



Statement Before the
House Ways and Means
Subcommittee on Social Security

***“Securing Americans’ Identities: The Future of
the Social Security Number”***

A Testimony by:

James A. Lewis

Senior Vice President

Center for Strategic and International Studies

May 17, 2018

1100 Longworth House Office Building

Mr. Chairman and Mr. Ranking Member, I thank you and the Committee for the opportunity to testify. The Social Security Number (SSN) is the key identifier for the United States. In many ways, it is also out of date. The SSN is widely used for commercial purposes. The prime reason for this is that the SSN is a free credential that is unique to each individual, issued by a trusted source, and links records held in different private and government databases back to the same person. In reality, this makes the SSN indispensable.

The SSN is invaluable for businesses, but it is also invaluable for criminals. One estimate is that 60% to 80% of all SSNs have been stolen. SSN's can be bought in bulk in the cybercrime black market, along with other personal information. Since they are used not only to identify an individual, but to authorize online transactions, stolen SSNs or fake SSNs are a potent source of fraud and identity theft.

SSNs were never designed for online commerce. They were created in 1936, and originally intended only to link citizens to federal benefits. Over time, its use has expanded in both government and private transactions and it has been adopted for online use. SSNs still come on a paper card that is not intended to be either a credential or an identifier. Once stolen, the SSN is very difficult to be replaced. This makes the current SSN system ineffective for electronic commerce. While there have been good steps to let people verify SSNs, fraud is still possible. Modernizing the SSN is a good goal for action and there are several options for replacement.

What I will not discuss is a national ID system, however. I encourage the Committee to avoid going down this rabbit hole. The U.S. has made several efforts over the last twenty years to create a secure digital identifier, but each of these efforts has run into problems of complexity, cost, and privacy concerns. The authentication of identity online is an intricate process. Many smaller countries have solved the problem by creating national identity systems that lets people securely identify themselves online. These are often based on a National Identity card, but the U.S. is not ready for such a bold step.

The committee should avoid a discussion of authentication of identity online and instead focus on modernizing and strengthening the SSN, a more achievable goal that will in itself provide real benefits and reduce the risk of online fraud. Modernizing the SSN could be a first step toward better digital authentication in the U.S. The goal should be to provide citizens with the same level of service they would expect from a credit card company or a major online retailer.

In thinking about how to do this, we need to consider how to manage continuity, cost, and complexity in any new system. The most important aspect of this is that any modernization should not break the SSNs critical role as a unique national identifier. A modernized SSN would require decisions on several elements.

There are basically two approaches to reducing the risk of using the SSN as an identifier. The first is to strengthen the SSN to make it harder to steal or use fraudulently. The second is to reduce or eliminate its value as a credential. Moving to a more secure and modern SSN will be a difficult and complex transition. The central goals are to take advantage of the growth in internet connectivity that has occurred in the last decade and to model a modernized SSN on existing online systems and their safeguards. There are several decisions required on what course to take and what options to select. We can sketch out one path (among several) for SSN modernization.

The first step is to replace the paper SSN card with a “smart card,” a plastic card with an embedded integrated circuit (a “chip”), like the credit cards most of us carry. This is the solution adopted by credit card companies some time ago as a way to reduce fraud. Most people are familiar with this kind of card, which would ease the burden of both acceptance and transition for SSN holders.

Even if nothing else was changed, a smart card would be an improvement over the current paper card. A smart card provides the foundation - for use now or for later - to build a more secure system. If the Congress decided to take advantage of a smart cards additional capabilities, it could model a modernized SSN on the credit card system and its safeguards. When your card is stolen, your financial institution cancels the old one and issues you a new card number. You are still linked to your account, but not to the old credit card number.

SSA could use a similar approach. SSA should have some way to replace an SSN when it is compromised, since compromise is unavoidable. The added complexity is that a replacement SSN must preserve the ability to link multiple records to the same individual. There are ways to do this but they involve additional cost and responsibility for the SSA.

The SSN itself would not be used in commercial transactions. It would instead be used to generate a number associated with the SSN account. If this number was compromised, a new number could be generated using the SSN “root.” The SSN itself could be kept secret, encrypted, and the generation of the replacement number could be controlled by the SSA.

For example, the new smart card SSN could use a proxy number, a replaceable number linked to your SSN account. You would still be issued an SSN at birth, but it would not be made public. Instead, you would get a proxy number, stored on the new smart card and linked to your SSA account number. People are already familiar with this from credit card or debit card use. Your credit card has a number used to authorize transactions. It is linked to an account at a financial institution that has its own account number. This account number is linked to your SSN, for tax and verification purposes. When your credit card is stolen or compromised, you notify the card company, which generates a new credit card with a new number for you, linked to your account, whose number does not change.

For the SSN, this means the number on your SSA-issued smart card will not be your SSN. Instead, it will be a “proxy” number that links to your SSN. The proxy number could use a different format than the nine-digit SSN to avoid confusion, and the SSN itself would not be used for commercial purposes - this might require legislation to require companies to transition to the new system and to replace the SSN in their account with the new proxy number.

For this to work, merchants, banks and others who now use the SSN will need some way to verify that the proxy number links to a real SSN account. This means SSA will need some sort of verification process similar to that used by credit card companies. When you present your credit card, the number is automatically checked to see if the card has been reported stolen or if there are indications of fraud. An SSN verification system could build off existing verification systems already in use by SSA, where an employer submits an SSN to see if it is a real number, except now these systems would need to be expanded to confirm that the proxy number is linked to a real account. At some point in the future, SSA could even develop a mobile “app” for the verification process.

SSA currently operates two verification services that confirm the social security number and name for wage reporting purposes. If it was to move to a system similar to that used by credit card, it would need to first use the SSN issued at birth to generate another number (a “pseudo-SSN”) that could be used for identification purposes (and which could be replaced if compromised), and then adapt the existing verification system to allow people to check if the pseudo-SSN was still valid. SSA could develop additional measures (similar to those used by financial institutions) to identify possible fraudulent use. SSA would also need some system for citizens to report when their number has been compromised and needs to be replaced.

Exchanging a compromised proxy number would require a citizen going to SSA and requesting a replacement. Before issuing a replacement, SSA would need to verify that the request was legitimate. This requires some kind of process for the authentication of identity. The system that banks and online merchants use is multifactor authentication. This uses a “shared secret,” usually a password, and then some other some other secret to verify identity. Again, the transition burden would be reduced as many citizens are already familiar with these systems.

To replace an SSN, a citizen could call or log onto the SSA website. There are several different approaches to multi-factor authentication that could be used to ensure that the replacement request was legitimate. SSA could issue a PIN number with the smart card, and the PIN would need to be entered to request a new number. SSA could use the mobile texting system many banks and online service provider use, where you enter a request and then are sent a code to verify identity, such as with Gmail or Office 365.

SSA would need to assign a password to each account, and then take additional steps depending on what authentication method Congress chooses, whether it is a PIN, additional shared secret (like

asking user to identify the color of their first home) or to generate an authorization code. SSA would need the ability to receive a request, verify the password, and have on file an email address or phone number to which an authorizing code could be sent.

This sounds complicated, but hundreds of millions of commercial transactions are carried out every day using these systems. Congress needs to move the social security system into the 21st century. There are costs, however. Non-recurring costs include replacing paper cards with plastic smart cards, building an online account verification system at SSA, and the cost to firms and agencies to change their number used in existing accounts from the real SSN to the proxy. Recurring costs would include providing the verification service and the cost of regenerating a new proxy number.

Given the complexity of these systems, and the immense experience of the private sector in implementing them, Congress could choose to rely on private sector service providers to supply the smart card and the proxy number. Commercial vendors already have the “backroom” processes needed for this smart card approach. Private sector suppliers would still rely on SSA to create and hold the “real” SSN. This would reduce the burden on SSA, but raises the question of who pays for all this? Does SSA subcontract the issuance process to the private sector, should there be user fees (something almost certain to be unpopular, although we charge for passports and driver’s licenses), or should a new system be subsidized from general revenues.

The options are to have SSA do this, to contract to the private sector, or to piggy-back on the existing driver’s license issuance process (where states could either charge customers or be subsidized). States have not yet moved to smart cards, however, and an effort to mandate this would almost certainly run into opposition. Further debate is required to decide which might be best, but no modern system comes without cost.

One consideration to bear in mind is that in the past, interoperability has been the principal flaw in private credential systems. Countries with smaller populations face a lesser burden as they have fewer companies involved (often only three or four), but the UK, with a population of 65 million, found it difficult to implement a “federated,” private sector authentication system, as did the U.S. in the mid-2000s. A bad outcome would be a world where each individual required multiple credentials - this is one of the advantages of the SSN and a replacement system would have to duplicate this.

If the Congress chooses to let private sector entities issue an SSN-based credential, it will need to create incentives for companies to offer this service. Incentivizing consumers might require some kind of appropriate liability limitation, mirroring that used in the Fair Credit Billing Act. Congress will also need to develop privacy rules that restrict the ability of a private sector provider to “harvest” user data for commercial purposes.

Congress would need to set a transition period for the move to a smart-card based system, and it would have to create negative incentives for companies and individuals to move from the SSN to the proxy number, perhaps by forbidding SSN use perhaps by publishing SSNs, which would lower their value as an identifier. Publication would force companies to find an alternative solution and, judging from the Swedish and Norwegian experiences, could incentivize a market for private credentials. Private credential issuers could be required to meet identification standards such as HSPD-12 or NIST's SP 800-63 *Digital Identity Guidelines*.

The security risks of publishing SSN could be reduced after publication, by replacing SSNs with a proxy number and its more robust identity verification system. For citizens, they would receive a new smart card in the mail with a new proxy number, perhaps followed by separate mailings with the PIN needed to access their account. There are ways to automate the replacement process that could be developed to ease the transition burden. This smart card approach would permit the adoption of blockchain technology should blockchain ever mature to the point where large scale deployments are possible.

Simple publication of SSNs is the least expensive option for the Federal government and for the private sector and would create incentives to use something other than the SSN as an identifier (it would still need to work as an identifier for tax and benefits purposes). While creating a searchable database has associated costs for SSA, it would be cheaper than the annual cost of fraud and identity theft (an estimate in the economist pegs this at \$16 billion).¹

The effect would be to make the SSN more secret. If a consumer was notified of a data breach that compromised their proxy SSN, they could go to an SSA website and generate a new number. To request a new number, SSA would need to move to some kind of multifactor authentication such as that now used by many banks, so that a consumer requesting a replacement would need a password, a PIN, and an access number sent to their cellphone or email (this would have to be the cellphone of a parent or guardian for minors).

This approach would retain the SSNs critical function as a unique identifier of an individual while providing some way to replace an SSN when it has been compromised - and compromise is unavoidable. The goal, as many have said is to separate the SSN as an identifier from its use as an authorizer.

I have not discussed a public key infrastructure or federated identity system. Having been deeply involved in earlier federal effort to create PKI or federated identity systems, I believe they are too complex and costly to be successfully implemented. Perhaps the best argument for this smart card approach is that we already use it on a massive scale, for credit or debit cards or for online accounts.

¹ <https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-be-charge-their-own-personal-data-right>

Companies and citizens are familiar with it. Implementation by SSA would be difficult, but we have the advantage of knowing that the technology and processes already work.

Thank you for the opportunity to testify on this subject and I look forward to your questions.