SEMI-SECURE NUMBERS? AUGMENTING SSNS IN THE AUTHENTICATION USE CASE

Kathryn E. Witchger, Kevin Chen, Jon Song, Alex Wortman, Joshua M. Zweig†

Abstract

Identity theft costs Americans more than $15 billion per year. Central to this problem is that Social Security Numbers (SSNs) serve a dual role as identifiers and authenticators. As unique identifiers, SSNs are used to retrieve an individual's records, such as a credit report. In this role, they are not meant to be secret. As authenticators, an SSN is used to prove identity. In this role, SSNs must be secret to be secure. This Article proposes a way to resolve the dual-purpose tension by layering smart cards on top of existing SSN-based processes in a way that is reconcilable with legal and political considerations. The card-based digital signatures act as a second factor of authentication to increase the security of processes in which SSNs act as authenticators, while not limiting or replacing the use of SSNs as identifiers. This leaves the tremendous economic value of SSNs as identifiers unabridged. Part I is an overview of the SSN system while Part II is a description of the dual-purpose problem. Part III describes the technical details of the smart card solution. Part IV proposes policy recommendations to foster the deployment and wide adoption of this system for the benefit of the American people.

TABLE OF CONTENTS

† The authors would like to thank Elizabeth Brasher, and Professors Steven Bellovin, Jason Healey and Matthew Waxman for their significant contributions to this paper. The authors would also like to thank John Grant for his comments and discussion. All authors should be regarded as joint authors.

INTRODUCTION

The Social Security Number (SSN) is an important method by which the government identifies citizens and the private sector identifies customers.[1] It

1. FED. TRADE COMM'N, STAFF SUMMARY OF COMMENTS AND INFORMATION RECEIVED REGARDING THE PRIVATE SECTOR'S USE OF SOCIAL SECURITY NUMBERS, 4–13 (2007) [hereinafter FTC STAFF SUMMARY], https://www.law.berkeley.edu/files/staffsummary.pdf.

has come a long way from its original, sole purpose of tracking individuals to distribute Social Security benefits.[2] The SSN has also taken on wide use as an authenticator, a secret whose knowledge allows an individual to prove their identity.[3] Since at least 2007, it has been well known that SSN's simultaneous use as both an identifier and authenticator is riddled with flaws, making Americans incredibly vulnerable to identity theft.[4] Since 2008, the Federal Trade Commission (FTC) has recommended the adoption of stronger authentication practices beyond simply relying on SSNs.[5]

There have been some attempts: certain systems require a driver's license number or presentation of the license as an additional factor of authentication.[6] However, no attempts have been effective.[7] This is evidenced by the stark increase in identity theft (both in number of victims and dollars lost) over the same period since 2008.[8] In 2016, it was reported that the number of identity theft victims in the U.S. hit an all-time high.[9] Since the first public recognition of the problem of using SSNs as authenticators, Americans have lost over $100 billion to identity theft, not including the cost of emotional distress and economic recovery that follow, which are much more difficult to quantify.[10] Previous attempts to resolve this issue either mistakenly rely on the inclusion of other identifiers (e.g. passport number or date of birth) or easily forgeable documents (e.g. drivers licenses).[11] These attempts fail to grasp the true root of the problem: Americans need a dedicated form of authentication to protect against identity theft.

The SSN is widely accepted as a *necessary* condition for identity theft.[12] This Article proposes a solution to the issue by developing a unique way to leverage digital signatures while maintaining compatibility with the legacy of the political, technical, and legal mire of the current SSN system. Upon attempting to use an SSN, individuals also use the system to prove that that SSN

2. *Id.* at 4.
3. *Id.* at 14–15.
4. *Id.* at 3.
5. FED. TRADE COMM'N, SECURITY IN NUMBERS ***–**–**** SSNS AND ID THEFT 2 (2008) [hereinafter SECURITY IN NUMBERS], https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.
6. FTC STAFF SUMMARY, *supra* note 2, at 7.
7. *Id.* at 8.
8. Press Release, Javelin, Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study (Feb. 1, 2017) [hereinafter Javelin], https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.
9. *See generally* AL PASCUAL, KYLE MARCHINI, & SARAH MILLER, 2017 IDENTITY FRAUD: SECURING THE CONNECTED LIFE (2017) [hereinafter PASCUAL] ("2016 will be remembered as a banner year for fraudsters as numerous measures of identity fraud reached new heights. The overall fraud incidence rose 16% to affect 6.15% of U.S. consumers, from 5.30% in 2015—the highest on record.").
10. *See* Javelin, *supra* note 9 (showing that the total sum of Fraud Losses according to *2017 Identity Fraud Study* exceeds $100 billion).
11. NAT'L RESEARCH COUNCIL, WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY 13 (Stephen T. Kent & Lunette I. Millett eds., 2003) [hereinafter NAT'L RESEARCH COUNCIL].
12. FTC STAFF SUMMARY, *supra* note 2, at 8.

is, in fact, their own. The novel design presented in this Article permits individuals, businesses, and the government to enjoy improved security without implementing radical changes to their existing workflows and business processes.

The authentication scheme gives each SSN holder a cryptographic certificate in addition to the SSN itself. The certificate will be distributed at birth by the SSA in tandem with the traditional Social Security card. The certificate will be stored in a smart card, similar to cards currently deployed in Germany and Estonia, allowing individuals claiming an SSN to cryptographically sign the document on which they claim an SSN. Upon verifying that a document's cryptographic signature matches the SSN being used, institutions can be sure that the claimant is who they say they are. In this way, authentication would include both *something you know* (SSN) and *something you have* (the smart card).[13] The system also provides a way for individuals to extend the trust of the card to the trust of an individual's phone.

This Article includes technical, legal, and policy analyses and recommendations to align incentives and introduce this system in both a public and private sector context. It does so while maintaining the key property that the identification use of the SSN will remain unencumbered, while improving the security of the SSN when used as an authenticator. The Article is organized into four parts. Part I details the background and legal history of the SSN system. Part II describes why the SSN system needs to be reformed. Part III details the technical solution. To showcase how the card would function in everyday situations, this Section also contains examples of how to utilize the card when applying for a loan and e-filing tax returns. Part IV describes how the proposed authentication method could be implemented in the general population starting with pilot programs involving federal student aid and government employees and discusses potential political and legal barriers.

I. THE SSN SYSTEM AND THE ISSUE OF ENTANGLEMENT

The SSN has existed for over 90 years, taking on a unique and important place in both the public and private sector.[14] The unique legal and political context of the U.S., and this Article's goal of an efficient fix to the problem of SSN theft, precludes a national ID/E-card system solution, such as the systems deployed in Estonia and Germany.[15] In moving toward a solution that acknowledges the complexity of our present situation, this Part will describe the use of the SSN and demonstrate the ways in which it has become entangled in the law and integral in the administration of many federal programs. It will also describe the important role the SSN has taken on in the private sector, especially

13. Technically, this is not two-factor authentication. SSNs are widely known, so the status quo of authenticating using only an SSN can be thought of as "zero-factor" authentication. This motivates the addition of another factor.

14. FTC STAFF SUMMARY, *supra* note 2, at 4.

15. *See infra* Section III.G (providing Comparisons and Alternative Solutions).

in the financial sector. Lastly, this Part will describe the recent damage caused by SSN-based identity theft.

A. History of the Social Security Number

In 1936, the Social Security Board created the SSN[16] to uniquely identify U.S. workers for the purposes of tracking their earnings history and administering Social Security entitlements.[17] Since this humble beginning, the Social Security Administration (SSA) has issued SSNs to both U.S. citizens and aliens under § 205(c)(2) of the Social Security Act,[18] and has issued over 450 million original SSNs as of 2008.[19] The SSN is a nine-digit number that, until recently, was comprised of a four-digit serial number, a two-digit year of birth indicator, and a three-digit number indicating the geographic area of registration;[20] however, the SSA in 2011 randomized the issuance of SSNs to extend the longevity of the nine-digit number across all geographic areas.[21]

1. SSN Use Required by the U.S. Government

The SSN is used widely by the government.[22] This Section will sort the current government uses into two categories: use for benefits, and use for tracking, both internally and externally. Because of its utility as a unique identifier for citizens, SSN use has expanded dramatically since 1936.[23] According to the SSA:

> "the simplicity and efficiency of using a unique number that most people already possess has encouraged widespread use of the SSN by both government agencies and private enterprises, especially as they have adapted their recordkeeping and business systems to automated

16. The Social Security Board preceded today's Social Security Administration (SSA). Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SEC. BULL. 55, 56 (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

17. *See, e.g.*, Puckett, *supra* note 17, at 55–56 (explaining that a number of alternatives to the Social Security Number (SSN) were considered. For instance, though other government agencies such as the Veterans Administration and Post Office Department used fingerprints as a means of identification, the Social Security Board declined to do so since "the use of fingerprints was associated in the public mind with criminal activity…").

18. 42 U.S.C. § 405(c)(2) (requiring that the Commissioner of Social Security "take affirmative measures" to assure the issuance of SSNs to, among others: aliens at the time of their lawful admission to the United States for permanent residence or under other authority of law permitting employment in the United States; and any individual who is an applicant for or recipient of benefits under any program financed in whole or in part from Federal funds).

19. Puckett, *supra* note 17, at 55.

20. *Id.* at 56.

21. *See Social Security Number Randomization*, SOC. SEC. ADMIN., https://www.ssa.gov/employer/randomization.html (stating that there are approximately 420 million numbers available for assignment) (last visited Jan. 28, 2019).

22. FTC STAFF SUMMARY, *supra* note 2, at 4–8.

23. The laws discussed in this Section are not comprehensive, but rather meant to be illustrative of the variety of purposes for which the U.S. government utilizes SSNs today. *See generally* Carolyn Puckett, *supra* note 17 (discussing the history of SSN use).

> data processing. Use of the SSN as a convenient means of identifying people in large systems of records has increased over the years and its expanded use appears to be an enduring trend."[24]

True to the SSN system's roots in public benefits, individuals are widely required to provide their SSN to receive federal, state, and local government benefits, loans and privileges.[25] The Social Security Act also mandates that states require applicants of the following programs to furnish their SSN: Medicaid, Unemployment Compensation, Temporary Assistance for Needy Families, Adult Assistance programs under the Social Security Act,[26] and the Food Stamp Program under the Food and Nutrition Act of 2008.[27] Further, applicants for loans under any federal loan program are required to furnish their SSN to the agency supplying the loan.[28] This includes student loan applicants.[29] Finally, the Social Security Act also requires individuals to provide their SSNs for certain privileges.[30] Any application for licenses, divorce decrees, support orders, paternity determinations, and death certificates requires an SSN.[31]

The government also requires SSN for internal and external tracking purposes[32] as federal law requires the SSA to disclose a person's SSN to other government agencies.[33] For example, the SSA must provide SSNs to the Office of Personnel Management to administer federal employee civil service

---

24. Carolyn Puckett, *supra* note 17, at 67.

25. For instance, 42 U.S.C. § 405(c)(2)(C)(i) authorizes a state or state agency to require SSNs to administer any tax, general public assistance, or motor vehicle registration. Social Security Act, 42 U.S.C. § 405(c)(2)(C)(i) (2018).

26. 42 U.S.C. 1320b-7 (showing that programs include old-age assistance, aid to the blind, aid to the permanently and totally disabled, and supplemental security income for the aged, blind and disabled. 42 U.S.C. §§ 30c–06, 1201–06, 1351–55, 1381–81a).

27. 42 U.S.C. § 1320b-7 (stating that federal law also requires the SSN of a parent or guardian to be provided to the Secretary of State for a child to be eligible for a free or reduced-price school lunch under 42 U.S.C. § 1758(d), and every member of a household to supply his or her SSN to the Secretary of State to be eligible for the food stamp program under 7 U.S.C. § 2025(e). 7 U.S.C. § 2025(e); 42 U.S.C. § 1758(d)).

28. Debt Collection Act, 5 U.S.C. § 5514 (2018).

29. Higher Education Amendments of 1986, 20 U.S.C. § 1001 (2018). Additionally, the National Student Loan Data System is required to collect borrower SSNs under the Omnibus Budget Reconciliation Act of 1989, 20 U.S.C. § 1092(b)(2)(A) (2018).

30. 42 U.S.C. § 666(a)(13); 42 U.S.C. §§ 405(c)(2)(B)(ii), (C)(ii).

31. These licenses include professional, driver's, occupational, recreational, or marriage licenses. 42 U.S.C. § 666(a)(13)(A). Further, the Real ID Act of 2005 also mandates that states require SSNs when issuing a driver's license, and parents are required to provide their SSNs for the issuance of an SSN or birth certificate for a child below the age of eighteen, unless good cause is shown not to. 42 U.S.C. §§ 405(c)(2)(B)(ii), (C)(ii).

32. *Id.*

33. The SSA is not required to obtain the individual's consent prior to disclosure. For the complete list of purposes for which the SSA is required to disclose SSNs to other governmental agencies without consent, see *GN 03325.002 Disclosure of Social Security Numbers (SSN) Without Consent*, SOC. SEC. ADMIN., https://secure.ssa.gov/poms.nsf/lnx/0203325002 (last visited Feb. 25, 2019). Moreover, the Privacy Act of 1974, 5 U.S.C. § 552(a)(b), discussed *infra*, contains twelve exceptions that allow federal agencies to disclose SSNs without written consent. 5 U.S.C. § 552(a)–(b) (2018). These exceptions include a routine use exception that allows Federal agencies to disclose SSNs to third parties for purposes compatible with the purpose for which the information is collected, as well as a law enforcement exception that applies to civil and criminal law enforcement activity. Additional exceptions include the following: provision to the SSA on a need-to-know basis, when required under FOIA, research and statistical purposes, health and safety purposes, and pursuant to a court order. *Id.*

programs;[34] to the Department of Veterans Affairs for purposes of determining eligibility for VA benefits;[35] to the Department of Homeland Security for aliens assigned SSNs for non-work purposes who have earnings posted to those SSNs;[36] and for those required to register with the Selective Service System.[37] On the external side, the Internal Revenue Service (IRS) requires individuals to provide their SSN for federal tax reporting purposes,[38] and the Department of Treasury requires individuals to provide their SSN to buy certain U.S. savings bonds.[39] The SSN is ubiquitous and entangled in almost every aspect of government.

2. SSNs, Private Entities, and Private Use Generally

For the same reasons of efficiency and ease, SSNs have become widely used in the private sector, particularly among financial institutions, insurers, credit reporting agencies, and health care entities.[40] There are a limited number of instances where the law compels individuals to provide their SSNs to such institutions.[41] Even when SSN disclosure is not required, individuals are motivated to provide their SSNs to receive the best possible service. For example, the SSN is used in the financial sector for money laundering prevention. Specifically, the U.S. Department of Treasury and the IRS require a private entity to collect an individual's SSN if the individual is involved in a financial transaction exceeding $10,000,[42] or the individual engages in a financial transaction subject to the federal Customer Identification Program (CIP) Rule.[43] These requirements are intended to fight money laundering and

34. 5 U.S.C. § 8347(m)(3) (2018).

35. 38 U.S.C. § 5106 (2018).

36. 8 U.S.C. § 1360(c) (2018).

37. Military Selective Service Act, 50 U.S.C. § 3801 (2018).

38. 26 U.S.C. § 6109(a). This applies to any person required to file a return, statement, or other document with the IRS—not merely those with taxable income. SSNs are also required to be furnished for all interest-bearing accounts. *See* Interest and Dividend Tax Compliance Act of 1983, 26 U.S.C. § 1 (2018) (requiring SSNs for all interest-bearing accounts and providing a penalty of $50 for all individuals who fail to furnish a correct Taxpayer Identification Number, which is usually the SSN) (requiring Series H savings bond buyers and Series E savings bond buyers to provide their SSNs).

39. *See Social Security Number Chronology*, SOC. SEC. ADMIN., https://www.ssa.gov/history/ssn/ssnchron.html (last visited Feb. 5, 2019) (requiring Series H savings bond buyers and Series E savings bond buyers to provide their SSNs).

40. 26 U.S.C. § 6055 (2018); *see, e.g.*, *Questions and Answers on Information Reporting by Health Coverage Providers (Section 6055)*, INTERNAL REVENUE SERV., https://www.irs.gov/affordable-care-act/questions-and-answers-on-information-reporting-by-health-coverage-providers-section-6055 (providing answers to common questions on information reporting by health coverage providers).

41. 26 U.S.C. § 6055.

42. Under these circumstances, the financial entity is required to file a currency transaction report with the IRS. *See* Bank Secrecy Act of 1970, 12 U.S.C. § 1951 (2018) (requiring the financial entity to file a currency transaction report with the IRS under these circumstances).

43. Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 31 C.F.R. § 1020.220 (2018); 31 U.S.C. § 5318 (2018) (requiring banks, savings and loan associations, credit unions, and broker-dealers in securities to collect the Taxpayer Identification Number (TIN) of their customers under the CIP Rule, defined as persons who open a new account); *see* Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated

prevent the funding of terrorism.[44] Additionally, the Affordable Care Act (ACA) imposes reporting obligations that require private entities to collect SSNs.[45] Health insurance issuers, certain employers, and others that provide minimum essential coverage to individuals must collect and report those individuals' SSNs to the IRS.[46]

Other uses of the SSN are not required by law but performed voluntarily by the private sector because they provide great utility.[47] For example, creditors use the SSN as an identifier when requesting credit checks from consumer reporting agencies (CRAs).[48] CRAs rely heavily on the SSN to build consumer credit reports.[49] When a creditor requests a credit report for a loan applicant, they provide the CRA with the applicant's SSN to ensure accurate retrieval of their credit report.[50] It is estimated that "if SSNs could not be used to match customer credit information . . . the content of an average consumer file [would be reduced by] 15–20 percent."[51]

In short, private entities widely collect customers' SSNs for purposes outside the scope of these limited legal obligations, largely due to the extent to which SSNs can serve as a universally adopted identifier and thereby enable easy tracking and efficient provision of services.[52] Thus, SSN use is inextricably entangled in the private sector as well.

B. Role of SSNs in Identity Theft

The widespread and valuable usage of SSNs is not without risk.[53] Knowledge of a potential victim's SSN is widely understood to be a necessary, and sometimes sufficient, condition for identity theft.[54] Indeed, the SSN is often viewed as the most valuable piece of information for identity theft.[55] The FTC

Banks, 31 C.F.R. § 103.121(a)(1) & (b)(2) (2018) (showing that the TIN is frequently the customer's SSN); 42 U.S.C. § 405(c)(2)(C)(i).

44. 31 U.S.C. § 5318 (2018).

45. *Information Reporting Requirements under the Affordable Care Act*, RSM: TAX ALERT (Dec. 27, 2017), https://rsmus.com/what-we-do/services/tax/new-information-reporting-requirements-under-the-affordable-care.html.

46. 42 U.S.C. § 1320b-7; 42 U.S.C. § 1758(d); 7 U.S.C. § 2025(e); 7 U.S.C. § 2025(e); 42 U.S.C. § 1758(d); *Questions and Answers About Reporting Social Security Numbers to Your Health Insurance Company*, IRS, https://www.irs.gov/affordable-care-act/questions-and-answers-about-reporting-social-security-numbers-to-your-health-insurance-company (last visited Feb. 25, 2019).

47. FTC STAFF SUMMARY, *supra* note 2 at 21; *Consumer Reports: What Information Furnishers Need to Know*, FED. TRADE COMM'N, [hereinafter *Consumer Reports*] https://www.ftc.gov/tips-advice/business-center/guidance/consumer-reports-what-information-furnishers-need-know (last visited Feb. 25, 2019) (showing uses of SSNs).

48. *Consumer Reports*, *supra* note 48 (discussing the uses of SSNs).

49. *Id*.

50. *Id*.

51. FTC STAFF SUMMARY, *supra* note 2, at 22.

52. *See, e.g.*, SECURITY IN NUMBERS, *supra* note 6, at 3 (describing identifying properties of SSNs).

53. FTC STAFF SUMMARY, *supra* note 2, at 14; *Tax Identity Theft Lower But Still A Problem*, KFMB-TV (Jan. 11, 2019), http://www.cbs8.com/story/39772508/tax-identity-theft-lower-but-still-a-problem.

54. SECURITY IN NUMBERS, *supra* note 6, at 3.

55. FTC STAFF SUMMARY, *supra* note 2, at 8.

has referred to the SSN as "the keys to the kingdom" for identity thieves.[56] Criminals can use SSNs to "facilitate the opening of new accounts, gain access to existing accounts, commit medical identity theft, seek employment, and obtain government benefits."[57] For financial institutions, the SSN is the key data required to assess credit worthiness in the opening of a new account.[58] In many cases, an additional factor of authentication, often a driver's license or birth certificate is required.[59] However, it is well known that such supporting documentation is easily counterfeited and insufficient for authentication purposes.[60]

Even if such authentication schemes were sufficient, there are other identity theft attacks that the population would be vulnerable to, the most well-known being *synthetic identity theft.*[61] In synthetic identity theft, an attacker will use a valid SSN, often that of a child victim, coupled with another victim's name and identifying information to open accounts.[62] Such attacks have been well known for at least ten years, but persist to this day.[63]

Given the extensive risk that SSNs pose, it is unsurprising that U.S. law imposes restrictions designed to protect the privacy and security of SSNs.[64] These restrictions range from disclosure obligations for SSN use to data security obligations.[65] For instance, the Privacy Act of 1974 states that "[a]n individual shall not be denied any right, benefit, or privilege provided by law . . . because of such individual's refusal to disclose his social security number."[66] However, the Privacy Act exempts from this rule any disclosure required by a federal statute.[67] The Privacy Act also requires any entity requesting an individual to disclose his Social Security number to inform that individual (1) whether disclosure is mandatory or voluntary; (2) what authority authorizes the solicitation; and (3) what uses will be made of the solicitation.[68] Additional

56. SECURITY IN NUMBERS, *supra* note 6, at 2.

57. *Id.* at 3.

58. FTC STAFF SUMMARY, *supra* note 2 at 14.

59. *Id.* at 27.

60. FTC STAFF SUMMARY, *supra* note 2, at 4; SECURITY IN NUMBERS; *supra* note 6, at 17 n. 45 (describing the impact of counterfeiting on authentication); NAT'L RES. COUN., *supra* note 12, at 13.

61. FTC STAFF SUMMARY, *supra* note 2, at 16; Bev O'Shea, *What is Synthetic Identity Theft?*, NERDWALLET (Apr. 27, 2018), https://www.nerdwallet.com/blog/finance/synthetic-identity-theft.

62. FTC STAFF SUMMARY, *supra* note 2, at 16.

63. FTC STAFF SUMMARY, *supra* note 2, at 16; *see also* Leticia Miranda, *A Dad Stole This Toddler's Identity To Open Credit Cards. Here's How The System Failed Him*, BUZZFEED NEWS (Feb. 1, 2018, 6:05 PM), https://www.buzzfeed.com/ leticiamiranda/what-happens-when-your-parent-steals-your-identity (illustrating possible effects of identity theft).

64. *See* Use and Disclosure of Social Security Numbers, 31 C.F.R. § 1.32(a) (2018) (showing how individuals are protected from being compelled to disclose their SSNs).

65. *Id.*

66. *Id.*

67. 31 C.F.R. § 1.32(b)(1) (2018).

68. 31 C.F.R. § 1.32(c) (2018). The SSN Protection Act of 2010 also limits the use of SSNs by government agencies. *See* Social Security Act, 42 U.S.C. § 405(c)(2)(C) (2018) (prohibiting federal, state, and local agencies from displaying an SSN or part of an SSN on any check issued for payment by that agency and prohibiting them from entering into a contract to use prisoners in any capacity allowing them to have access to SSNs).

restrictions include several industry-specific federal laws[69] and a large number of state laws[70] imposed on both public and private entities' collection, use, and disclosure of SSNs.

Despite these legal protections, SSNs remain easy to obtain.[71] They appear in public documents such as court filings, tax lien records, property records, death certificates, and even missing persons reports.[72] Additionally, the widespread leakage of SSNs by the private sector has increased the ease with which one can learn a potential victim's SSN.[73] Numerous private companies maintain databases of SSNs, names, and other information about consumers, posing an enormous risk.[74] The latest example is the Equifax data breach, in which 143 million records were stolen.[75] Breaches like this drive down the price of SSNs in illegal markets: in 2016, they cost just $1 each.[76] As the "keys to the kingdom,"[77] the low price of an SSN is not tied to the value of SSN-based identity theft, but to the vast number of SSNs available.

69. Several industry-specific privacy laws restrict the use and disclosure of SSNs, among other personal information. These laws include the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transaction Act (FACTA), which govern consumer report and background screening information, the Gramm-Leach-Bliley Act (GBLA), which governs financial information, the Driver's Privacy Protection Act (DPPA), which governs information collected by the Departments of Motor Vehicles, and the Health Insurance Portability and Accountability Act (HIPAA), which governs health information. Fair Credit Reporting Act, 15 U.S.C. §1681 (2018); Fair and Accurate Credit Transactions Act, 15 U.S.C. §1601 (2018); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2018); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2018); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 210 (2018).

70. At the state level, as of 2008, more than thirty states had adopted laws limiting how SSNs can be collected, used, and disclosed. Six of those states had provisions specifically requiring organizations to safeguard SSNs; these states include: Connecticut, Massachusetts, Michigan, New Mexico, New York, and Texas. In any of these six states, a business must first implement and maintain internal policies and procedures to protect SSNs, and specifically maintain an SSN Protection Policy that (1) protects the confidentiality and security of SSNs, (2) prohibits the unlawful disclosure of SSNs, (3) limits access to SSNs, (4) documents when employees can keep, access, and transport SSNs outside of business premises, (5) provide for the proper disposal of SSNs, and (6) provide penalties for violations of the SSN protection policy. *See* Ct. H.B. 5658; 201 Mass. Code Regs. §§ 17.01–17.04; Mich. Comp. Laws § 445.85; N.M. Stat. §§ 57-12B-2–57-12B-3; N.Y. Gen. Bus. Law § 3990dd(4); Tex. Bus. & Com. Code §§ 501.051–501.053. *See also* Miriam H. Wugmeister & Nathan D. Taylor, *Six States Now Require Social Security Number Protection Policies*, MORRISON FOERSTER (Dec. 9, 2008), https://www.mofo.com/resources/publications/six-states-now-require-social-security-number-protection-policies.html (providing an overview of the laws restricting SSNs in these six states).

71. Herb Weisbaum, *Hackers Scored More Social Security Numbers Than Stolen Credit Card Numbers in 2017*, NBC NEWS (Feb. 21, 2018), https://www.nbcnews.com/tech/security/smarter-criminals-find-new-ways-commit-cyber-fraud-n849691.

72. FTC STAFF SUMMARY, *supra* note 2, at 9.

73. Beth Givens, *Uses of Social Security Numbers in the Private Sector: Why SSNs are Not Appropriate for Authentication*, PRIV. RIGHTS CLEARINGHOUSE (Dec. 10, 2007), https://www.privacyrights.org/blog/uses-social-security-numbers-private-sector-why-ssns-are-not-appropriate-authentication.

74. PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 22 (2007) [hereinafter PRESIDENT'S IDENTITY THEFT TASK FORCE], https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

75. *The Equifax Data Breach*, FED. TRADE COMM'N, https://www.ftc.gov/equifax-data-breach (last visited Feb. 25, 2019).

76. Don Reisinger, *Here's How Much Your Social Security Number Is Worth on the Dark Web*, FORTUNE (Aug. 3, 2016), http://fortune.com/2016/08/03/social-security-dark-web.

77. SECURITY IN NUMBERS, *supra* note 6, at 2.

II. THE PROBLEM: CONFLATING IDENTIFICATION & AUTHENTICATION

As shown above, SSN usage is deeply rooted in the U.S. because of legal requirements and because it provides great utility in both the public and private sectors. This Section analyzes the cause of SSN-based identity theft. It will also highlight aspects of the law that intensify the magnitude of the problem by providing insufficient protection.

Today, SSNs are used for the two distinct purposes: identification and authentication.[78] This dual use creates an inherent and intractable tension. SSNs are used as identifiers and authenticators.[79] An identifier is by definition widely known, especially in cases when it is shared between organizations, as is the case for the SSN.[80] Contrarily, a knowledge-based authenticator, such as the SSN, is used to verify the bearer of an identifier and must be kept secret to serve their purpose.[81] Thus, these two use cases are fundamentally incompatible.

A. Conflation of Identification and Authentication in Practice

First, SSNs are used as a unique identifier.[82] This makes them widely known to government agencies, private businesses, and the public.[83] They even appear in public documents.[84] As described in Part I, SSNs provide value as unique identifiers, and have a significant amount of infrastructure built around them, such that they would be extremely difficult and undesirable to abandon.[85] Countless databases and forms, both public and private, would have to be updated, as would the myriad of processes based on the SSN serving as an identifier.[86] From their roots in the administration of the Social Security

78. Adrianne Jeffries, *Identity Crisis: How Social Security Numbers Became Our Insecure National ID*, THE VERGE (Sept. 26, 2012), https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic.

79. *Id.*

80. *Id.*

81. *Id.*

82. That each individual is issued a unique SSN makes the SSN an attractive identifier. Identifiers are something that points to an entity that is being identified, such as an individual or a row in a database of some individual's records. Credit cards are another good example of identifiers. *See* NAT'L RESEARCH COUNCIL, *supra* note 12, at 18 (discussing unique identifiers).

83. *See* Jeffries, *supra* note 79 (referencing identifiers as related to different public and private sectors).

84. Many police departments published the SSNs of missing persons, they also appear in numerous court filings and other locations cited in Section I. *See* PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 75, at 22 (2007) (referencing public documents SSNs).

85. *See* Part I (describing a plethora of examples). OPM published a draft regulation to limit the collection, use, and display of employee SSNs. Personnel Records, 73 Fed. Reg. 3,410, 3,410 (proposed Jan. 18, 2008) (to be codified 5 C.F.R. pt. 5) (withdrawing a proposed regulation because "no alternate…identifier was available that would provide the same utility as SSNs). However, it withdrew the proposed regulation because "no alternate . . . identifier was available that would provide the same utility as SSNs." U.S. Gov't Accountability Off., GAO-17-553, OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display 11 (2017). *See also* NAT'L RESEARCH COUNCIL, *supra* note 12, at 139 (discussing unique identifiers).

86. *See* Sections I.B & I.C, *supra* (referencing updating databases); *see generally* FTC STAFF SUMMARY, *supra* note 2 (reporting that without SSNs used as identifiers, it would take two weeks longer than it currently does for a bank to extend a loan).

program, SSNs have become widely used as identifiers in such diverse cases as establishing medical records, credit reporting enabling loan decisions by financial institutions, and law enforcement.[87]

SSNs also serve as authenticators.[88] Authentication is the process of establishing the truth of some claim: in this case the truth that an individual is in fact the person they are attempting to identify themselves as.[89] In a 2007 report, the Presidential Identity Theft Task Force found that SSNs are often the "key piece of information used in authenticating the identities" of consumers.[90] In the public sector, the Free Application for Federal Student Aid (FAFSA) uses name, date of birth, and SSN as sufficient knowledge for an authenticator.[91] The same can be said for the private sector, where SSNs are used to authenticate the identity of individuals seeking important medical procedures and financial transactions.[92] A committee of the National Research Council reported that "many of the foundational identification documents used to establish individual user identity are very poor from a security perspective."[93] Therefore, as noted earlier, the SSN remains the key to the kingdom for identity thieves. While the SSN, in its role as a secret, plays an important role in authenticating the identities of individuals, it cannot simultaneous play its immovable and invaluable role as an identifier. Therefore, the solution to this problem must be in augmenting the way in which SSNs are used for authentication. This is the nature of the solution posed in Section III.

B. Conflation of Identification and Authentication in Law

In addition to the issues faced in practice, the current legal framework amplifies the problem by not always differentiating between the SSN as a means of identification or authentication.[94] For instance, the Office of Personnel Management (OPM) uses the SSN as an identifier when it tracks employees internally,[95] and the SSA is required by law to give SSN information to OPM on request for employee programs.[96] However, under 5 C.F.R. pt. 297, when the employee is seeking to retrieve records, the employee is required to produce her

87. Section IV; *see also* FTC STAFF SUMMARY, *supra* note 2, at 4–8 (discussing the use of identifiers).

88. Jeffries, *supra* note 79.

89. NAT'L RESEARCH COUNCIL, *supra* note 12, at 19.

90. *Id.* at 23.

91. Brian Krebs, *Name+DOB+SSN=FAFSA Data Gold Mine*, KREBSONSECURITY, https://krebsonsecurity.com/2017/11/namedobssnfafsa-data-gold-mine (last visited Feb. 25, 2019).

92. *See* Section III.B (discussing authentication in the private sector); *see also* FTC STAFF SUMMARY, *supra* note 2, at 22 (referencing authentication of individuals and the private sector).

93. NAT'L RESEARCH COUNCIL, *supra* note 12, at 168.

94. *See infra* notes 97—98 (discussing the differentiation between identification or authentication).

95. For instance, to find a general personnel record, "various combinations of name, agency, birth date, social security number, or identification number" are required. OFFICE OF PERSONAL MGMT., OPM GOVT-1 9 [hereinafter OPM], https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf (last visited Feb. 25, 2019).

96. *See* 5 U.S.C. § 8347(m)(3)(2018) (requiring the SSA to furnish the OPM with information, including SSNs, upon written request).

SSN as an authenticator.[97] Other federal laws also employ SSN collection for both authentication and identification purposes: for instance, the provision of SSNs to the IRS upon filing taxes at once enables the IRS to ensure that the taxpayer is who they claim to be by providing a secret identification number to authenticate their identity while also enabling the IRS to track their identity.[98]

Sometimes, in moments of clarity, a crucial distinction is made between identification and authentication.[99] In sentencing criminals, the District Court of Nebraska recognized the difference between an SSN as a means of identification and as a method of authentication when determining the level of punishment for identify theft.[100] However, this differentiation has not been the norm.[101]

C. Lack of Legal Protection for SSNs

The current legal framework does not adequately protect citizens from disclosure of their SSNs.[102] There are gaps at both the statutory and the enforcement level.[103] For example, at the federal level for many years, Social Security numbers were printed on Medicare cards.[104] The Medicare Access and CHIP Reauthorization Act (MACRA) of 2015, now requires SSNs to be removed from all Medicare cards,[105] but this law will not go into full effect until April 2019.[106] At the state level, some states, like California, have restricted

97. Privacy Procedures for Personnel Records, 5 C.F.R. § 297.201(b)(1)-(5) (2018). For instance, to retrieve general personnel records the individual is required to provide, "a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature." OPM, *supra* note 96, at 10. Even the additional provisions of 5 C.F.R. Part 297 (Privacy Procedures for Personnel Records) require no additional protection with another authenticator.

98. *See supra* Section I.A (providing different laws related to SSNs).

99. *See generally* Jeffries, *supra* note 79 (referencing the difference between identification and authentication).

100. United States v. Rodriguez-Cisneros, 916 F. Supp. 2d 932, 933 (D. Neb. 2013). While the court did recognize the difference, it also said that under the sentencing guidelines for 18 U.S.C. § 1028(d)(1), (7), an SSN alone was a means of identification and did not qualify as an "authentication feature," within the meaning of the guidelines. *Id.*

101. *See generally id.* at 933 (referencing the commonplace of differentiation between authentication and identification).

102. *See generally* KATHLEEN S. SWENDIMAN, THE SOCIAL SECURITY NUMBER: LEGAL DEVELOPMENTS AFFECTING ITS COLLECTION, DISCLOSURE, AND CONFIDENTIALITY (2008) (discussing the legal protection concerning SSNs available to American citizens).

103. *Id.*

104. *Id.*

105. Medicare & Medicaid Guide 8743051 (C.C.H.), 2015 WL 8743051, at § 501 (including testimony to the Senate Special Committee on Aging regarding the harms of the Medicare card SSN disclosures stating, "there is no other form of individual identification that plays a more significant role in record-linkage and no other form of personal identification that poses a greater risk to personal privacy"); EPIC.ORG, PROTECTING SENIORS FROM IDENTITY THEFT: IS THE FEDERAL GOVERNMENT DOING ENOUGH? 2–3 (Oct. 7, 2015), https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf.

106. *See* Medicare & Medicaid Guide 8743051 (C.C.H.), 2015 WL 8743051, at § 501 (discussing MACRA going into effect). Other areas include government payments. For instance, it was not until the Social Security Number Protection Act of 2010 that government bodies were prohibited from displaying SSNs on payment checks issued. 42 U.S.C. § 405(c)(2)(C)(xi).

when private companies can display SSNs.[107] However, many other states have only prohibited SSN disclosure in a piecemeal manner.[108] This leaves many applications of SSN vulnerable to public dissemination.

There are also issues with enforcement of unlawful disclosures of SSNs.[109] For instance, when a claimant's SSN was shown on a hearing notice in violation of the Privacy Act of 1974, the Supreme Court held that, absent a showing of actual damage, a claimant could not recover.[110] This is a high threshold requirement given that it is difficult to trace a disclosure of an SSN to a specific instance of identity theft.[111] Most cases, however, are not even lucky enough to make it that far, and are instead stopped because plaintiffs fail to show an injury-in-fact and therefore do not have standing to bring a case in federal court in the first place.[112]

Even if the law filled in all the gaps and fixed these intransigent enforcement issues, a legal solution can only remove a use case, i.e. refuse to allow SSNs to be used as an authenticator.[113] There will still be a problem with how to authenticate.[114] Attempts at such a solution using legal and public policy tools were made in 2008, when the recommendations of the President's Identity Theft Task Force were accepted.[115] However, this solution was not adequate as evidenced by enormous costs of identity theft on the economy and the rise of ID theft since 2008.[116] A fundamental lack of a strong form of authentication remains.[117] Therefore, a pure legal solution is insufficient.

In sum, SSNs today are used, and are required by law to be used, in two different capacities: as identifiers and as authenticators.[118] The identification function of SSNs inherently compromises their ability to securely function as

107. Cal. Civ. Code § 1798.85 (West). *See also* N.Y. Gen. Bus. Law §399-dd (including similar SSN limitations).

108. *See* FTC STAFF SUMMARY, *supra* note 2, at 9 (describing briefly state responses to public and private sector entities use of SSN in public records).

109. *See, e.g.*, Doe v. Chao, 540 U.S. 614, 642 (2004) (establishing "the Government need not fear liability based upon a technical, accidental, or good-faith violation of the statute's detailed provisions.").

110. *Id.*

111. *See, e.g.*, In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 38 (D.D.C. 2014) (finding that most plaintiffs did not have standing given that they could not show injury in fact, or causation, but, in regard to one plaintiff whose SSN had been used for a loan application: "the Court is willing to give Curtis the benefit of the doubt [for finding Article III standing only], since there is at least a plausible connection between some of the harm he has suffered and the SAIC theft.").

112. *See, e.g.*, In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., No. MC 15-1394 (ABJ), 2017 WL 4129193 (D.D.C. Sept. 19, 2017) (on appeal to the U.S. Court of Appeals for the District of Columbia) (holding that none of the claimants from the OPM breaches had Article III standing).

113. Jeremy Grant, *Scrapping Social Security Numbers Won't be Enough to Protect Our Identities*, THE HILL (Oct. 27, 2017 6:00 AM), https://thehill.com/opinion/technology/357374-scrapping-social-security-numbers-wont-be-enough-to-protect-our-identities.

114. *Id.*

115. PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 75, at 25.

116. *See* Section IV.B (exploring the economic feasibility of implementing a program against identity theft).

117. *See, e.g.*, SECURITY IN NUMBERS, *supra* note 6, at 2 (demonstrating the problems with the current authentication practices).

118. Jeffries, *supra* note 79.

authenticators. The remaining sections of this Article focus on resolving this issue.

III. NEW SYSTEM DESIGN

While a purely legal solution is not sufficient, a technical solution can provide an elegant and relatively simple means of solving the problem. Consistent with the previous sections, a correct solution will not interfere with the use of SSNs as an identifier but will increase the strength of SSNs when used as an authenticator.[119]

This Article proposes that the SSA issue smarts cards, similar to EMV cards, that contain a cryptographic certificate, with the SSA acting as the certificate authority (CA).[120] These will be distributed with the traditional Social Security card. The smart cards will be a required second factor of authentication for transactions that currently require an individual's SSN. An individual seeking services will prove that she *knows* the SSN by providing it. She will then use the smart card to cryptographically sign documents containing the SSN. Verifying the certificate with the SSA authenticates her and proves that she *has* the authority to use that SSN. When the SSA verifies the certificate, the requesting organization can move forward with the knowledge that the individual is who she claims to be. Importantly for privacy, the SSA can verify a signature's authenticity without accessing the contents of the document. The certificate model provides the additional benefit that smart cards can be used to extend the chain of trust to an individual's cell phone. This improves the system's usability.

The Sections will introduce the solution's design considerations and describe the relevant threat actors. Given this comprehensive set of design and security concerns, the next Sections will detail the technical components of the solution, including the system design, sample workflows, and use cases. The fourth Section will detail the important procedural safeguards supporting the system. The fifth, sixth, and seventh Section then describes privacy implications, possible threat vectors that might be deployed against this system, and the processes for replacing a lost or stolen card. The final two Sections discuss comparisons with other countries, explain design alternatives, and summarize the proposed system.

119. *See* Lily Hay Newman, *Replacing Social Security Numbers Won't Be Easy, But it's Worth it*, WIRED (Oct. 13, 2017), https://www.wired.com/story/social-security-number-replacement (providing solutions to strengthen SSN as identifiers).

120. MCAFEE, MODERNIZING THE SOCIAL SECURITY NUMBER: A FOUNDATION FOR ONLINE AUTHENTICATION OF IDENTITY 21, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-modernizing-social-security-number.pdf.

A. Design Considerations and Threat Actors

This Section outlines the criterion a successful design must meet. The proposed system must be capable of effectively being deployed to all SSN holders. This poses a host of design and usability challenges that must be met.[121] In addition, because of the sensitive data this system is designed to protect, it is also vulnerable to a variety of motivated threat actors.[122] Section 1 will present the relevant design considerations, and Section 2 will discuss the relevant threat actors the system must protect against.

1. Design Considerations

This system must be, and is, designed with all Americans in mind. Designing for 350 million individuals with a large variance in technical literacy and accessibility involves broad usability concerns.[123] However, technical solutions have risen in popularity, and the IRS e-filing system provides compelling data on such a solution's feasibility.[124] The IRS has seen the percentage of all tax returns filed through its e-file system jump from 30% in 2001 to 92% in 2016,[125] showing the potential for vast adoption of an electronic government system. Still, only 84% of Americans use the Internet, a number that decreases for low-income, rural, and historically disadvantaged populations.[126] Therefore, the system makes minimal assumptions about users' capabilities. It accommodates individuals without smartphones, reliable Internet connections, and disposable income and time, while also being user friendly for users without such constraints.[127] These considerations were accounted for in the formulation of the following design goals:

121. *See* Newman, *supra* note 120 (explaining the challenges of using SSN as an identifier).

122. *See* Anthony Giandomenico, *Know Your Enemy: Understanding Threat Actors*, CSO FROM IDG (June 27, 2017), https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html (explaining the different types of threat actors).

123. *See* Brandi Vincent, *Experts Agree That Social Security Numbers Need To Change—But There's No Solution In Sight*, NBC NEWS (Nov. 4, 2018, 6:36 AM), https://www.nbcnews.com/tech/tech-news/experts-agree-social-security-numbers-need-change-there-s-no-n930611 (explaining the issues with a new SSN system).

124. *Income Tax Return Statistics*, EFILE.COM, https://www.efile.com/efile-tax-return-direct-deposit-statistics (last visited Feb. 26, 2019) (illustrating that U.S. taxpayers e-filed more than 128 million returns in 2016).

125. *Id.*

126. Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RES. CTR. (June 26, 2015) http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015.

127. *See Frequently Asked Questions about Filing Your Taxes Electronically*, INTERNAL REVENUE SERV.: USTAXCENTER, https://www.irs.com/articles/electronic-filing-e-file-faqs (last visited Feb. 26, 2019) (answering publics concerns about e-filing constraints).

(1) *No identifying properties*. Maintaining any identifying properties will fundamentally weaken the strength of the authentication system.[128]
(2) *Modern.* As government services move online[129], the design must protect both online and in-person transactions.
(3) *Backward compatible.* Although the plan intends to replace SSNs as the sole factor in authentication, this transition could take several decades.[130] Any new system must work around existing processes built for SSNs. Those who do not adopt the new system must not be any worse off than they were before.
(4) *Universally accessible.* The design must be compatible with the computers and phones that individuals already have, without additional hardware. But it also should not require these devices.
(5) *Easy to use*. Cryptography is essential in security applications but cannot come at the cost of usability.[131]
(6) *Cheap and boring.* The design should reuse existing technologies and administrative processes, as they have proven reliable and are available at scale.
(7) *Respects privacy*. To assuage Americans' fears of tracking,[132] the system should only collect information necessary for providing additional authentication where SSNs are already used and should minimize centrally stored information.
(8) *Resilient.* It is inevitable that there will be security breaches of different magnitudes.[133] In the event of a breach in one component, the system should be designed to minimize impact on other parts of the system.
(9) *Error tolerant.* In a system of this scale and complexity, errors are inevitable.[134] The system design must be resilient against both user errors (e.g., losing a smart card) and system errors (e.g., software bugs).

It is likely impossible to achieve all goals simultaneously. However, a new system can still be considered a success if it offers stronger authentication to a meaningful portion of the population.

---

128. Proving this statement was the subject of Part II. *See also* NAT'L RESEARCH COUNCIL, *supra* note 12, at 30 (giving examples of privacy concerns).

129. *Digital Government: Building a 21st Century Platform to Better Serve the American People*, DIGITAL GOV., https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html (last visited Feb. 26, 2019).

130. Vincent, *supra* note 124.

131. *See* NAT'L RESEARCH COUNCIL, *supra* note 12, at 7–8 (explaining usability concerns).

132. RonPaul2008dotcom, *Ron Paul: A National ID Card? Outrageous!*, YOUTUBE (Mar. 10, 2010), https://www.youtube.com/watch?v=n9CZ5OUet3s.

133. Dan Goodin, *Millions of High-Security Crypto Keys Crippled by Newly Discovered Flaw*, ARS TECHNICA (Oct. 16 2017, 7:00 AM) https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids (describing how the Infineon key generation vulnerability compromised 750,000 of Estonia's national ID cards).

134. Newman, *supra* note 120.

2. Threat Actors

Various types of threat actors pose different threats to the system, each of which must be considered. This Article identifies four groups of actors: friends and family, common criminal, organized crime, and foreign powers. The smart card design in Section B will take into account these considerations.

(1) *Friends and Family.* This actor may have knowledge of the target's SSN and likely has access to the same physical spaces. It is unlikely that this actor will have the ability to forge identifying documents, though they will likely have access to the legitimate documents. It is unlikely that this actor will have the ability to compromise any centralized infrastructure.
(2) *Common Criminal.* This threat actor has the ability to steal a person's wallet, which may include identifying documents. This actor may have the ability to purchase stolen identities, including SSNs, on the black market.[135] This actor is unlikely to compromise any centralized infrastructure.
(3) *Organized Crime.* This threat actor is similar to the common criminal, though they may have the ability to forge identifying documents.[136] This actor may also have the ability to launch more sophisticated attacks on electronic systems.[137]
(4) *Foreign Powers.* Physical access is unlikely to be this actor's cheapest attack vector. This actor is likely to have the ability to compromise different aspects of the backend system that supports the usage of the smart card.[138]

B. Smart Card Design

As has been established, SSN use as an identifier should not be abandoned.[139] Instead, additional authentication should be provided where SSNs are already used.[140] The plan proposes issuing every user a smart card similar to those in EMV payment cards. The card will contain an individual's

135. Megan Leonhardt, *Here's How Much Hackers Get for Your Social Security Number and Other Information on the Black Market*, CNBC (Aug. 22, 2018, 10:59 AM), https://www.cnbc.com/2018/08/22/how-much-hackers-get-for-social-security-numbers-on-the-black-market.html.

136. *See generally*, NAT'L RESEARCH COUNCIL, *supra* note 12 (discussing document forgery).

137. *See* Annie Nova, *Scammers Create a New Form of Theft: 'Synthetic-Identity Fraud'*, CNBC (June 7, 2018, 9:00 AM), https://www.cnbc.com/2018/06/07/scammers-create-a-new-form-of-theft-synthetic-identity-fraud.html (demonstrating organized identity theft crimes).

138. Jen Schwartz, *The Vulnerabilities of Our Voting Machines*, SCI. AM. (Nov. 1, 2018), https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines (discussing the possibility of foreign power attack on backend voting systems).

139. *See* sources cited *supra* note 87 (describing studies that show that there is no other identifier that offers the same utility).

140. This proposal explicitly does not attempt to address the privacy implications of linking individuals across databases via their SSNs. Maintaining the status quo on privacy allows us to focus on identity theft, which we believe to be a more urgent source of consumer harm.

certificate and SSN, the possession of which proves ownership of an individual's SSN. A central authority trusted by all parties, in this case the SSA, manufactures the cards, signs their embedded certificates and SSNs, and maintains a certificate revocation list (CRL). In this section, Part 1 will present the design and properties of the physical card. Part 2 will discuss the recovery properties for the card. Lastly, Part 3 will discuss the statutes governing the construction of the current SSN cards.

1. Card Security

Smart cards provide a secure foundation upon which the rest of the scheme sits. Embedding each user's secret key within a card takes advantage of the inherent usability of a physical device over password-based authentication,[141] while making impossible the kinds of accidental secret disclosure associated with applications that store keys as files on the user's computer.[142] This achieves the design goal of being "easy to use." The cards also contain a processor that performs cryptographic operations on the embedded secret key. For any threat actor, recovering the secrets stored in the card would be an expensive and time-consuming process. Unlike desktop computers, cards' simple firmware leads to a reduced attack surface and forces hardware-based attacks with high marginal costs,[143] satisfying the "resistant to breaches" design goal.

No identifying information will be printed on the cards[144] because a moderately sophisticated threat actor with a name, home address, and the smart card could easily purchase the cardholder's SSN on the black market.[145] The identifying information would allow an attacker to pair the identity with an SSN, defeating the purpose of multifactor authentication. Ensuring that the card does not have any identifying properties is consistent with the first design goal.

2. Recovery Properties

Recovery properties of this system fall into two categories: (1) failures or errors discovered in the system, and (2) an individual's loss or misuse of the

141. *See* Ugo Piazzalunga et al., *The Usability of Security Devices*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 221, 229 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005) (explaining the different systems that can be implemented).

142. *See* Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, 8 PROC. USENIX SEC. SYMP. 169, 180 (1999) (discussing a usability study that showed that users often disclose their private keys while attempting send encrypted emails using PGP).

143. *See* Ross Anderson et al., *Cryptographic Processors: A Survey*, 94 Proc. IEEE 100, 113 (2006) (explaining how chip-level attacks mostly revolve around dissolving the plastic chip package using a solvent, then probing the exposed chip. There also exist statistical attacks based on timing and power consumption, but they are not unique to smart cards. These attacks are very expensive).

144. Some users may have multiple cards: for example, a parent might manage the cards of their minor children. We propose the following system to distinguish cards securely. The SSA provides a collection of about 100 patriotic images, which each user can select when applying for a card. The parent would remember that their own card has an image of Grand Teton, while their child's card has the Lincoln Memorial.

145. Reisinger, *supra* note 77.

card. In the event of a compromise of the certificate generation procedures, as happened in Estonia,[146] the SSA revokes all certificates generated during the window of compromise by updating its CRL. Then, all affected individuals will need to apply for new cards. In the event of an issue with an individual's card, the card can be revoked and replaced through the same mechanism that is used for replacing Social Security cards today.[147] Each of these two cases will be further detailed in Section D.

3. Nature of the Card

To allow the SSA the authority to issue smart cards, certain legislation must change.[148] The SSN card is described in law under 42 U.S.C. § 405(c)(2)(G) which requires that the Commissioner of Social Security issue each citizen a card "made of banknote paper . . . which cannot be counterfeited."[149] As a first step, Congress would need to amend 42 U.S.C. § 405(c)(2)(G) so that it requires the Commissioner to issue an account number on banknote paper *and* a smart card. This will fix one issue within the case law: any time an SSN card is required in the current legislation, the smart card will now be required. The card technology should not be specified in detail: this will allow the card to change as the underlying technology advances.

C. System Design and Use Cases

This new smart card will need to operate within a secure cryptographic system.[150] In describing the scheme, the Article presents two examples: applying for a loan in person and filing taxes online. These examples are important because fraudulent lines of credit and tax refunds are instances of identity theft that greatly harm consumers.[151] The workflows presented in these examples can be deployed to support any number of authentication tasks in the public and private sectors. Both workflows are designed to leverage hardware that is already widely adopted to minimize the risks of deployment. In this Section, Part 1 will present the authentication mechanism relying on the card. Part 2 will present the method by which the chain of trust can be extended to a phone and will subsequently present the authentication mechanism relying on the phone. For clarity, much of the technical justification has been placed in the footnotes.

146. *See* Goodin, *supra* note 134 (explaining that the Infineon weak keys bug compromised 750,000 of Estonia's national ID cards).

147. *See infra* Section III.E. (discussing the privacy implications of usage of SSN's).

148. *E.g.*, Social Security Act, 42 U.S.C. § 405(c)(2)(G) (2018).

149. *Id.*

150. *See supra* Section III.A.2 (several types of actors pose threats to the system).

151. PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 75, at 18, 21.

1. In-person Authentication: Applying for a Loan

Suppose a user walks into a bank branch to apply for a loan. The user and the bank follow this procedure to authenticate the user:[152]

(1) The bank prepares a loan contract on a terminal[153] at the branch
(2) User inserts card into the terminal and enters SSN[154]
(3) If the SSN entered matches the SSN stored on the card,[155] the card accepts a signing request
(4) Terminal sends the hash of the document[156] and a nonce[157] to the card
(5) Card performs the signing operation using its private key, returning its certificate and the signature to the terminal
(6) Terminal forwards the file, signature, and card's certificate to the bank's server
(7) Bank server queries the SSA server to ensure the card's certificate has not been revoked in the CRL[158]
(8) Bank server verifies that the SSN in the document matches the SSN in the card's certificate[159]
(9) Bank server processes the application as usual

152. It is important to note that to protect the card's security, a user should only have the card with them when they intend to conduct a transaction they must have it present for, such as the one described in this example. It is unlikely that a user will have the card with them with any meaningful frequency. This is also the case for the example in Section 2, *infra*. Discouraging users from having their card with them in general will help to assuage the fear that the authentication token has any identifying properties, consistent with the "no identifying properties" design goal. *See supra* Section III.A.1 (discussing identifying properties).

153. A terminal is taken to be a system that has the ability to read the card, receive documents to be signed by the card, and communicate with the upstream processing server. For example, it may consist of a card reader connected to a desktop computer.

154. To use the card, the user must provide the associated SSN. This ensures that card theft alone is insufficient for identity theft. We use the SSN to avoid forcing users to generate and memorize a password, which is likely to be reused elsewhere. *See* Anupam Das et al., *The Tangled Web of Password Reuse*, 14 NETWORK & DISTRIBUTED SYS. SEC. SYMP. 75, 75–78 (2014) (introducing some of the most frequently used password composition policies and summarizing recent academic literature in the field of password analysis).

155. To prevent brute-force attacks, the fifth unsuccessful SSN attempt causes the card to disable itself permanently. At this point, the user must request a replacement card as specified in Section 3. *See also infra* Section F (providing a discussion on techniques to ensure reader security).

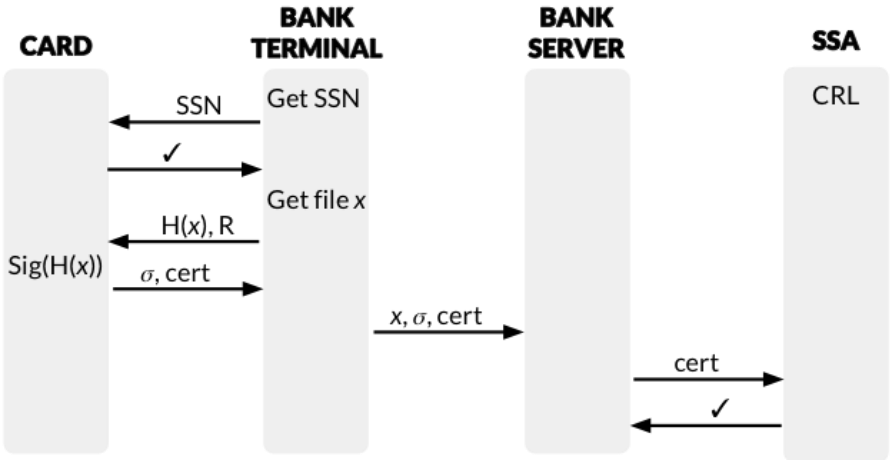
156. This operation implicitly trusts that the reader will provide the correct hash to the card. *See* Section F, *infra* (providing a discussion on techniques to ensure reader security); *see also infra* note 177 (describing the activation process).

157. The nonce prevents replay of the signed document. Note that, in this particular use case, the bank could also prevent replay attacks by refusing to approve any loan applications identical to previously submitted applications. Other applications' signed data may not exhibit this property. *See* footnote and accompanying text *infra* note 172.

158. The SSA revokes lost or stolen cards by distributing a Certificate Revocation List (CRL). In the authentication process, the SSA is only responsible for verifying certificates. It never receives the contents or hash of any document. *Revoking certificates*, CERN (June 6, 2017), https://ca.cern.ch/ca/help/?kbid=021004.

159. The SSN in the card's certificate links the certificate to an identity. The SSN on the document is used in the bank's business processes, such as sending loan information to a credit reporting agency. If these SSNs do not match, but the bank proceeds with the loan, identity theft can still occur.

The following diagram summarizes these steps, where *x* is the loan application, *R* is the nonce, *H(x)* is the hash function, and *Sig(x)* is the cryptographic signing function. The remaining symbols are as described in Section A.



2. Online Authentication: E-filing Tax Returns

The previous example requires a smart card and a card reader. However, most computers do not have built-in card reader functionality.[160] The following example presents a mechanism for SSN holders to perform transactions in the absence of a card reader, fulfilling the "modern" and "universally accessible"[161] design goals.

In this model, the user can provision a certificate to their phone, allowing it to fulfill the task of cryptographically signing documents without needing to use the card. This is similar to the loan application example described earlier[162]; however, the card issues a certificate to the phone by signing the phone's public key, rather than signing loan documents. This gives the phone the ability to sign documents as if it were the card.

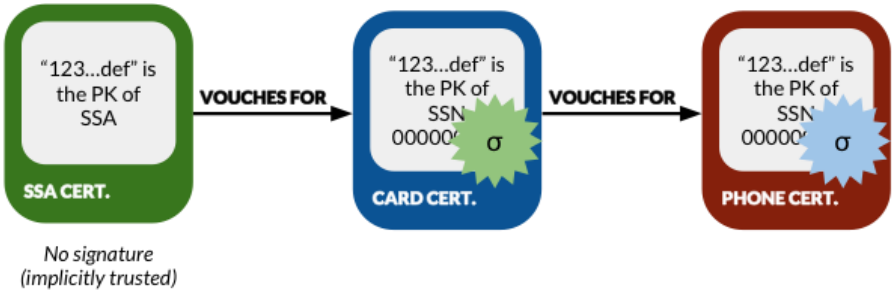
The end goal is to construct a chain of trust as follows. The SSA certificate, which is implicitly trusted by all parties, signed a certificate embedded in the user's smart card at the time of manufacturing. This means the SSA vouches for the card's authenticity.[163] Then, during the phone provisioning workflow, the card signs the phone's certificate, showing that it has verified that the user of the phone is also the user of the card. The diagram below depicts this chain of trust.

160. Estonia's system suggests that users without card readers "ask for one from a computer store." ID, *ID-card and Digi-ID*, https://www.id.ee/index.php?id=30500 (last visited Feb. 26, 2019). These readers would be difficult to distribute at scale.

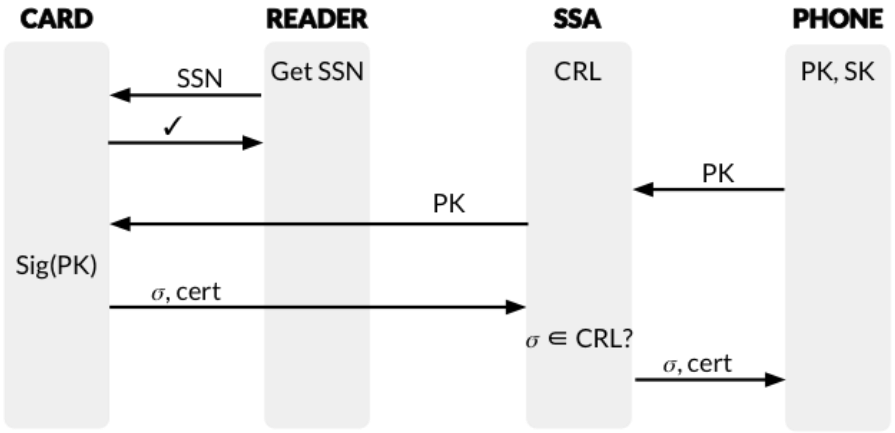
161. *See supra* Section III.A.1 (describing the modern and universally acceptable design goals, one of which is providing users with more ways to authenticate).

162. *Supra* Section III.C.1.

163. *See supra* Section III.C.1 (providing the authentication procedure for in-person loans).



The following diagram depicts the workflow for extending the chain of trust to a phone:



Once the mobile device has been provisioned a certificate, a user who wishes to e-file their tax return, but does not have a card reader, would follow this workflow:

(1) Tax preparation software submits the tax return to IRS as usual
(2) IRS provides a 2D barcode for the tax software to display. The barcode represents some IRS-defined identifier for the user's tax return, such as a transaction number or the hash of the submitted file, concatenated with a nonce
(3) User scans the 2D barcode with mobile device
(4) Mobile device signs the barcode's contents, then transmits its certificate chain and signed data directly to the IRS
(5) IRS queries the SSA server to verify the certificate chain's validity
(6) IRS verifies that the SSN in the certificate matches the SSN on the tax return
(7) IRS processes the tax return as usual

The figure below illustrates this process from the user's perspective:

D. Procedures and Safeguards

The technical architecture above describes how the system functions, but there remain important procedural questions regarding how the system is to be administered. A strong technical infrastructure does little good without equally strong procedural safeguards.[164] Toward a system that meets the "backward compatible" and "error tolerant" design goals, this Section addresses the following questions:

(1) How does an individual procure her first card?
(2) How does an individual report a card as lost or stolen?
(3) How does an individual replace a lost or stolen card?
(4) What limits should be placed on replacing cards?

1. Authentication and Legal Verification Requirements

The overarching concern for these four questions revolves around how an individual can reliably authenticate his or her identity to the SSA without the card. For ease in implementation, the card will be subject to the same authentication requirements that the SSA already implements for a new or replacement Social Security card.[165] It follows that it should be no more difficult to obtain the second factor of authentication for an SSN than it is to get the SSN. Pinning the authentication procedure, and other procedures, that support the card

164. *See supra* note 71 (a business is required to first implement and maintain internal procedures to protect SSNs in several states).
165. *See infra* Section III.D.2 (describing the procedure for obtaining the smart card).

to already existing procedures and practices employed by SSA and other agencies helps achieve the design goals of "cheap and boring" and "universally accessible."[166]

2. Procuring the First Card

As with current Social Security cards, newborns will be issued a smart card at birth. However, when the system is implemented, the existing population must have a method to request a smart card.

To obtain a smart card, the SSA will require the same documents that it does currently for paper SSN cards: proof of identity (such as a driver's license), proof of citizenship (such as a birth certificate), and proof of age.[167] This is a strong form of authentication: in fact, individuals applying for a U.S. passport are subject to the same requirements.

Thus, the procedure for obtaining the smart card will be as follows:

(1) User applies online through SSA.gov
(2) User provides her SSN and select her preferred post office[168] for picking up the card.
(3) The SSA issues a case number[169]
(4) User brings her authenticating documents and case number to the post office
(5) Post office employees will verify the individual's identity and give him or her the card associated with her case number[170]

166. *See supra* Section III.A.1 (presenting relevant considerations in designing the systems).

167. *See Social Security Cards: Documents Required to Obtain a Social Security Number and Card or a Replacement Card*, CONN. 2–1–1, http://uwc.211ct.org/social-security-cards-documents-required-to-obtain-a-social-security-number-and-card-or-a-replacement-card (last visited Feb. 26, 2019) (listing the documents required to obtain a Social Security number).

168. The proposed system uses post offices because there are 31,324 post offices, compared to only 1,400 Social Security offices. *See* 20 C.F.R. § 422.106 (2018) (allowing filing for a new social security card with other agencies so long as the SSA enters into an agreement with the federal agency); *Sizing it up*, U.S. POSTAL SERV. https://about.usps.com/who-we-are/postal-facts/size-scope.htm (last visited Feb. 26, 2018) (providing various United States Postal Service statistics); *see also* Doug Walker, *Social Security Serves Nearly 41 Million Visitors a Year in 1,400 Offices Across the Nation!*, SOC. SEC. MATTERS (Nov. 10, 2016), https://blog.ssa.gov/social-security-serves-nearly-41-million-visitors-a-year-in-1400-offices-across-the-nation (providing a map illustrating all the visitors to the social security offices).

169. The card cannot be mailed to the individual directly, because the name on the envelope would create a link between a card and an individual. The randomly chosen case number serves the same function to protect against a rogue postal employee. In addition, applying online also ensures that users can make a single trip to the post office in which they receive the physical card and authorize a mobile device. This furthers the "universally accessible" design goal by reducing the burden on low-income users who may have less scheduling flexibility. *See supra* Section III.A.1 (describing the modern and universally acceptable design goals).

170. Such verification is already an extremely familiar task of the post office, as in the case of passport applications.

(6) User unlocks the card by entering SSN.[171] The card signs a message to the SSA, which activates the card by removing it from the CRL and returns a signed response communicating this activation to the card[172]
(7) User optionally authorizes a mobile device using the terminal in the post office[173]

3. Replacing a Lost or Stolen Card

To replace a lost or stolen card, the SSA requires the same proof of citizenship and identity. Additionally, the SSA currently has many processes in place to help individuals replace lost or stolen cards. These can be leveraged in the new card system. However, for the new system it is essential that it is difficult to link an individual's card with her identity. Therefore, physically obtaining the card and activating it will need to be completed by the same process undertaken in obtaining a new card.

Applying for a new card will trigger revocation of the certificate of the lost or stolen card. Therefore, applying for a new card is the mechanism by which a card can be reported lost or stolen.

E. Privacy Implications

Any discussion of the usage of SSNs immediately merits an analysis of its privacy implications.

For its core operation, this system does not include the collection of any personally identifiable information (PII). However, there will necessarily be some collection of PII in the administration of this system. For example, the SSA will need to gather some PII to successfully distribute a card to an individual. Any privacy concerns stemming from this collection can be mitigated by strict data retention schedules for this information. Additionally, there will be some PII received and maintained by the SSA for the functioning of an individual's SSA account if an individual loses her card and needs to bootstrap trust from scratch. This information will be the same information that is maintained from credit reporting agencies[174] and can be subject to strict usage requirements to prevent against any potential for misuse.

One might raise the concern that this will allow the SSA to be privy to document and data used by public and private entities, which is signed with the user's certificate. However, the system is designed such that the signed

171. This requires the individual to enter the SSN into the card to gain access to the signing certificate, verifying that the individual claiming the card is the true individual associated with the case number given.

172. The card signs a random challenge string (nonce). The server ensures that the card has not already been activated, then signs the challenge string plus the card's identifier or public key. The card firmware only activates when it receives a properly signed message. The above activation process ensures that cards are only activated when a user proves their possession of the card and knowledge of the embedded SSN. The process is similar to the activation process for Apple iOS devices. *See iOS Security: iOS 12.1*, APPLE, 6 (Nov. 2018) [hereinafter IOS SECURITY], https://www.apple.com/business/docs/iOS_Security_Guide.pdf (describing the activation process on iOS).

173. *See supra* Section III.C.2. (explaining authentication process for e-filing of tax returns).

174. *See supra* Section I.A.2 (citing the use of SSN in the private sector).

document is never sent to the SSA. Only a certificate that never contains any PII or other sensitive data is sent.

F. Relevant Threat Vectors

There exist a number of methods an attacker may deploy to thwart the system outlined in this Article. This Section considers these attacks, the threat actors that might carry them out, and how the system might be affected by each attack.

(1) *Theft of Card*

Available to: All Actors

This threat is mitigated by the recommendation that individuals only carry this card when they intend to use it for sensitive authentication matters. It is also mitigated because the SSN is needed to enable the usage of the certificate stored on the card. The damage of a stolen card is small due to both the difficulty of linking a card with an individual's identity and a revocation mechanism.[175]

(2) *Compromise of SSA Phone App*

Available to: Organized Crime, Foreign Powers

If an actor gained access to the secret key on the phone,[176] it is possible that the actor would be able to successfully impersonate the target.[177] This is a difficult risk to manage.[178] The same threat is present for the many financial services mobile applications that exist today, and these institutions have been able to deploy these applications with an acceptable level of risk.[179]

(3) *Theft of SSN*

Available to: All Actors

---

175. OECD, *National Strategies and Policies for Digital Identity Management in OECD Countries*, OECD DIGITAL ECON. PAPER NO. 177 (2011) [hereinafter OECD], https://www.oecd-ilibrary.org/science-and-technology/national-strategies-and-policies-for-digital-identity-management-in-oecd-countries_5kgdzvn5rfs2-en (referencing the Australian ID Theft Booklet).

176. In the future, key material may be stored in a phone's secure coprocessor to prevent this type of attack. (iOS currently does not allow third parties to store secrets in the coprocessor. IOS SECURITY, *supra* note 173, at 15–16. We hope that, as more Android devices add these security features, market pressure will cause iOS to do the same.)

177. Piazzalunga et al., *supra* note 142, at 229. *See generally* OECD, *supra* note 176 (discussing the current problems multiple countries face with respect to mobile applications and impersonation).

178. OECD, *supra* note 176.

179. *See generally* Brooke Satti Charles, *Is Mobile Banking Safe?*, SECURITY INTELLIGENCE (June 7, 2016), https://securityintelligence.com/is-mobile-banking-safe (showing the security risks inherent in mobile banking that are being confronted by banks).

This threat is only problematic if it is combined with the theft of an active card. Stealing an SSN and matching card will be difficult because the card will have no identifying information.[180]

(4) *Compromise of Terminal*

Available to: Organized Crime, Foreign Powers

Compromising the terminal with attacker-written malware would allow an attacker to sign arbitrary content. This can be mitigated by using code signing to ensure that only SSA-authorized code run on the terminal, and a software activation mechanism to prevent downgrading terminal software to older versions that may contain more vulnerabilities. Apple's iOS shows the practicality of these techniques.[181]

(5) *Denial of Service*

Available to: All Actors

Denial of service could occur in two ways. First, it could occur if the threat actor denied service over one of the network links that makes this system possible. The second mechanism it could be triggered through reporting a target's card as stolen, invoking the revocation of their certificate, which would prevent the target from using their card.

(6) *Compromise of Key Generation Process*

Available to: Organized Crime, Foreign Powers

If an actor were able to record the private keys as they are copied to the cards, they could use the target's SSN freely.[182] They may also create their own key pair and trick the SSA into signing it.

G. Comparisons and Alternative Solutions

Finally, there are examples of countries which have implemented e-cards, and a number of other possible alternatives to the authentication/identification problem.[183] The countries provide an example of working systems, that have

180. *See supra* note 142 and accompanying text (describing how the card will have no identifying information).

181. *See* iOS SECURITY, *supra* note 173, at 5–6 (showing Apple's technique used to prevent users from downgrading to an older operating system with more security vulnerabilities).

182. *See supra* Part III.B.2. (discussing recovery procedures).

183. *See The German National Identity Card*, FED. MINISTRY OF THE INTERIOR, BUILDING AND CMTY., https://www.personalausweisportal.de/EN/Citizens/German_ID_Card/German_ID_Card_node.html (providing information regarding the functions, features, and application for the German ID card.). *See generally* OECD, *supra* note 176 (illustrating the current landscape surrounding various countries' eID cards).

experienced (and continue to experience) issues, but still use e-cards.[184] The working aspects of their structure is incorporated into the solution provided above, and the imperfections have provided a cautionary tale for certain design choices. The alternatives in Section 2 give a brief analysis of some of the various alternatives considered and set aside for their insufficiencies in this context.

1. Review of Estonian and German National Identity Cards

This Section will briefly review Estonia and Germany's national ID cards. There are two main differences between the proposed system and these three countries. First, unlike the cards issued in Estonia and Germany, the cards proposed in this Part do not carry information, printed or electronic, that could be used for identification.[185] They are only used for SSN authentication.[186] Second, the cards issued in Germany are difficult to use online.[187] These two countries demonstrate, however, the security and viability of a smart card system.[188]

The Estonian government has issued smart cards that also serve as national ID cards since 2002.[189] The cardholder's identifying information, including name, national ID number, birthdate, and citizenship status, are both printed onto the card and stored electronically.[190] The cards also contain the user's certificate, which is generated and trusted by the government, allowing users to authenticate transactions using a digital signature.[191]

When vulnerabilities in some Infineon-produced smart cards came to light, the Estonian government was able to identify and disable the affected cards by revoking their certificates.[192] This ensured that that the cards could not be abused while replacement cards were being manufactured.[193] Even with the vulnerability, breaking a single card took several days and cost $40,300.[194] This

184. *See generally* OECD, *supra* note 176 (illustrating the current landscape surrounding various countries' eID cards); *see also* Tarvi Martens, *Electronic Identity Management in Estonia Between Market and State Governance*, SPRINGERLINK.COM (Feb. 4, 2010), https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0044-0.pdf (providing a broad overview of the Estonian system).

185. As discussed throughout this Article, the proposed card is used for authenticating the SSN only and does not display any identifying information. National IDs have been a hot-button political issue in the United States for generations. *See generally* JOSEPH W. EATON, CARD-CARRYING AMERICANS: PRIVACY, SECURITY, AND THE NATIONAL ID CARD DEBATE (1986) (discussing the issues with National ID cards).

186. *See* AS SERTIFITSEERIMISKESKUS, THE ESTONIAN ID CARD AND DIGITAL SIGNATURE CONCEPT: PRINCIPLES AND SOLUTIONS 6, https://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf (last visited Feb. 27, 2019) (describing the data on the card).

187. *See* Andreas Poller et al., *Electronic Identity Cards for User Authentication: Promise and Practice*, 10 IEEE SECURITY & PRIVACY 1, 10 (2012), https://ieeexplore.ieee.org/document/6035661 (noting the German card is difficult to use online).

188. *Id.*

189. AS SERTIFITSEERIMISKESKUS, *supra* note 187, at 5.

190. *Id.* at 6.

191. *Id.* at 7–12.

192. Goodin, *supra* note 134 (explaining that the Infineon weak keys bug compromised 750,000 of Estonia's national ID cards).

193. *Id.*

194. *Id.*

incident illustrates the improved security provided by digital signature systems based on government-issued smart cards.[195]

Beginning in 2010, newly issued German national ID card also included smart card functionality.[196] The cardholder's identifying information, including name, date of birth, and nationality, are both printed on the card and stored electronically.[197] The new cards are also capable of producing digital signatures; however, this feature is optional and users must obtain certificates from private-sector issuers.[198] The card instead serves its purpose as an authenticator through its "eID" feature, which authorized organizations use to receive a copy of the personal information stored in the card. It is comparable to making a photocopy of the printed information.[199]

Although the eID functionality allows organizations to verify that an individual possesses a genuine identification card, its online and mobile functionality is cumbersome: users must acquire a reader and install the associated driver and browser plug-in.[200] By contrast, the use of digital signatures proposed in this Part provides a generic framework for delegating card functionality to the user's other devices.

2. Alternative Technical Solutions

There are many technical architectures that could be leveraged to solve the SSN identity theft issue.[201] This Article includes the fundamental design requirement that the solution minimize disruption of the current SSN system.[202] As discussed in Part I, the SSN is thoroughly entangled in both the private and public sector. Under these constraints, a second form of authentication is needed, but the SSN must remain. Authentication solutions are of three categories: *something you know*, *something you have*, or *something you are*.[203] This Section will investigate alternative solutions in each of these categories with respect to the design goals.[204]

a. Something You Know

The first factor of authentication, the SSN, is *something you know*, or a knowledge-based authenticator. It is an accepted rule of authentication that a

195. *Id.*
196. *See* Poller et al., *supra* note 188, at 2–3 (noting the German card was issued and distributed in 2010).
197. *Id.*
198. *Id.* at 2.
199. *Id.*
200. *Id.* at 6.
201. *See supra* Part III.C (describing design architecture).
202. *See supra* Part A (describing the history of the SSN); *see also* Steven M. Bellovin, *Replacing Social Security Numbers Is Harder Than You Think*, VICE: MOTHERBOARD (Oct. 5, 2017, 10:30 AM), https://motherboard.vice.com/en_us/article/pakwnb/replacing-social-security-numbers-is-harder-than-you-think (explaining the inherent difficulty in replacing SSNs).
203. NAT'L RESEARCH COUNCIL, *supra* note 12, at 106.
204. *See supra* Part 1 (discussing various design considerations).

second factor of authentication must not be of the same form as the first.[205] This is because authentication methods of the same factor are generally susceptible to the same attacks.[206] Since the SSN is *something you* know; the second factor of authentication therefore cannot be an additional *something you know*.

Something you know is not a strong factor of authentication for the proposed system for additional reasons.[207] A commonly argued positive aspect of using a knowledge-based authenticator, such as a password, is that people are generally familiar with how to use them.[208] Therefore, the authenticator appears to satisfy the *usability* design goal.[209] However, in practice people find managing passwords difficult and use this form of authentication incorrectly by recycling the same password for different systems.[210] If a password authenticator was used to protect the SSN, an attacker could steal a password that is easy to find and subsequently use that same password to receive credit with the victim's SSN.[211] Therefore, because users tend to incorrectly employ knowledge-based authenticators, such as passwords, it would not be an effective second factor of authentication.

b. Something You Are

The most developed form of authentication is based on *something you are*. This is the "automatic identification or identity verification of human individuals on the basis of behavioral and physiological characteristics."[212] This authentication method is usually biometric, which would offer added protection at too high a cost.[213]

A solution based on a biometric factor of authentication simplifies the process and eliminates the need to manage a secret or token.[214] Biometrics do not require any management because they, by design, measure an aspect of an individual that is unlikely to change. There are still, of course, problem cases

205. NAT'L RESEARCH COUNCIL, *supra* note 12, at 118.

206. Let's say an authentication system requires two passwords. If an attacker can successfully steal the first password, she will likely not find any trouble stealing the second. Therefore, the second factor of authentication does not add much security, as it does not increase the cost of the attack for the attacker. If, however, the second factor was *something you have*, and the attacker, in additional to needing to steal your password needing to steal a token off of a physical person, this would meaningfully increase security and the cost of the attack.

207. *See* NAT'L RESEARCH COUNCIL, *supra* note 12, at 107 (explaining the vulnerability due to the inherent simplicity and static nature of a one-way authentication system).

208. *Id.*

209. *Id.* at 80–103 (noting the need for improved usability).

210. This also gives the password identifying properties. For instance, if a person uses the same password across two different systems, and one system contains identifying information about the individual, the password would effectively identify the individual to an attacker.

211. *Id.*

212. NAT'L RESEARCH COUNCIL, *supra* note 12, at 121.

213. *See id.* at 122 (arguing that the expenses associated with biometric authentication have served as a barrier to its adoption).

214. *See id.* ("Although all biometric measures change over time, an individual cannot forget his or her biometric values, unlike passwords and PINs, nor can they be lost, like hardware tokens.").

with biometrics (e.g. individuals that do not have easily discernable fingerprints, or those who lose their fingerprints to burns).[215]

Biometric authentication presents more challenges than solutions as applied to the proposed system. First, because it is not safe to conduct biometric authentication remotely,[216] it would not meet the *modern* design goal to offer services online.[217] Secondly, the infrastructure needed to conduct biometric scanning is not widely deployed, and the cost of deploying the necessary infrastructure would be extremely high, forcing this form of authentication to fall short of the design goal of being *backward compatible.*[218] More problematic still, are the social and privacy issues that a government-run biometric identification system would raise.[219] Many people are extremely concerned that government collection of their biometric information is a breach of their privacy, and are further concerned that the government will use this information for illicit purposes outside of solely storing the information for authentication purposes.[220] Public backlash to national identification systems[221] suggest that U.S. citizens are not ready to surrender biometric data to the government. Many privacy challenges still remain in the development of the technology itself.[222] Additionally, biometric technology has a track record of behaving differently when used by individuals of different races.[223] This presents a tremendous risk for using a biometric authentication system in sectors that have experienced racism or are more heavily regulated, such as extending credit, which is a particularly important use of the SSN.[224] For these reasons, a solution based on a biometric factor of authentication would not suffice.

c. Something You Have

Something you know and *something you are* each present tremendous challenges and fail to meet many of the design goals. However, *something you have* as a factor of authentication meets all of the design goals unique to SSN

215. *Id.* at 123.

216. *Id.*

217. *See id.* (arguing that "[t]he use of biometrics for local authentication . . . is a more appropriate type of use for biometrics.).

218. *Id.* at 122.

219. *See id.* at 123 (arguing that using biometrics for remote authentication or requiring biometric samples to be compared against stored templates "can pose serious privacy . . . concerns").

220. Steven Furnell and Konstantinos Evangelatos, *Public Awareness and Perceptions of Biometrics*, COMPUTER FRAUD & SECURITY 8, 12 (2007).

221. *See generally* Goodin, *supra* note 134 (describing how national identification systems can exacerbate the chances of impersonating those involved and allow for greater access to their data).

222. *See* NAT'L SCI. AND TECH. COUNCIL SUBCOMM. ON BIOMETRICS AND IDENTITY MGMT., THE NATIONAL BIOMETRICS CHALLENGE 23 (2011), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometricschallenge2011.pdf (discussing privacy, civil rights, and liberty protection).

223. *See generally*, Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, N.Y. TIMES (Feb 9, 2018) (noting that facial recognition technology faces more errors when determining the gender of darker skinned women).

224. *See generally* Bellovin, *supra* note 203 (noting the varied and important uses to which SSNs serve, and the difficulties that amending the SSN system would face).

use in the U.S.[225] This Article has already discussed the smart card solution in Section B, therefore, this Section will consider another possession-based authentication method—the magnetic strip card.

The magnetic strip card is a common form of authentication that has many of the same properties as a smart card which makes it desirable for the same reasons, including their usability, backward compatibility and error tolerance.[226] However, the magnetic strip card's security properties are far weaker.[227] Most notably, the lack of a secure co-processor requires that during any transaction, the secret stored in the card would be exposed to the reader.[228] This poses immense security vulnerabilities, as any malicious reader could allow for the theft of the secret and its usage by a malicious actor.[229]

Generally, one drawback of relying on *something you have* is that the token cannot be easily shared amongst multiple parties. In the case of magnetic stripe cards, it would be hard to copy the card and give it to a trusted party to use on one's behalf if needed.[230] It would also be impossible to ever revoke the token, because one could not be sure that the trusted party did not create any additional copies.[231] More importantly, sharing the token with a third party is not a desired property of a solution in this context.[232] Furthermore, if it became a requirement, the certificate infrastructure presented in this Article could easily be extended to allow sharing by using an individual's card to provision a certificate for the party the individual desires to share his or her token with.[233] This method of sharing could also be easily revoked—a property that is not present with *something you know* or *something you are*.[234] Therefore, for the particular problem of SSN theft, *something you have*, is the superior form of authentication.

H. System Design Summary

The Sections above presented a system design that meets the unique challenges presented by Social Security numbers. The system meets the design

225. *See infra* Section H (further discussing the design goals of the SSN supplement).

226. Magnetic strip cards, such as credit cards, are a very familiar and widely used technology in the US. Infrastructure for their usage exists widely and procedural mechanisms around their secure management are well developed. *See also* NAT'L RESEARCH COUNCIL, *supra* note 12, at 110.

227. *Id*.

228. *Id*.

229. *See id.* at 110–111 (noting the danger that compromised readers could be used to obtain secrets from magnetic strip cards).

230. *See id*. at 111 (pointing out that the security risks inherent in magnetic strip cards militate against copying or sharing the card, hence adding to the costliness of their usage).

231. *See id*. (recounting steps that the New York Metropolitan Transportation Authority had taken to ensure that magnetic strip cards were not being copied and pointing out the costliness and invasiveness of these measures).

232. *See supra* Section 1 (as the certificate infrastructure has to deal with supplementing SSNs, the feasibility of sharing the token is not desirable).

233. *See supra* Section III.A.2 (arguing that the proposed system would allow for the legitimate use of documents by parties that the individual desires to share his or her token with, and the protections against abuse by such parties).

234. *See supra* Section 2 (pointing out the ease with which compromised certificates could be revoked and replaced).

goal of being *modern* because it offers users the option of using their own devices, but also fulfills the design goal of being *universally accessible* because it does not require them to do so. It relies on smart cards, a *breach resistant, cheap,* and *boring* commodity technology that is *easy to use* by not predicating security upon the willingness of users to learn new behaviors. The design offers *backward compatibility* by not attempting to change the Social Security number in its existing role as an identifier. It provides *error tolerance* through processes for deactivating compromised cards and issuing replacements.

Most importantly, it *respects privacy* by including only the features necessary for authentication—preventing use as a means of identification.

IV. IMPLEMENTATION

This Part discusses possible avenues for implementing the proposed system more widely. Section A discusses necessary aspects of a Pilot Program. Section B comments on the economic feasibility of the program. Section C applies the concepts in Part III to a concrete scenario—Federal Student Aid—to understand the solution as applied to a segment of U.S. society. Finally, Section D explores the challenges and benefits of broader implementation.

A. Pilot Program

A pilot program is a prudent and necessary first step that will provide critical information needed to effectively and efficiently implement the system proposed in Part III. One need only look at the roll out of *Healthcare.gov* to understand the importance of testing a system of this scale before unveiling it nationwide.[235] In the case of *Healthcare.gov*, only six people in the country were able to select health plans on its first day of operation,[236] causing massive embarrassment and, more importantly, lack of confidence in the system.[237] Launching a pilot program prior to roll out will serve as a method to gain empirical data to forecast future costs, ease of adoption, and ability to scale, as well as to provide an opportunity to address potential security flaws.[238]

The pilot program will be a learning exercise during which the system can be tested from both a technical and policy standpoint, while still providing value. It is essential to discover and resolve any usability and security flaws in the system before full-scale deployment for the system presented in this Article. Any security breach of a system designed to provide increased security would

235. Amy Goldstein, *HHS Failed to Heed Many Warnings That Healthcare.gov Was in Trouble*, WASH. POST (Feb. 23, 2016).

236. *Id.*

237. Kate Pickert, *Americans Losing Faith in Obamacare*, TIME (Oct. 22, 2013) http://swampland.time.com/2013/10/22/americans-losing-faith-in-obamacare/.

238. *See generally* Goldstein *supra* note 236 (arguing that unresolved issues with *Healthcare.gov* were ignored as the site was being launched, suggesting that a pilot program may have made these issues manifest to those responsible for the site).

undoubtedly undermine confidence in the program and harm adoption rates.[239] Usability being a key property of good security, it will be crucial to ensure that people across all demographics can use the system easily.[240] It will also be crucial to measure the efficacy of the adoption strategies across different demographics, especially the younger generations who, having little credit history, are particularly susceptible to identity theft.[241] Through the pilot program strategies can be refined to promote adoption among the groups described. In addition, other vulnerable demographics could be targeted to ensure that those most at risk are introduced to the system and understand how the technology will protect them from fraud.[242] The pilot will also be used to verify that the program will impose the least amount of burden necessary to enroll.[243]

B. Economic Feasibility

Identity theft has continued to grow over the past decade.[244] In 2016 alone, identity theft cost consumers more than $16 billion, approximately a $1 billion increase from the year before.[245] Estimating the cost of implementing this program is an extraordinarily difficult task.[246] Given that this program depends on well-established technology, cheap hardware,[247] and solves a large portion of the identity theft problem, pursuing such an estimate is worthwhile and will

239. *See* Pickert *supra* note 238 ("The harder the exchange websites are to use—or the harder consumers think they are to use—the less likely people are to log on or sign up.").

240. Aaron Smith, *Older Adults and Technology Use*, PEW RES. CTR. (Apr. 3, 2014), http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/.

241. Susannah Snider, *How to Protect Yourself from Identity Theft*, U.S. NEWS (Jan. 26, 2018, 9:00 AM), https://money.usnews.com/money/personal-finance/articles/2015/01/13/5-prime-target-groups-for-identity-thieves.

242. *See generally* Smith, *supra* note 241 (pointing out the factors that make interfacing with digital devices difficult for seniors, and changes that digital literacy causes in seniors' opinions about the given technologies).

243. *See* Pickert, *supra* note 238 (arguing that increasingly negative attitudes towards the Affordable Care Act may be attributable to the difficulty of enrolling in health care plans through Healthcare.gov).

244. Javelin, *supra* note 9.

245. Kelli B. Grant, *Identity Theft, Fraud Cost Consumers More Than $16 Billion*, CNBC (Feb. 1, 2017, 9:11 AM), https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

246. Making such an estimate would be a project that requires a team of people and many weeks to complete. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO COST ESTIMATING AND ASSESSMENT GUIDE (2009) https://www.gao.gov/new.items/d093sp.pdf (noting the difficulties inherent in determining the costs of such programs).

247. A primary cost driver of the program is the manufacture and distribution of cards. Smart cards cost about $0.50 per card, scaled to include the entire US population of 330 million, would result in a cost of $165 million. SANDRA L. COLBY & JENNIFER M. ORTMAN, U.S. CENSUS BUREAU, PROJECTIONS OF THE SIZE AND COMPOSITION OF THE U.S. POPULATION: 2014 TO 2060 2 (2015), https://census.gov/content/dam/Census/library/publications/2015/demo/p25-1143.pdf; *Blank Chip Cards*, DHGate.com, https://www.dhgate.com/wholesale/blank+chip+ cards.html. Another relevant cost is that of the card readers. According to the Bureau of the Fiscal Service at the Department of Treasury, in 2015 when the U.S. Government conducted EMV implementation, the EMV card terminal "cost agencies $314 apiece," plus $8–15.00 shipping per terminal, and installation support of $73. BUREAU OF THE FISCAL SERV., U.S. DEP'T OF TREASURY, FISCAL SERVICE GOVERNMENT-WIDE IMPLEMENTATION OF EMV CHIP & PIN AT THE POINT-OF-SALE FREQUENTLY ASKED QUESTIONS 4 (2015), https://fiscal.treasury.gov/files/cas/FS_ EMV_FAQs.pdf.

result in a clear verdict: implementing this program will be extremely favorable from an economic standpoint.

C. Applying the Solution to Federal Student Aid

This Section describes why the solution proposed is both practical and applicable to federal student aid programs. It examines the current security measures for the application processes and how they could be strengthened through the proposed scheme. Furthermore, it considers methods to expand outreach as wide as possible among the US student base seeking loans. Lastly, it inspects the legal statues surrounding the federal student aid program and what modifications, if any, need to be made to employ the solution.

Applying the solution to federal financial student aid gives insight into the solution and the potential challenges it might face. Within the context of federal student aid, the new card system would be practical, as well as legally and technically simple. All federal student aid is administered through the Free Application for Federal Student Aid (FAFSA).[248] The application has a widespread impact on college and graduate school-aged students: in the 2015–2016 cycle over 19 million people submitted a FAFSA application.[249] Implementing the new card in the context of this system would ensure that a large portion of the under-30 U.S. population is given a card.[250]

From a technical perspective, applying card use would be relatively simple given that FAFSA is the single application used to apply for many different federal loans.[251] The application starts with a request for the person's date of birth, SSN, and full name, or Federal Student Aid (FSA) ID.[252] After this point card use would not be required, because the additional burden of authorization for every sign-in would not outweigh the costs.[253] After the student has filled in all the required information, FAFSA requires that a student create a FSA ID to

248. Also known as Title IV aid, this includes, Federal Direct Stafford loans, Federal Direct Parent PLUS loans, Federal Direct Graduate PLUS loans, Federal Perkins loans. Higher Education Act of 1965, 79 Stat. 1219.

249. *FAFSA Volume Reports*, FED. STUDENT AID, https://studentaid.ed.gov/sa/about/data-center/student/application-volume/fafsa-school-state (scroll to FAFSA Data by Demographic Characteristics; select 2015–2016 Application Cycle: finding exactly 19,757,764 people).

250. *Id.*

251. Also known as Title IV aid, this includes, Federal Direct Stafford loans, Federal Direct Parent PLUS loans, Federal Direct Graduate PLUS loans, or Federal Perkins loans.

252. *Login*, FED. STUDENT AID [hereinafter *Login*], https://fafsa.ed.gov/FAFSA/app/fafsa?locale=en_US (last visited Feb. 27, 2019).

253. While the information in the application is sensitive, such information will not be useful to an identity thief after the full implementation the card. For instance, in 2017 the tax information in FAFSA accounts were used to file fraudulent tax returns. *See* Danielle Douglas-Gabriel, *Identity Thieves May Have Hacked Files of Up to 100,000 Financial Aid Applicants*, WASH. POST (Apr. 6, 2017) https://www.washingtonpost.com/news/grade-point/wp/2017/04/06/identity-thieves-may-have-hacked-files-of-up-to-100000-financial-aid-applicants/. Once tax returns also require the new social security card for authentication, the information that can be potentially gathered on FAFSA will no longer be a problem. In the meantime, the added burden of using a card, or scanning a phone, each time a student logs into the FAFSA would prove very heavy. Studies show that the complexity in the FAFSA program is a barrier to low income students who would like to attend college. *See generally* Susan Dynarski & Mark Wiederspan, *Student Aid Simplification: Looking Back and Looking Ahead*, 65 NAT'L TAX J. 211 (2012) (providing a five-year retrospective of what has changed in the aid application process).

sign and submit the application.[254] Creating an FSA ID requires the same information as FAFSA: full name, date of birth, and SSN.[255] If a student forgets their FSA ID, they can answer security questions and receive a security code by SMS or an email to reset the password.[256] The FSA does not provide much added security, only an additional burden.[257] The card (or phone authorization) presented in this paper and the student's Social Security number will replace the FSA ID as the method of signing and authentication. Upon the submission of the application, the student will sign the application with their card or phone to complete the submission process.

Each student would need to apply for a card. The process is simple, but still an additional burden. Studies show that the complexity of FAFSA can be a barrier to low income students.[258] Yet the use of the FSA ID demonstrates the need for additional security in order for the FAFSA program to operate correctly.[259] The new Social Security card may create an initial burden but will provide a future benefit. After the initial pilot phase, the card will be used for other services, such as filing taxes and obtaining government benefits. Those who already own the new card will be prepared to use it when it is applied to these other services.

Another potential practical barrier is authenticating the FAFSA submission. Students will have the option of using an authorized smartphone, purchasing a reader, or going to a library computer and reader to electronically authorize the transaction. This is a potential concern because according to Pew Research, "[r]oughly three-in-ten adults with household incomes below $30,000 a year don't own a smartphone."[260] In addition, one-fifth of adults in "households earning less than $30,000 a year were 'smartphone-only' internet users—meaning they owned a smartphone but did not have broadband internet at home."[261] FAFSA already poses a burden in this regard, because it is an online application.[262] Providing communities with access to readers at local libraries can greatly mitigate this gap, given that 45% of library users ages 16 to 29 use libraries to connect to the web.[263]

---

254. *Create a New FSA ID*, FED. STUDENT AID, https://fsaid.ed.gov/npas/index.htm (last visited Feb. 27, 2017).

255. *Id.*

256. *Id.*

257. Kim Clark, *New FAFSA Security Rules Cause Hassles For Some College Aid Applicants*, MONEY (Jan. 22, 2016), http://time.com/money/4191342/fafsa-security-hassles.

258. *See* Susan Dynarski & Mark Wiederspan, *supra* note 254, at 230 (finding that the "effect of a simplified application on college attendance rates was comparable to that of offering an applicant thousands of dollars in grant aid.").

259. *See Login*, *supra* note 253 (illustrating the type of information that FAFSA requires of its applicants).

260. Monica Anderson, *Digital Divide Persists Even As Lower-Income Americans Make Gains in Tech Adoption*, PEW RES. CTR. (Mar. 22, 2017), http://www.pewresearch.org/fact-tank/2017/03/22/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption.

261. *Id.*

262. *See Login*, *supra* note 253 (explaining what is needed for a new FAFSA application).

263. John B. Horrigan, *Library Usage and Engagement*, PEW RES. CTR. (Sept. 9, 2016), http://www.pewinternet.org/2016/09/09/library-usage-and-engagement.

Legally, implementing the card may create some difficulties. A global legislative change that defines use of a Social Security number to include authentication with the new card would not be a viable solution. For example, in the case of federal financial student aid regulation, loan administrators pass documents between one another and use the SSN as an identifier.[264] Such "backend" uses to match records should not require the card to be present.

On the other hand, legal implementation in the context of FAFSA would not require additional regulation or legislation. 20 U.S.C. § 1091 provides that, to receive "any grant, loan, or work assistance," a student must file an application with their SSN.[265] This statute requires a minimum amount of other information as well, but it does not set a maximum limit to what the Secretary of Education may request in connection with FAFSA.[266] Therefore, at first glance it appears that no further legislative change is needed to § 1091.[267] The Privacy Act of 1974, however, may prove a barrier. It provides that "[a]ny Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."[268] Arguably, the addition of the social security card would not require additional explanation in § 1901 for two reasons: (1) § 1901 already complies with the Privacy Act of 1974 when it requires SSN use, and (2) the card is not the equivalent of the actual "social security number," rather it is a technical means of authenticating that the person using the number has the authority to do so.[269]

At the regulatory level, the Department of Education already requires that the "Secretary attempt[] to confirm the social security number a student provides on the Free Application for Federal Student Aid (FAFSA) under a data match with the Social Security Administration."[270] Further regulation provides that the time it takes to verify should not stall the application process for the student.[271] This suggests that such verification is a burden to the agency. However, the new card will become the almost instantaneous means of authenticating the use of the student's SSN, streamlining the process.

In sum, deploying the system presented here in FAFSA will have many positive implications for FAFSA applications. Furthermore, the FAFSA context provides a legal and technical environment that demonstrates this system will fit into with ease.

---

264. 34 C.F.R. § 681.56 (2018) (requiring "each school must maintain an accurate, complete, and easily retrievable record with respect to each student who has a HEAL loan" including their SSN). *See also* 34 C.F.R. § 370.49 (2018) (requiring designated agencies to disclose social security numbers if the Secretary requests).

265. 20 U.S.C. § 1091(a)(4)(B) (2018).

266. *Id.*

267. *Id.*

268. Privacy Act of 1974, 93 P.L. 579, 88 Stat. 1896 § 7(b).

269. 5 U.S.C. § 552a (2018).

270. Social security number, 34 C.F.R. § 668.36 (2018).

271. 20 U.S.C. § 1091(p)(1) (2016) ("[A]n institution shall not deny, reduce, delay, or terminate a student's eligibility for assistance under this part because social security number verification is pending.").

D. Broader Adoption Strategy

The broader adoption strategy explores expansion of the program after proof-of-concept to the public. The approach depends on two different, but concurrent methods of growth to achieve rapid implementation: one through the public sector and other through the private sector. These approaches are informed through learnings gleaned from similar examples where institutions faced comparable challenges in harnessing incentives.[272]

The adoption strategy for the new card can broadly be described by a two-pronged approach: (1) focusing on getting individuals the new cards and (2) convincing relevant private sector entities to adopt the authentication procedure. With this methodology, the proposal can effectively lay the groundwork to standardize this procedure and reduce the threat of fraudulent transactions linked to identity theft. At the individual level, the plan is to leverage individual's interactions with the federal government to execute this new program, starting with federal employees and then seeking additional relationships to mandate adoption. To encourage implementation within the private sector, the Article's recommendation is to alter regulations within key industries, such as commercial banking, to align market forces so firms are economically incentivized to strengthen the authentication process.

1. Federal Employee Mandate

In FY 2016, the total number of federal civilian employees working for the United States government was over 2 million.[273] Although this accounts for less than 1% of the American population, mandating that all executive branch employees adopt the card will provide ample opportunity to expand the experimental group to further test the authentication procedure for a more diverse user base, as well as integrate the system into government functions.[274] Greg Touhill, the first Federal Chief Information Security Officer (CISO), estimated that the 2014 data breach at the OPM could cost the government over $1 billion in identity theft protection fees over the next decade.[275] Thus the potential savings in shifting from active monitoring to a stronger authentication method is significant and provides a strong rationale for implementation.

Execution of this mandate would be logistically straightforward. The Office of Management and Budget (OMB) is the executive branch agency that serves to implement the directives of the President and is broadly tasked with

272. *Id.*

273. U.S. OFFICE OF PERS. MGMT, SIZING UP THE EXECUTIVE BRANCH: FISCAL YEAR 2016 4 (2017), https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/sizing-up-the-executive-branch-2016.pdf.

274. *Id.*

275. Chris Townsend, *OPM Breach Costs Could Exceed $1 Billion*, SYMANTEC: SYMANTEC OFFICIAL BLOG (Mar. 23, 2017), https://www.symantec.com/connect/blogs/opm-breach-costs-could-exceed-1-billion.

enforcing the regulatory policies that span across the federal government.[276] Through an executive order, the President can task the OMB Director to alter regulations to stipulate that all federal employees must adopt the new system of authorization for the purpose of enhanced security.[277] Under this change, all existing and future federal workers would be required to confirm their identity with their relevant government agency, necessitating that individuals acquire the new card to authenticate. Even though this may appear burdensome, the new card will benefit federal employees by mitigating the threat of identity theft, as the process of authentication stops malicious actors from approving fraudulent transactions with a few key pieces of information.

2. Expansion into the General Public

Large-scale adoption and roll out of such a program is not without precedent. India's Aadhar system issued its first number in 2010[278] and by March 2017 the system will be required to be linked to 139 services including bank accounts, SIM cards, and PAN (similar to the TIN).[279] India has a population of 1.3 billion with 67% living in rural areas[280] yet was able to cover 99% of citizens over the age of 18 with the new system[281] by 2017. Part of its adoption strategy included tying the new system to the receipt of subsidies and services by the government to create incentives for citizens across different socioeconomic statuses.[282] A subsequent initiative will attempt to phase in financial institutions by March.[283] Drawing from these examples can help develop scaling strategy.[284]

As part of the initial effort to expand the program to the public, it is critical that individuals and corporations both understand what the new authentication system does and does not do. It is essential that the U.S. government utilizes available tools to inform the public on how the new card works and in what situations it can be used. In this instance, it would be ideal to use the resources

276. *About Office of Management and Budget*, FED. PRIVACY COUNCIL, https://www.fpc.gov/resources/omb (last visited Feb. 27, 2019).

277. Comprehensive Plan for Reorganizing the Executive Branch, 82 Fed. Reg. 13959 (Mar. 13, 2017).

278. *About UIDAI*, UNIQUE IDENTIFICATION AUTH. OF INDIA [hereinafter *About UIDAI*], https://uidai.gov.in/about-uidai/about-uidai.html (last visited Feb. 27, 2019).

279. Krishnadas Rajagopal, *Deadline for Aadhaar Linking To Be Extended to March 31*, HINDU: BUS. LINE (Dec. 7, 2017), http://www.thehindubusinessline.com/news/centre-willing-to-extend-aadhaar-linking-deadline/article9985238.ece.

280. *Rural Population (% of Total Population)*, WORLD BANK, https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS (last visited Feb. 27, 2019).

281. Mahendra Singh, *99% of Indians Over 18 Now Have Aadhaar Cards*, TIMES OF INDIA (Jan. 28, 2017, 4:06 PM), https://timesofindia.indiatimes.com/india/99-of-indians-over-18-now-have-aadhaar/articleshow/56820818.cms.

282. Dhaval Kulkarni, *Link Your LPG Connection to Aadhaar or Bank A/C to Keep Getting Subsidy*, DNA (Jan. 2, 2015, 7:30 AM), http://www.dnaindia.com/mumbai/report-link-your-lpg-connection-to-aadhaar-or-bank-ac-to-keep-getting-subsidy-2048799; Devika Banerji, *In Convergence Push, NREGA Card to Carry Aadhar Number*, ECON. TIMES (May 2, 2012, 2:54 AM), https://economictimes.indiatimes.com/news/economy/policy/in-convergence-push-nrega-card-to-carry-aadhar-number/articleshow/12957318.cms.

283. As a primary entity, not a secondary entity like in the example of receiving subsidies.

284. The original role out of the SSN itself in 1936 serves as an additional example.

available at the Consumer Finance Protection Bureau to educate individuals on how adopting this new technology will better protect them from identity theft.

Additionally, the National Institute of Standards and Technology (NIST) within the Department of Commerce would be a prime conduit to provide transparency on the underlying technology of the card, emphasizing the minimal collection of PII and strong security.[285] NIST will also develop the technical specification and a reference implementation of the smart card and reader to make adoption cheaper and faster, and to prevent implementation errors.

Based on India's experience with the Aadhar model, the primary strategy for expansion would be to attach the program to recipients of Social Security benefits.[286] In 2015, there were 65.1 million Americans that received benefits from the SSA, 5.4 million of which were new beneficiaries.[287] Moreover, authentication can be an effective method to cut down on fraudulent claims or other means to abuse the system.[288] SSA is ranked third for government agencies that administer improper payments, filing an estimated $9.8 billion in incorrect expenditures in 2015 alone.[289] By having recipients authenticate themselves each year to obtain their benefits, the government can add an additional layer of accountability that can cut down on graft, addressing a bipartisan concern.

Ultimately, the U.S. government must move to apply this system within the IRS for all who file their taxes, including dependents and spouses filing jointly. This implementation method offers the best opportunity to reach the largest segments of the general population to adopt the new authentication process.

To account for individuals who are not technologically savvy or do not own smartphones, easy public access to readers can be provided. The 31,324 post offices[290] will serve as hubs with readers that allow users to use their cards in a trusted location. As the plan scales to the wider public, readers will be provided to public libraries and community colleges to further provide access to individuals who would otherwise be disenfranchised by this scheme. Finally, the SSA would publish user guides to assist those who have difficulties using the new card.

---

285. *See generally National Institute of Standards and Technology*, NORTHWESTERN UNIV., https://www.northwestern.edu/standards-management/collaborators/organizations/nist.html (last visited Feb. 27, 2019) (finding NIST promotes standards that enhance economic security).

286. *See About UIDAI*, *supra* note 279 (describing the objective of issuing a unique identification number that prevents fake and duplicate identities and is easily verified).

287. *Fast Facts & Figures About Social Security, 2016*, SOC. SEC. ADMIN., https://www.ssa.gov/policy/docs/chartbooks/fast_facts/2016/fast_facts16.html (last visited Feb. 27, 2019).

288. Brian Krebs, *Social Security Administration Now Requires Two-Factor Authentication*, KREBSONSECURITY (Aug. 1, 2016), https://krebsonsecurity.com/2016/08/social-security-administration-now-requires-two-factor-authentication/comment-page-2 (last visited Feb. 27, 2019).

289. Jim Prodasco, *Social Security Fraud: What Is It Costing Taxpayers?*, INVESTOPEDIA (Dec. 5, 2016, 2:18 PM), https://www.investopedia.com/articles/retirement/120516/social-security-fraud-what-it-costing-taxpayers.asp.

289. *Id.*

290. *About: Size and Scope*, U.S. POSTAL SERV., https://about.usps.com/who-we-are/postal-facts/size-scope.htm (last visited Feb. 27, 2019).

3. Private Sector Adoption

There are two mechanisms used in the adoption of the new technology in the private sector: leveraging existing technology and leveraging risk. Credit cards currently deploy a chip mechanism to prevent fraud from compromised points of sale devices.[291] As of June 2018 there have been 1.7 billion Visa EMV transactions completed in the U.S. alone.[292] A 2013 survey released in 2015 by the Federal Reserve Bank of Boston revealed that 70% of consumers had at least one credit card.[293] Although leveraging private sector corporations, such as banks, to deploy this new system to Americans would be efficient and easily scalable, it presents a significant risk. An important principle in systems security is to isolate valuable data stores from each other.[294] This deployment strategy would run directly contrary to this principle.[295]

To scale adoption beyond public sector employees and citizen interactions with the U.S. government, it would be prudent to leverage market mechanisms and crystallize the risk to commercial entities. Precedent has been established in 2017 by credit card companies where, in most cases, the party that has not adopted the EMV card technology is liable[296] in an event of a fraudulent transaction. If all involved parties have adopted the new technology, then the liability of the fraud is on issuer of the card.[297] If the risk is not apparent to the financial institutions, the U.S. government can amend the CIP's risk-based procedures for verifying the identity of each customer[298] such that the identification number required (TIN)[299] will be the SSN instead. Considering the SSN often serves as the TIN[300], the new system for authentication via the new card would ultimately be more secure. Due to the way the card communicates the SSN with the requester, mandating that the SSN be provided ensures the most secure process.

Mandating that the SSN be provided by federal statute for financial institutions[301] means that the solution offered would not violate the Privacy Act

---

291. *Chip Technology Helped Reduce Card-present Counterfeit Payment Fraud by 82%*, VISA: SECURITY, https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html (last visited Feb. 27, 2019).

292. *Id.*

293. SCOTT SCHUH & JOANNA STAVINS, FED. RES. BANK OF BOSTON, THE 2013 SURVEY OF CONSUMER PAYMENT CHOICE: SUMMARY RESULTS 19 (2015), https://www.bostonfed.org/publications/research-data-report/2015/the-2013-survey-of-consumer-payment-choice-summary-results.aspx.

294. *See Basic Security Principles for Information Systems Development/Deployment*, UNIV. WATERLOO (Nov. 6, 2012), https://uwaterloo.ca/information-systems-technology/about/policies-standards-and-guidelines/security/basic-security-principles-information-systems#isolation (stating highly sensitive information should be isolated from public systems to reduce exposure from attack and manage flow and access of information).

295. *See infra* Section VI.B. (discussing *Alternative Designs Considered*).

296. U.S. PAYMENTS FORUM, UNDERSTANDING THE U.S. EMV LIABILITY Shifts 5 (2017) http://www.uspaymentsforum.org/wp-content/uploads/2017/07/EMV-Fraud-Liability-Shift-WP-FINAL-July-2017.pdf.

297. *Id.*

298. 31 C.F.R. § 1020.220(a)(2) (2018).

299. 31 CFR § 1020.220(a)(2)(i)(A)(4) (2018).

300. *Id.*; *see* sources cited *supra* note 26 (authorizing a state or state agency to require SSNs to administer any tax, general public assistance, or motor vehicle registration).

300. *See* sources cited *supra* note 26.

301. 31 U.S.C. § 5312(a)(2) (2018).

of 1974[302] by disclosing to the individual that (1) the disclosure is mandatory, (2) the SEC[303] under the Department of Treasury will be the authority that authorizes the solicitation as a federal functional regulator[304] and (3) the SSN will be used for anti-money laundering and anti-fraud programs.

V. CONCLUSION

The Article outlines a proposal to implement an authentication method to enhance security, while maintaining the current structure of how SSNs are used, to mitigate the threat of identity theft. This Article proposed a method for securing the use of SSNs, then explored some of the initial legal and policy issues that would arise from employing such a system. Future work will comprehensively address additional considerations in the policy, legal, and technical realm that were not in the immediate purview of this Article. These include secondary effects of implementation, such as the impact on undocumented workers, and additional examples of how the card could be applied in different use cases. Future work could also analyze the cost of each implementation stage. Regardless, the proposal lays groundwork that covers the major issues that would arise in crafting and executing an authentication mechanism to prevent SSN-based identity theft.

302. Use and Disclosure of Social Security Numbers, 31 C.F.R. § 1.32(b)(1) (2018).

303. 31 C.F.R. § 1010.100(r) (2018) (providing "(1) The Board of Governors of the Federal Reserve System; (2) The Office of the Comptroller of the Currency; (3) The Board of Directors of the Federal Deposit Insurance Corporation; (4) The Office of Thrift Supervision; (5) The National Credit Union Administration; (6) The Securities and Exchange Commission; (7) The Commodity Futures Trading Commission" as federal functional regulators, among these, the SEC seemed to have the most "teeth").

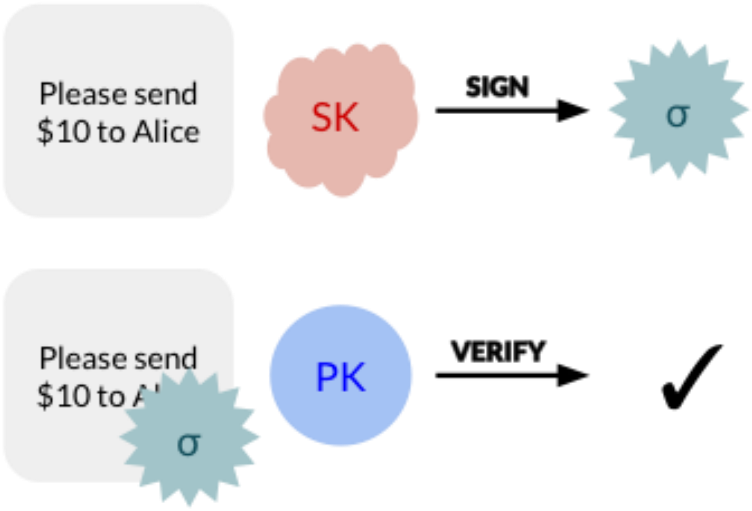
304. *Id*.

VI. APPENDIX

A. Cryptography Primer: Signatures & Certificates

This Section provides the technical background on public key cryptography, also known as asymmetrical cryptography.

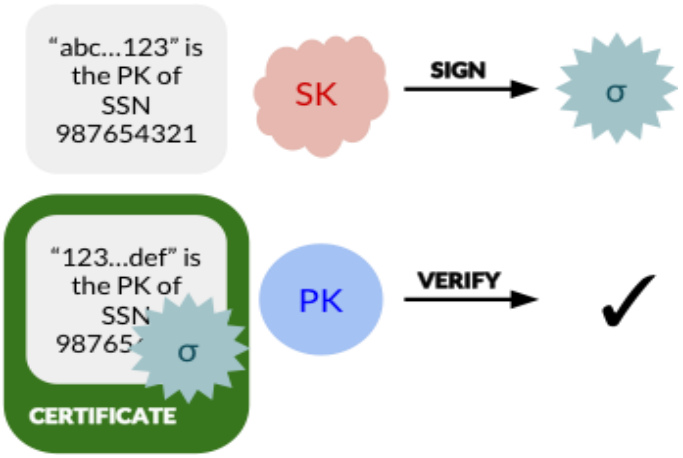
In the public key signature scheme, each user holds two keys.[305] The public key (PK) is widely known, while the secret key (SK) must be known only to the user.[306] Only the secret key holder can produce a signature (σ).[307] But anyone can verify the signature's authenticity using the public key.[308]



The signature scheme described above assumes that every recipient already knows every possible sender's public key.[309] If a system has many users, this is impractical to achieve in practice.

To work around this problem, all users could trust some central authority, who verifies the real-world identity associated with every public key.[310] Upon verifying a public key, the authority signs a message attesting to the identification, more commonly known as a certificate.[311]

305. Tiffany A. Mendez, *Adopting the Digital Signature Guidelines in Implementing Public Key Infrastructure for Federal Procurement of Electronic Commerce*, 29 PUB. CONT. L.J. 285, 290–91 (2000).
306. *Id.*
307. *Id.* at 292.
308. *Id.* at 293.
309. *See id.* at 290–91 (describing public key cryptography).
310. *Id.* at 291–92.
311. *Id.*



Recipients only need the public key of the central authority.[312] With the authority's public key, the recipient can verify whether the authority has certified the identity behind the sender's public key.[313]

B. Alternative Designs Considered

1. Federated Card Issuance

Banks already issue EMV payment cards with similar chips,[314] so at first glance, it seems reasonable to make them federated providers of the cards. This architecture was not chosen for several reasons.

Asking banks to become certificate authorities amounts to asking them to bear a substantial cost[315] to implement a system that has not yet been proven. They may propose to reduce costs by combining payment cards and the proposed Social Security cards. If payment cards also have the power to approve loans and file taxes, then the theft of a wallet or purse now has a much greater chance of leading to identity theft.

Additionally, securing many banks' individual systems would be much more difficult than securing a single system run by the SSA.

312. *Id.* at 293.

313. *Id.*

314. *See* Taylor Tepper, *Here's Why Your Credit Card Now Has a Chip and Why You Should* Care, MONEY (Sept. 28, 2015), http://time.com/money/4040808/credit-card-chip-fraud-emv (finding credit cards with chips became widespread in 2015).

315. Running a properly secured certificate authority costs at least a few million dollars per year. *See* Josh Aas, *Looking Forward to 2018*, LET'S ENCRYPT (Dec. 7, 2017), https://letsencrypt.org/2017/12/07/looking-forward-to-2018.html.