a legitimate user.

71 It would not provide a full estimate because it would still not capture potential fraud deterred by the system (i.e., if people know there is a high likelihood of being caught under the new system, they may not attempt fraudulent transactions in the first place).

In Andhra Pradesh, India, for example, an average of 17.4 percent of individuals experienced failed pension payment transactions after multiple attempts at fingerprint authentication between April 2015 and March 2017 (of these, 84.2 percent were due to biometric mismatches, rather than Aadhaar database-related errors or server/operational issues). In Telangana State, NREGA payment transactions failed after multiple attempts at fingerprint authentication for an average of 7.8 percent of beneficiaries (94.8 percent due to biometric mismatches) (Abraham et al. 2017). Given the challenge of knowing which are "true" vs. "false" rejections, a simple measurement of the rejection rate cannot be equated with fraud reduction. Instead, such figures would need to take into account reported grievances from authentic recipients who might have been falsely rejected during authentication. Although no measurement strategy will be perfect, collecting as many metrics (e.g., as shown in Table 6) as possible will improve the accuracy of data and estimates used to calculate reductions in fraud due to identification systems.

Table 6: Suggested Metrics for Evaluating the Effect of Identification Systems on Fraud

Removing Ghosts, Duplicates, Ineligible	Reducing Impersonation
Data to collect: A. attempted enrollments (or original # in database) B. initially flagged (disaggregate by duplicates, ghosts, ineligible) C. total enrolled/kept in database after addressing flags D. total rejected/removed after addressing flags (disaggregate by duplicate, ghost, ineligible E. grievances submitted after rejections/removals	**Data to collect:** A. attempted authentications B. initially rejected authentications that move to repeated attempts or alternate mechanisms C. total accepted authentication attempts D. total rejected authentication attempts E. grievances submitted after authentication failures F. FRR according to technical/lab specs of technology
Unobserved: *F. ghosts/duplicates/ineligible deterred from enrolling* *G. unique, eligible persons deterred from enrolling* *H. true number of false rejections* *I. true number of false accepts*	**Unobserved:** *G. impersonators deterred from attempting authentication* *H. real beneficiaries deterred from authentication* *I. true number of false rejections* *J. true number of false accepts*
Hypothetical measures: • Reduction in ghosts, dupes, ineligible = **D** + *F* – (*H* + *I*) • Inclusion of targeted beneficiaries = **C** – (*G* + *H* + *I*)	**Hypothetical measures:** • Reduction in impersonation = **D** + *G* – *J* • Exclusion of true beneficiaries = *H* + *I*
Potential proxies: • Reduction in ghosts, dupes, ineligible = **D – E** • Inclusion of targeted beneficiaries = **C – E**	**Potential proxies:** • Reduction in impersonation = **D x (1 – F)** or **D – E** • Exclusion of true beneficiaries = **B** + **E**

Reducing Administrative Costs

The opportunities to reduce administrative costs through the implementation of a strong identification system also vary greatly by country and can be difficult to quantify as a whole. As with reducing fraud, the first step in assessing potential avenues for administrative savings is to take stock of the wide range of agencies and departments whose business processes include the need to identify, verify or authenticate users, issue credentials, or manage personal data.

STEP 1. Inventory of administrative procedures that require identification/verification/authentication

As shown in Table 7, this is likely to include departments that administer core foundational and functional systems, such as those that maintain the national ID, civil register, immigration databases, passport

agencies, electoral administrators, G2P transfers, driver's licenses, education departments, tax authorities, business registers, property registers, and vital statistics systems.

Table 7: Example Inventory of Identity-Related Assets and Procedures

Agency	ID proofing	Deduplication	Credential issued	Verification/ authentication for transaction
National ID provider	yes	biometric	NID	for third parties
Passport agency	yes	no	passport	no
Border control	no	no	no	for travel
Electoral commission	yes	biometric	voter ID	for voting
Tax authority	yes	no	tax ID number	for taxpayers
Transportation authority	yes	no	driver's license	no
Social transfer agency	yes	biometric	benefits card	for transfers
Payroll	yes	biometric	civil servant ID	for payments

For each of these registers and processes, an assessment of expected cost savings from foundational identification systems can include an examination of the potential to either (1) decrease the cost of existing transactions, and/or (2) rationalize or eliminate particular redundant elements of the identity ecosystem.

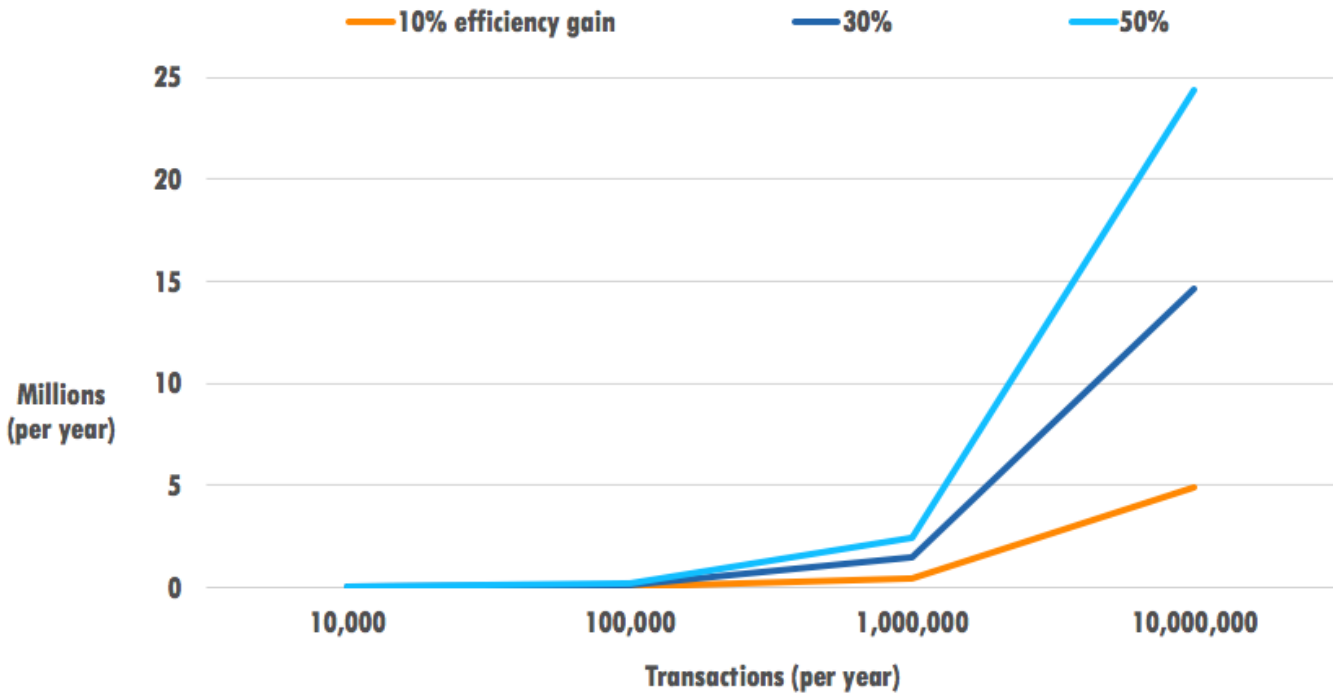
STEP 2. Calculate expected savings from increasing efficiency of transactions

For each register/process, consider:

- **Current costs for performing identity-related transactions.** This should include staff time required to complete certain tasks and other additional resources and materials—such as those needed for printing, scanning, searching, photocopying, and mailing documents, etc.
- **Efficiency gained by identification systems.** Expected reduction in terms of staff time and resources with (a) digitization, (b) a unique ID that facilitates interoperability or integration for identity verification, and (c) digital authentication.
- **Number of transactions.** Estimated current number of transactions per year, as well as potential future transactions if the demand for services grows.

Some efficiency benchmarks from Europe, for example, suggest that digital transactions (e.g., to verify an identity or file an application) range between 2 to 4 percent of the cost of face-to-face transactions (UK Cabinet Office 2012). Absolute savings, however, will be largely determined by the number of identity-related transactions that are transitioned to the new the system, as shown in Figure 8. First, economies of scale are not likely to be achieved with small numbers of transactions. A study of e-Governance in the UK, for example, notes that moving to online transactions would have a much greater potential for fiscal savings in those agencies where transactions were higher than a threshold of 1 million per year, and that moving transactions online for smaller agencies may not be worth the adaptation costs (UK Cabinet Office 2012).

Figure 8: Stylized Savings from Reducing Transaction Costs for Identity Verification/Authentication



Note: Calculations assume a baseline per-transaction cost of 5, based on 30 minutes of staff time per transaction + 2 in additional costs (e.g., printing, photocopies, envelopes, postage, telephone calls, etc.). Staff cost assumptions include an annual salary of 12,000 and 260 8-hour days worked per year. These stylized savings are for *one* identity provider or user; establishing linkages that allow for identity verification/authentication for multiple agencies could multiply this savings.

The number of transactions will depend on a variety of factors, including the overall coverage levels of the identification system (people must have access to an ID in order to use it). In the UK, the government estimated that a digital ID would result in GBP 1.2 billion in savings by facilitating e-Government services that would reduce transaction costs. However, this figure assumed an 82 percent take-up of e-Government services, based on the estimated percent of the total population that has access to the internet (UK Cabinet Office 2012). The coverage and take-up necessary for transaction-related savings are also likely to vary over time. In Estonia, for example, use of the eID card was minimal for the first five years after implementation due to low Internet usage and the fact that few registers and services had linked to the system. As in the UK estimates, the adoption of digital-identity-enabled transactions followed an S-curve pattern, increasing exponentially after approximately 75 public and private actors had connected their databases to the X-Road system (Vassil 2015).

STEP 3. Calculate expected savings from rationalizing systems

In addition to reducing transaction costs, a strong foundational identification system linked to functional registers may offer opportunities to eliminate redundant data collection processes, credentials, or even databases. For each of the assets in Table 7, consider the following:

- **Desirability and feasibility of:**
  a. *Streamlining data collection efforts* (e.g., basing a voter register off of a national population register, rather than conducting a separate registration exercise)

b. *Eliminating a credential* (e.g., separate voter or social security cards)

c. *Eliminating an identity register or database* (e.g., a legacy identity database with poor coverage)

- **Costs saved through (a), (b), and/or (c)** using past and protected expenditures from relevant agencies.

For example, the World Bank recently led a cost-benefit analysis of different options for rolling out an integrated civil registration and identification system (ICRIS) in Zambia. One of the key benefits considered was the ability of the biometric national ID card to streamline election administration by (a) avoiding the need to issue a separate voter ID card, and (b) reducing the time it takes to verify voter identity. Depending on the rollout schedule and how many elections were covered, the analysis indicated that integrating the national ID into voter registration and verification could save the government between $US95 and 135 million (World Bank 2017a).

The potential for savings by rationalizing the identity ecosystem is heavily dependent on preexisting architecture and the cost currently incurred by the government for its maintenance. As with other potential savings estimates, estimates of administrative efficiency gains should also take into account the costs needed for adaptation, which are discussed further in the Key Considerations section below.

Increasing Tax Collection

Identification systems can help increase tax revenue by improving the accuracy of information about current and potential taxpayers. However, they are not a panacea for increasing tax collection. As such, an important first step is to think through the main causes of under-collection and the degree to which improving foundational identification will address these problems.

STEP 1. Identify main sources of lost tax revenue

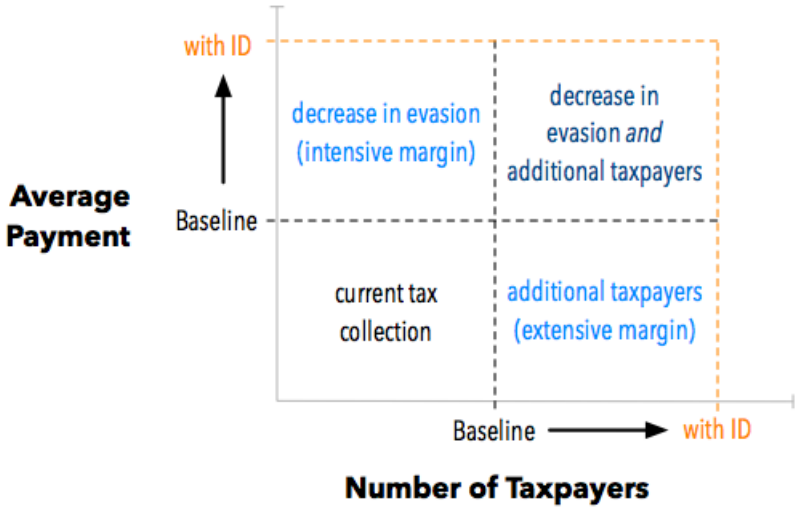
Identification systems can help increase tax revenue to the extent that they help expand the tax base or increase knowledge taxpayers' identities and other attributes used to establish their liability (e.g., their assets and income). For example, improvements in taxpayer identification might help address the following types of issues, among others:

- **Registered taxpayers who underreport liabilities.** Without the ability to independently verify tax liabilities, individuals will have an incentive to underreport (or simply not file) their tax forms. Unique IDs and interoperability frameworks can help ameliorate this issue by linking tax databases to other sources of information, such as property records, utility bills, vehicle registers, and more, which can be used to generate risk scores and better target audits.
- **Nonregistered individuals.** In addition to registered taxpayers who under-declare, there may be large groups of individuals who *should* be registered and paying taxes but are not. Developing a foundational system with high coverage and linking this to the tax database can help identify new taxpayers, widening the tax base.
- **The use of multiple tax ID numbers.** In some cases, individuals may evade taxation through the use of multiple taxpayer numbers or accounts. Integrating a unique ID into the tax register can help deduplicate these records.
- **Fake or duplicate dependents.** In tax systems where individuals receive deductions or other benefits by claiming dependents (e.g., children, disabled or elderly family members, etc.), there are incentives to create fake dependents or for multiple taxpayers to claim the same dependent. Requiring the unique ID for each dependent can reduce these types of fraud.

- **Taxpayer impersonation.** Where the tax administration makes refunds to individuals who have overpaid their taxes, there are opportunities for fraudsters to impersonate these individuals and divert these transfers. A strong authentication system during the tax filing and payment/refund process can help reduce this type of fraud.

Where individual tax identification is improved, this may also lead to **improvements in taxation of businesses,** for example by incorporating owner's unique ID numbers into enterprise tax forms.

Figure 9: Potential Effects of ID on Tax Collection



For the above types of fraud, deduplicating tax databases, linking them to other sources of information, and improving authentication can help increase tax collection on the *intensive* margin by reducing evasion and underpayment among existing taxpayers (see Figure 9). In addition, integrating a high coverage foundational system with the tax database also has the potential to increase taxation on the *extensive* margin by identifying and incorporating new taxpayers into the system. The relative size of these effects, however, is highly context dependent. In addition, it is important to note that strong identification systems will not solve other issues that depress tax collection, including the ability to enforce payments or the prevalence of the informal business and wages that are difficult to tax. Furthermore, if enforcement is weak, simply identifying instances of tax fraud or nonpayment may be insufficient to improve tax collection.

STEP 2. Calculate expected savings from improved tax identification

Estimating the ability of identification systems to increase tax revenue is challenging for the very reason that these systems may be beneficial: governments often have incomplete information on who should pay taxes and how much they should pay. However, countries can begin to estimate expected benefits from improving individual identification to the extent that the following data are available:

- Current number of registered taxpayers and revenue by income group/tax rate
- Estimated level of underreporting by existing taxpayers (e.g., via the methods listed above)
- Estimated number of nonregistered, potential taxpayers by income group/tax rate

The largest gains from improved identification for taxation are likely to come from identifying wealthy individuals and firms that are not registered or are underpaying their taxes. However, as discussed below under *Key Considerations,* these groups likely have vested interests in maintaining the status quo and may resist such reforms. In addition, while improving identification systems can increase the efficiency of tax

administration, these gains often take time, and the link between improved processes for tax administration and increased revenues is not always direct.

Charging User Fees

Charging fees for identity credentials, verification, and authentication services can be an important revenue stream for identity providers, offering some level of autonomy and helping to isolate agencies from short-term fiscal pressures (Gelb and Diofasi Metz 2018). Although this does not strictly *require* digital integration between these systems and third parties—other actors could physically transfer records to be verified via paper or DVD—platforms such as API interfaces or hardwired connections can drastically increase the potential opportunities for fee-charging models. Similarly, digitization of databases and credentials can create opportunities to charge individuals for "luxury" type services such as advanced smart cards or expedited processing. A first step in determining potential revenue from such fees is to enumerate potential services and users.

STEP 1. Enumerate potential fee-charging opportunities

These may include, for example:

- **Third-party users.** Consider both public and private sector users of verification and authentication services, such as G2P transfers, health services, education, passport agencies, driver's licenses, banks, mobile operators, credit reporting agencies, and airlines, etc. A good place to start is with the inventory of identity-related transactions created in the section above (Table 7).
- **Third-party services.** This may include fees for verification of identity credentials (e.g., cards, NINs, etc.) as well as authentication of individuals (e.g., using biometrics) against the central database.
- **Individual services.** This could include, for example, add-on fees for expedited processing or an additional smart card. In principle, such fees should be for optional services in order to ensure the accessibility—and cross-subsidize—basic services to all segments of the population.
- **Transaction volume.** For each of the above potential users and services, estimate current and future annual transactions.

STEP 2. Consider price levels

Setting fees too high may suppress demand and increase exclusion. Because identity services are a public good, some should be highly subsidized or free, including the issuance of basic identity credentials and potentially some verification fees for third parties.[72] For third parties, fees should be affordable both for large organizations and for smaller ones that serve poor, rural, and other marginalized groups.[73] Indeed, fees need not be uniform over time or across users or types of transactions. Some options for price discrimination include:

- **Phasing in fees to grow demand.** In order to ensure rapid up-take by third parties, one option is to initially wave fees or set prices extremely low, and later increase them if demand is sufficient. In India, for example, UIDAI has initially kept all authentication services free in order to lower the barrier to entry for service providers.

72 In accordance with the *Principles on Identification for Sustainable Development, first identity credentials should be issued free of charge.*

73 In Pakistan, for example, there have been concerns from banks that NADRA's verification fees are set too high for small transactions and poor user (Gelb and Diofasi Metz 2018).

- **Pricing based on the user.** In order to harness the utility of identity services across the public sector, most countries have opted for different pricing for government agencies than private-sector users. In Pakistan, for example, NADRA's fees for the public sector are less than half of the cost of those for the private sector. Peru uses a "you charge, I charge" philosophy, providing free verification and authentication services for those entities that do not charge end users, and waives fees for poor individuals.
- **Bulk pricing models.** Identity providers, such as Peru's RENIEC, can also offer bulk pricing discounts for frequent users of identity services. Peru notably also offers different fees depending on the type of data requested and whether authentication and verification services are performed online or via a hardwired database connection.

Other important safeguards against overcharging include consultation with a diverse array of potential users as well as independent oversight and regulation. Given that identity providers often have a monopoly on verification and authentication services, a strong regulatory and oversight framework is necessary to help ensure that rates remain affordable and transparent, and that the ability to generate profits does not create perverse incentives for identity agencies. In Peru, for example, RENIEC's prices are set equal to the cost of the particular service, as determined by an independent regulatory body. This periodic review has allowed the agency to adjust its fee structure over time, helping to keep prices low and credible.

STEP 3. Calculate expected savings from fees

Calculating expected savings from fee-charging models can be calculated simply by **multiplying anticipated fees** by the **expected number of transactions** over a given period. Where services are new, it may be difficult to estimate the latter number. When services—e.g., a biometric card, or identity verification—are first introduced, users may be unfamiliar with the service and it benefits, driving down the expected number of transaction. For example, a country with low Internet penetration may expect low initial demand for digital authentication for online services. In many cases, it may therefore be appropriate to conservatively assume that **initial uptake will be low.** Furthermore, due to the **elasticity of demand**—as prices increase, demand for a particular service is likely to decrease, reducing the overall number of expected transactions.

Hopefully, as the system proves its utility and demand for services grows, the **number of transactions will increase over time.** However, the sustainability of a fee-based revenue stream depends on the system's capacity to handle such growth. In India, for example, UIDAI's capacity is approximately 100 million authentications per eight-hour workday.[74] UIDAI plans to increase capacity by four times in order to handle the anticipated increase in demand for services due to a growing cashless economy and the uptake of the Aadhaar authentication system across a growing number organizations. Advanced planning and investment will help to ensure the long-term adaptability of the system.

4.2. Key Considerations

Any cost-benefit analysis of identification systems should take into account a number of factors beyond the initial estimates of savings and revenue opportunities calculated above. This includes assessing the cost of systems as well as the additional sources of savings discussed in Section 2. Importantly, identity stakeholders must also consider that certain measures that generate fiscal savings and revenue may also risk increasing exclusion or infringing on individual privacy. In addition, measures to reduce identity-related fraud and inefficiency may also encounter resistance from actors who benefit from the status quo.

74 See https://authportal.uidai.gov.in/ for real-time stats on authentication.

Cost of Systems

As discussed in Section 2, the ability of identification systems to generate savings and/or revenue requires significant investment. This includes the cost of deploying system features—digitization, a unique ID, integration and interoperability between systems, and/or digital authentication—with sufficient robustness and then extending coverage to a majority of the population. Recent work by the World Bank benchmarks the cost of various system types and components and provides an in-depth look into key drivers of cost, including credential choice, enrollment timing and operating model, links with the civil registry, choice of biometrics, and type of data collected (World Bank 2018d).[75]

In addition to these main drivers, there may be particular investments needed to take full advantage of fiscal savings and revenue mechanisms. This could include costs associated with:

- **Digitizing functional registers** (e.g., for social transfers, health insurance, taxes, etc.) in addition to foundational ones.
- **Integrating foundational and functional systems** via seeding existing registers with a unique ID number and/or creating interoperability frameworks, API interfaces, etc.
- **Deploying digital authentication infrastructure,** including investments in ICT back-end infrastructure, broadband connectivity across the country, point of sale devices, etc.
- **Implementing fee-based service models** including website development, back-end systems, information campaigns, and outreach.

These adaptation costs may be substantial, and so a full cost-benefit analysis for an identification system should carefully consider these investments alongside potential opportunities for savings and revenue.

Exclusion

Although identification systems can produce fiscal and other benefits for a variety of stakeholders, they may leave some people worse off. Importantly, there is a risk that individuals will be illegitimately excluded from identification and the rights and services it facilitates through the very mechanisms that save governments money. This is a particular concern for two of the cost-savings mechanisms described in this paper: (1) reducing fraud and leakage in G2P transfer programs, and (2) charging fees for identification services.

In the first mechanism, integrating a unique ID into G2P registers and/or linking various G2P registers together can generate savings by reducing the inclusion of ghosts, duplicates, and ineligible beneficiaries. At the same time, the process of rationalizing a G2P database may erroneously remove real and eligible beneficiaries. This may occur, for example, if a cash transfer register or other database is seeded with a unique ID that does not have truly universal coverage. If individuals who cannot provide a unique ID are declared "ghosts" and removed, this will include some true ghosts as well as real people who have not yet enrolled in the identification system, as discussed above in the Guide for Practitioners.

Individuals may also be excluded from identification systems that rely on biometrics for unique or authentication if they are unable to provide fingerprints or iris scans, and no contingency mechanisms exist. The same is true for digital authentication; as processes become stronger at detecting impersonators, the risk of false rejections increases. Fingerprint identification and authentication failures tend to be highest among certain groups such as children, the elderly, manual laborers, and disabled individuals. This means that those at highest risk for exclusion by increasing the robustness of identification systems are also likely

75 See http://www.worldbank.org/en/programs/id4d website for forthcoming work on costing for identification systems.

to be among society's most vulnerable. Finally, it is also possible that requiring individuals to reenroll in the new system or attempting new methods of authentication may be difficult or undesirable for some individuals, who may simply exit the identification system altogether. Thus, while robust systems can deter attempts at fraud, they can also deter legitimate users.

Table 8: Exclusion Errors vs. Fraud Detection

Truth	Enrollment/Authentication: Accepted	Enrollment/Authentication: Removed/rejected	Enrollment/Authentication: Doesn't attempt
Eligible	A **Inclusion** (true positive)	B **Exclusion** (false negative/rejection)	C **Exclusion** (deterred)
Ineligible	D **Inclusion error** (false positive/acceptance)	E **Fraud prevented** (true negative)	F **Fraud prevented** (deterred)

Similarly, the mechanism of charging for identity-related services—e.g., verification and authentication of identities, issuing and renewing credentials, etc.—provides a revenue-generating opportunity that can underwrite the expenses of identification agencies but also risks exclusion. As discussed above, if fees for services to individuals are set too high, this may undermine access for poor people. Similarly, exorbitant fees charged to third parties may be passed along to consumers, raising the barrier to access basic services. In each of these cases, there is a tradeoff between cost savings and exclusion. Although cost-saving features may be attractive, identity providers must take care to ensure universal coverage and access to identification, the first of ten *Principles on Identification for Sustainable Development.*[76]

Privacy and Fair Use

In addition to the risk of exclusion, certain identification system features and savings mechanisms—particularly integration and interoperability between databases—have important implications for data protection and privacy. Of the many models countries can use to streamline their identity ecosystems, some that offer the highest potential gains in efficiency (e.g., creating a single data warehouse) may also pose the highest risks to privacy and security. No matter the design, identification systems should adhere to the *Principles on Identification* by protecting user privacy, control, and data security through system design (Principle 6) and a comprehensive legal framework (Principle 8).

Although integrating or interoperating multiple databases can help identify ineligible G2P recipients and reduce administrative costs, it must be done in a way that upholds these principles. This should include following the principle of proportionality and minimal disclosure of data sharing to ensure that government agencies and third parties have access only to the minimal amount of information necessary for reconciling or verifying identity records across databases. Interoperability and integration should be underpinned by legal frameworks and procedures (e.g., MOUs) that clearly specify who has access to different databases and attributes and under what conditions, are subject to user control (e.g., allowing users to see who has access their records), and include sufficient security measures (e.g., encryption) to ensure data protection.

76 See http://www.worldbank.org/en/programs/id4d.

At the same time, it is important to recognize that some models of integration and interoperability may also be *privacy enhancing.* Estonia's legal framework, for example, prevents identity providers from collecting data that are already maintained by a register connected to the X-Road, minimizing the number of times that individuals are asked to provide duplicate personal information. In addition, the eID system allows users oversight and control over who has access to their data. Adopting systems and institutions that generate fiscal benefits while promoting—rather than detracting from—individual privacy and data protection is therefore possible, but requires careful thought and intention.

Vested interests

Although governments at large may benefit from savings and revenue generated by robust and inclusive identification, the source of these benefits may go against the vested interests of certain actors. This includes those officials, service providers, intermediaries, and private individuals who currently benefit from weak or inefficient identification systems that offer opportunities for corruption and fraud. To the extent that they are able, these groups may actively work against reforms to identification systems precisely because of the potential to generate savings at their expense.

In Ghana and Nigeria, for example, civil servants have resisted the rollout of biometric-enabled payment systems for payroll management (Gelb and Diofasi Metz 2018). In Pakistan, a number of NADRA projects—including identifying tax evaders, rooting out fraud in pension and payroll systems, and finding proxy prisoners—were thwarted due to vested interests. In addition, after the agency began to assist election tribunals to investigate potential voter fraud during the 2013 elections, NADRA's then-Chairman began to receive threats against his family, eventually prompting him to resign his post and leave the country (Malik 2014).

In some cases, however, incentives can be altered to induce compliance with cost-saving systems. In the Krishna district of Andhra Pradesh State in India, for example, the government incentivized Aadhaar take-up among service providers using both rewards and punishments. To begin, it revoked the licenses of FPS dealers who refused to comply with the requirements of the Aadhaar-enabled payment system for the PDS, appointing new dealers in their place. In addition, it increased the fees that FPS dealers received per commodity sold and gave an additional 17 percent increase for adopting the e-POS system (World Bank 2018a). In Argentina, the government addressed the initial reluctance of certain agencies to share their data with the SINTyS system by financing database improvements for these institutions to ease the cost of integration, in addition to developing a legal framework with clear regulations and responsibilities (Pessino and Fenochietto 2007). Creating these incentives, however, also requires investments that may reduce overall savings.

5. Conclusion

This paper provides a theoretical framework for assessing potential fiscal benefits from identification systems and presents early evidence that savings and revenue generation are, indeed, possible. Where countries adopt identification systems with particular features—including digitized databases and credentials, unique identifiers, interoperability or integration, and digital authentication—these can be used to reduce fraud and leakages in transfer programs, improve efficiency across the identity ecosystem, increase tax collection, and generate revenue by providing identity-related services. They can also have indirect benefits by providing platforms for digital payments and e-Government services, increasing convenience and inclusion for individuals, and generating savings and revenue in the private sector, in addition to creating other difficult-to-measure sources of savings for the government. As a result, identification systems can have large positive impacts on the economy as a whole.

The full extent of these benefits, however, remains difficult to quantify. As such, this paper has highlighted the need for more data and research to develop a reliable model of expected return on investment for identification systems. We encourage country practitioners, donors, and researchers engaged in the development and analysis of such systems to give more consideration to the measurement of ID-related fiscal savings and revenue, and to make these figures public whenever possible. Where feasible, studies to estimate the causal impact of identification systems on government finances through controlled or natural experiments would also help overcome many of the difficulties in attributing changes in expenditure and revenue to various features of identification systems.

Even without such estimates, however, it is clear that savings and revenue sources may not be cheap, automatic, or fast. To create these opportunities, identification systems must be sufficiently robust, have high levels of coverage, and be designed with the goal of maximizing efficiency. This requires overall up-front investment in identification infrastructure, and costs associated with adapting systems to enable savings and revenue generating mechanisms. Furthermore, the scope of potential benefits depends on the particular circumstances of a given country. Strong identification systems can only reduce ghosts and impersonators in G2P transfers or decrease tax evasion to the extent that these issues are prevalent. In addition, savings via certain mechanisms—such as efficiencies gained by digital authentication—will not be realized until there is sufficient demand for online and remote services and Internet connectivity is widespread. Vested interests must be also addressed to minimize resistance to identity-related reforms.

These constraints should be taken into account when conducting a complete analysis of the costs and benefits of identification systems. Furthermore, practitioners must carefully weigh the potential fiscal impacts of certain features and mechanisms—particularly integration and interoperability, efforts to identify fraud and leakage, and fee-charging models—against risks to privacy and exclusion. While some of the benefits of identification may be fiscal, many are not. In the end, identification should be a public good, provided to facilitate the rights and inclusion of individuals and to improve administration and service delivery. Through thoughtful design, however, countries should be able to achieve these goals while maximizing long-term fiscal sustainability.

References

Abraham, R., E. Bennett, N. Sen, and N. B. Shah. 2017. "State of Aadhaar Report, 2016–17." IDinsight. http://stateofaadhaar.in/.

ADB. 2016. "Identity for Development in Asia and the Pacific." Mandaluyong City, Philippines: Asian Development Bank.

Angel-Urdinola, D., F. El-Kadiri, and M. Pillares-Millares. 2014. "Morocco: World Bank Operational Study No. 23817." Washington, DC: World Bank.

Atick, J. 2016a. "Digital Identity: The Essential Guide." ID4Africa Identity Forum.

Atick, J. 2016b. "The Identity Ecosystem of Rwanda." ID4Africa Case Study. http://www.id4africa.com/prev/img/ID4Africa2016_The_Identity_Ecosystem_of_Rwanda_eBooklet.pdf.

Barnwal, Prabhat. 2016. "Curbing Leakage in Public Programs with Direct Benefit Transfers: Evidence from India's Fuel Subsidies and Black Markets." Working Paper, April 11, 2016. http://pubdocs.worldbank.org/en/826341466181741330/Barnwal-DBT-India.pdf.

BBC. 2010. "Millions of Pakistan Children at Risk of Flood Diseases." BBC News Online. 2010. http://www.bbc.com/news/world-south-asia-10984477.

Boston Consulting Group. 2012. "The Value of Our Digital Identity." Liberty Publishing.

BusinessLine. 2016. "Use of Aadhaar for KYC Authentication Will Cut Costs." *The Hindu Online,* April 18, 2016. http://www.thehindubusinessline.com/money-and-banking/use-of-aadhaar-for-kyc-authentication-will-cut-costs/article8490492.ece.

CAG. 2016. "Report of the Comptroller and Auditor General of India on Implementation of PAHAL (DBTL) Scheme." Comptroller and Auditor General of India.

Cavallo, E., and T. Serebrisky, eds. 2016. *Saving for Development: How Latin America and the Caribbean Can Save More and Better.* Washington, DC: Inter-American Development Bank.

Clarke, Kieran. 2016. "More Ghost Savings: Understanding the Fiscal Impact of India's Direct Transfer Program—Update." Policy Brief. International Institute for Sustainable Development. http://www.iisd.org/sites/default/files/publications/more-ghost-savings-india-direct-transfer-program-policy-brief.pdf.

Dahan, Mariana, and Alan Gelb. 2015. "The Role of Identification in the Post-2015 Development Agenda." Working Paper. Washington, DC: World Bank.

DBT Mission. 2018. "Estimated Gains Due to Better Targeting."

DFID. 2009. "Designing and Implementing Financially Inclusive Payment Arrangements for Social Transfer Programmes." UK Department for International Development. http://www.microfinancegateway.org/sites/default/files/mfg-en-toolkit-designing-and-implementing-financially-inclusive-payment-arrangements-for-social-transfer-programmes-dec-2009.pdf.

Dhoot, V. 2017. "What Is the Lowdown on Linking of Aadhaar-PAN for Taxes?" The Hindu Online, June 17, 2017. http://www.thehindu.com/news/national/aadhaar-pan-linkage-what-is-the-lowdown-for-taxes/article19094848.ece.

e-Governance Academy. 2016. "E-Estonia: E-Governance in Practice." e-Governance Academy Foundation. http://www.ega.ee/publication/e-estonia-e-governance-in-practice/.

ET. 2017. "Aadhaar Can Reduce Digital Transaction Cost to Almost Nil: NITI Aayog." *The Economic Times Online,* September 13, 2017. https://economictimes.indiatimes.com/news/economy/policy/aadhaar-can-reduce-digital-transaction-cost-to-almost-nil-niti-aayog/articleshow/60499215.cms.

European Commission. 2016. "Analysis of the Value of New Generation of E-Government Services and How Can the Public Sector Become an Agent of Innovation through ICT." FINAL REPORT: A study prepared for the European Commission DG Communications Networks, Content & Technology. European Commission.

Evrensel, Astrid. 2010. *Voter Registration in Africa: A Comparative Analysis.* Electoral Institute for the Sustainability of Democracy in Africa (EISA).

Falak, A. 2017. "Aadhaar-PAN Link May Help Curb Tax Evasion." *Sunday Guardian Live,* June 25, 2017. http://www.sundayguardianlive.com/news/9905-aadhaar-pan-link-may-help-curb-tax-evasion.

Gabrijel, Tadej. 2013. "Interoperability Components for Electronic Data Gathering: Implementation for e-Social Security." Presentation to United Nations Public Service Forum, Workshop 1, Bahrain, May 26.

Gelb, Alan, and Julia Clark. 2013a. "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development.

———. 2013b. "Performance Lessons from India's Universal Identification Program." CGD Policy Paper 020. Washington, DC: Center for Global Development.

Gelb, Alan, and Caroline Decker. 2011. "Cash at Your Fingertips: Biometric Technology for Transfers in Developing and Resource-Rich Countries." CGD Working Paper. Washington, DC: Center for Global Development.

Gelb, Alan, and Ana Diofasi. 2016. "Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment." CGD Working Paper 435. Washington, DC: Center for Global Development.

Gelb, Alan, and Ana Diofasi Metz. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, DC: Center for Global Development.

Government of Peru. 2012. "Guía de Simplificación Administrativa y Determinación de Costos de Procedimientos Administrativos y Servicios Prestados En Exclusividad." Presidencia del Consejo de Ministros, Secretaría de Gestión Pública. http://www.gobernabilidad.org.pe/buen_gobierno/galleries/103884362_052-Guia%20Simplificacion%20y%20Costos%20GN.pdf.

Hakeem, Ali Arshad. 2010. "Citizens Damage Compensation Mechanism: National Database and Registration Authority." Presentation by Ali Arshad Hakeem, NADRA Chairman, Government of Pakistan.

Joon Song, Hee, Kang Minah, Kim Churin, and Kim Yeonsoo. 2016. "Korea: An Integrated System of Civil Registration and Vital Statistics." Knowledge Sharing Program, World Bank and Korea Institute of Public Administration.

Lahoti, Rahul. 2016. "Questioning the 'Phenomenal Success' of Aadhaar-Linked Direct Benefit Transfers for LPG." *Economic & Political Weekly* 51 (52).

Malik, Tariq. 2014. "Technology in the Service of Development: The NADRA Story." CGD Essay. Washington, DC: Center for Global Development.

———. 2016. E-mail correspondence.

———. 2017a. E-mail correspondence.

———. 2017b. Phone conversation.

Masood, Mansoor Ali. 2017. "Evolution of National Targeting System in Pakistan: The Poverty Scorecard." Presentation by Mansoor Ali Masood, Deputy Director (NSER), BISP, January. http://bisp.gov.pk/wp-content/uploads/2017/01/nser/2_presentation_nser.pdf.

Min, Wonki, and Carlo Rossotto. 2012. "Broadband and Job Creation: Policies Promoting Broadband Deployment and Use Will Enable Sustainable ICT-Based Job Creation." World Bank ICT Policy Notes 1. Washington, DC: World Bank.

Ministry of Finance. 2017. E-mail correspondence with Ministry of Finance, Thailand.

———. 2018. "Union Budget 2018–19. Statement of Subsidies and Subsidies Related Schemes." Government of India. http://www.indiabudget.gov.in/ub2018-19/eb/stat7.pdf.

Mittal, Neeraj, Mukherjee, Anit, and Gelb, Alan. 2017. "Fuel Subsidy Reform in Developing Countries: Direct Benefit Transfer of LPG Cooking Gas Subsidy in India." CGD Policy Paper. Washington, DC: Center for Global Development. https://www.cgdev.org/publication/fuel-subsidy-reform-developing-countries-india.

MPS. 2018. "E-mail Correspondence with the Ministry of Public Service, Uganda," March 3, 2018.

Muralidharan, Karthik, Paul Niehaus, and Sandip Sukhtankar. 2016. "Building State Capacity: Evidence from Biometric Smartcards in India." *The American Economic Review* 106 (10): 2895–2929.

Nanda, P. K. 2017. "Aadhaar Linkage: Three States Strike out 272,000 Fake Students," August 26, 2017. http://www.livemint.com/Politics/fAAkrlWoXWYTrQFjdNA6DP/Aadhaar-linkage-Three-states-strike-out-272000-fake-studen.html.

New Indian Express. 2017. "Aadhar-Enabled Biometric Attendance System Serves GHMC Rs 2.86 Crore Each Month," 2017. http://www.newindianexpress.com/cities/hyderabad/2017/jul/16/aadhar-enabled-biometric-attendance-system-serves-ghmc-rs-286-crore-each-month-1629377.html.

News24. 2015. "Tanzania Orders Probe into 'Ghost' Government Workers." *News24 Online,* 2015. http://www.news24.com/Africa/News/Tanzania-orders-probe-into-ghost-government-workers-20150329.

NIPFP. 2012. "A Cost-Benefit Analysis of Aadhaar." New Delhi: National Institute of Public Finance and Policy. http://planningcommission.nic.in/reports/genrep/rep_uid_cba_paper.pdf.

NIST. 2013. "Planning Report 13-2 Economic Case Study: The Impact of NSTIC on the Internal Revenue Service." Washington, DC: National institute of Standards and Technology.

OAG. 2014. "Comprehensive Audit of the Government Payroll, Volume 3: Forensic Investigation into the Suspected Invalid Records in the Government Payroll." Office of the Auditor General of Uganda.

OWI. 2017. "Don't Believe the (Blockchain) Hype: The Definitive Primer on Identity and Blockchain." One World Identity Labs. oneworldidentity.com.

Pessino, Carola, and Ricardo Fenochietto. 2007. "How to Implement a National Coordinated System for the Identification of Individuals and Information Exchange to Improve Fiscal and Social Equity. Lessons from LACs." In *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance, ICEGOV 2007,* edited by Janowski Tomasz and Theresa A. Pardo.

Povoledo, E. 2013. "Italians Have a New Tool to Unearth Tax Cheats." New York Times, 2013. http://www.nytimes.com/2013/01/28/world/europe/italys-new-tool-for-tax-cheats-the-redditometro.html?mcubz=1.

Qiang, C. Z., and C. Rossotto. 2009. "Economic Impacts of Broadband." In *Information and Communications for Development 2009: Extending Reach and Increasing Impact,* 35–50. Washington, DC: World Bank.

RENIEC. 2017a. "Texto Único de Procesos Administrativos/TUPA 2017." Registro Nacional de Identificación.

———. 2017b. "Correspondence with RENIEC, Peru," January 11, 2017.

———. 2018. "Correspondence with RENIEC, Peru," January-March, 2018.

Revenue Department. 2017. Phone Conversation with Revenue Department of Thailand.

Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* Yale University Press.

Subramanian, A., and Siddharth George. 2016. "Clearing the Air on LPG." The Indian Express Online, 2016. http://indianexpress.com/article/opinion/columns/clearing-the-air-on-lpg-direct-benefit-transfer-subsidies/.

Times of India. 2017. "Over 11.44 Lakh PANs Deactivated: Govt." *Times of India Online,* August 2, 2017. http://timesofindia.indiatimes.com/india/over-11-44-lakh-pans-deactivated-says-gangwar/articleshow/59868924.cms.

UK Cabinet Office. 2012. "Digital Efficiency Report: Research and Analysis." Government Digital Service. https://www.gov.uk/government/publications/digital-efficiency-report/digital-efficiency-report#annex-1-list-of-case-studies.

Vassil, Kristjan. 2015. "Estonian E-Government Ecosystem: Foundation, Applications, Outcomes." World Development Report 2016 Background Paper, Digital Dividents. Washington, DC: World Bank.

World Bank. Forthcoming. "South Africa Civil Registration and Identification Good Practice Case." Washington, DC: World Bank Group.

———. 2008. "Project Appraisal Document on a Proposed Loan in the Amount of US$20 Million to the Republic of Argentina for a Social and Fiscal National Identification Project." Washington, DC: World Bank Group.

———. 2014a. "Delivery Systems Assessment—Identification Module: Peru Country Report (Draft Version)." Identification for Development (ID4D) Country Diagnostic. Washington, DC: World Bank.

———. 2014b. "Implementation Completion and Results Report on a Loan in the Amount of US$20 Million to the Republic of Argentina for a Social and Fiscal National Identification System (SINTyS) Project." Washington, DC: World Bank Group.

———. 2015. "Nigeria Country Assessment." Identification for Development (ID4D) Country Diagnostic. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/136541489666581589/pdf/113567-WP-P156810-PUBLIC-1618628-Nigeria-ID4D-Web.pdf.

———. 2016. "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation." Working Paper. Washington, DC: World Bank.

———. 2017a. "Identity Management Cost-Benefit Analysis for Zambia (Draft)." Washington, DC: World Bank.

——. 2017b. “Principles on Identification for Sustainable Development: Toward the Digital Age.” Washington, DC: World Bank. http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf.

——. 2017c. “The State of Identification System in Africa: A Synthesis of Country Assessments.” Washington, DC: World Bank.

——. 2018a. “Aadhaar in Action: The Krishna District Experience.” Identification for Development (ID4D) Case Study. Washington, DC: World Bank.

——. 2018b. “India’s Aadhaar Program: Transformative Unique Digital Identification.” Identification for Development (ID4D) Case Study. Washington, DC: World Bank.

——. 2018c. “Private Sector Economic Impacts from Identification Systems.” Washington, DC: World Bank.

——. 2018d. “Understanding Cost Drivers of Identification Systems.” Washington, DC: World Bank.

Yeboah, O. A. 2016. “E-Zwich Helps Flush Out 35,000 Ghost Names from Payroll . . . Saves Gov’t GH146m.” *The Business & Financial Times Online,* 2016. http://thebftonline.com/business/ict/18576/e-zwich-helps-flush-out-35000-ghost-names-from-payroll-saves-govt-gh146m.html.

Zelazny, F. 2012. “The Evolution of India’s UID Program: Lessons Learned and Implications for Other Developing Countries.” CGD Policy Paper 008. Washington, DC: Center for Global Development.

Appendix: Cases

Mechanism	Case	Description*	Key Factors
1a. Reducing fraud and leakage: Ghosts, duplicates	**India**	The unique Aadhaar number has been seeded into databases and used to authenticate beneficiaries for dozens of social programs, resulting in significant savings—potentially in the billions of dollars—from removing fakes and duplicates.	unique ID digital authentication interoperability/integration
	Pakistan	The NADRA database was used to eliminate duplicates and ineligible beneficiaries for emergency relief (Watan Card and IDPs), saving an estimated US$378 million.	unique ID interoperability/integration
	Uganda	Verifying the identities of civil servants against the national ID database reportedly saved the government US$6.9 million in less than a year by removing some 4,664 ghost workers from the public payroll.	unique ID interoperability/integration
1b. Reducing fraud and leakage: Ineligible	**Argentina**	Using its SINTyS system to link databases at the federal, provincial, and local levels, the government identified inclusion errors in its pension and social program databases, saving at least US$300 since implementation, or nearly eight times the cost of its World Bank financing.	unique ID interoperability/integration
	Thailand	The national ID number was used in a cash transfer program for the poor to cross-check the eligibility of beneficiaries against tax, occupational, and other databases, saving between US$29.7–59.4 million.	unique ID interoperability/integration
	Pakistan	The NADRA database was used to eliminate ineligible beneficiaries for the initial targeting of the BISP cash transfer program and the government's Zakat program, saving an estimated US$52.9 million.	unique ID
1c. Reducing fraud and leakage: Impersonation	**India**	Biometric authentication using a functional smart card in the State of Andhra Pradesh reduced leakage in NREGA benefits by approximately 12.7 percentage points, and in pension benefits (SSP) by approximately 2.8 percentage points.	digitization digital authentication
2a. Reducing administrative costs: Transactions	**Slovenia**	An interoperability platform to verify identity information for safety nets across 50+ databases has saved the Ministry of Social Affairs approximately US$14.5 million per year.	digitization interoperability/integration
	United States	Projections estimate that a secure, digital identity credential would save the IRS between US$91–318 million per year by reducing authentication costs and facilitating online services.	digitization digital authentication

Mechanism	Case	Description*	Key Factors
	Estonia	The eID and X-Road systems—which provide digital authentication and signatures, and facilitate data exchange—save an estimated 2 percent of GDP per year by reducing identity-related transaction costs and facilitating online services.	digitization unique ID interoperability/integration digital authentication
2b. Reducing administrative costs: Redundancy	**South Africa**	Integration between the national ID and voter registration contributed to some of the falling costs of elections (from US$250 million in 1994 to US$32 million in 2009).	unique ID interoperability/integration
	Malawi	Integration between the national ID and voter registration eliminated the need for a separate voter ID card, saving approximately US$44 million ahead of the 2019 elections.	unique ID interoperability/integration
3. Increasing tax collection	**Argentina**	Integration between tax databases and other registers (e.g., property and vehicles) via the SINTyS system improved tax audits, generating approximately US$44 million in additional revenue from a reduction in tax fraud.	unique ID interoperability/integration
	Pakistan	NADRA's cross-checks of taxpayers against a variety of databases identified some 3.6 million potential taxpayers who were not filing taxes; had this information been used to increase payments by these individuals, it could have saved an estimated US$1 billion within a few months.	unique ID interoperability/integration
	India	The government will require Aadhaar numbers when filing taxes in order to weed out duplicate or fake tax ID numbers (PANs), commonly used for money laundering and tax evasion.	unique ID interoperability/integration
4. Charging fees	**Peru**	RENIEC has earned approximately US$45 million in revenue annually by charging fees for verification and other services, while ensuring that services remain free for the poor.	unique ID interoperability/integration digital authentication
	Pakistan	NADRA charges both public and private sector users to verify identities against its database; for example, it earns approximately US$9.3 million per year from verifying the identity of BISP beneficiaries.	unique ID interoperability/integration digital authentication

* Note: All savings figures should be taken as approximations; see full descriptions in text for data sources, limitations, and caveats.

worldbank.org/id4d

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP