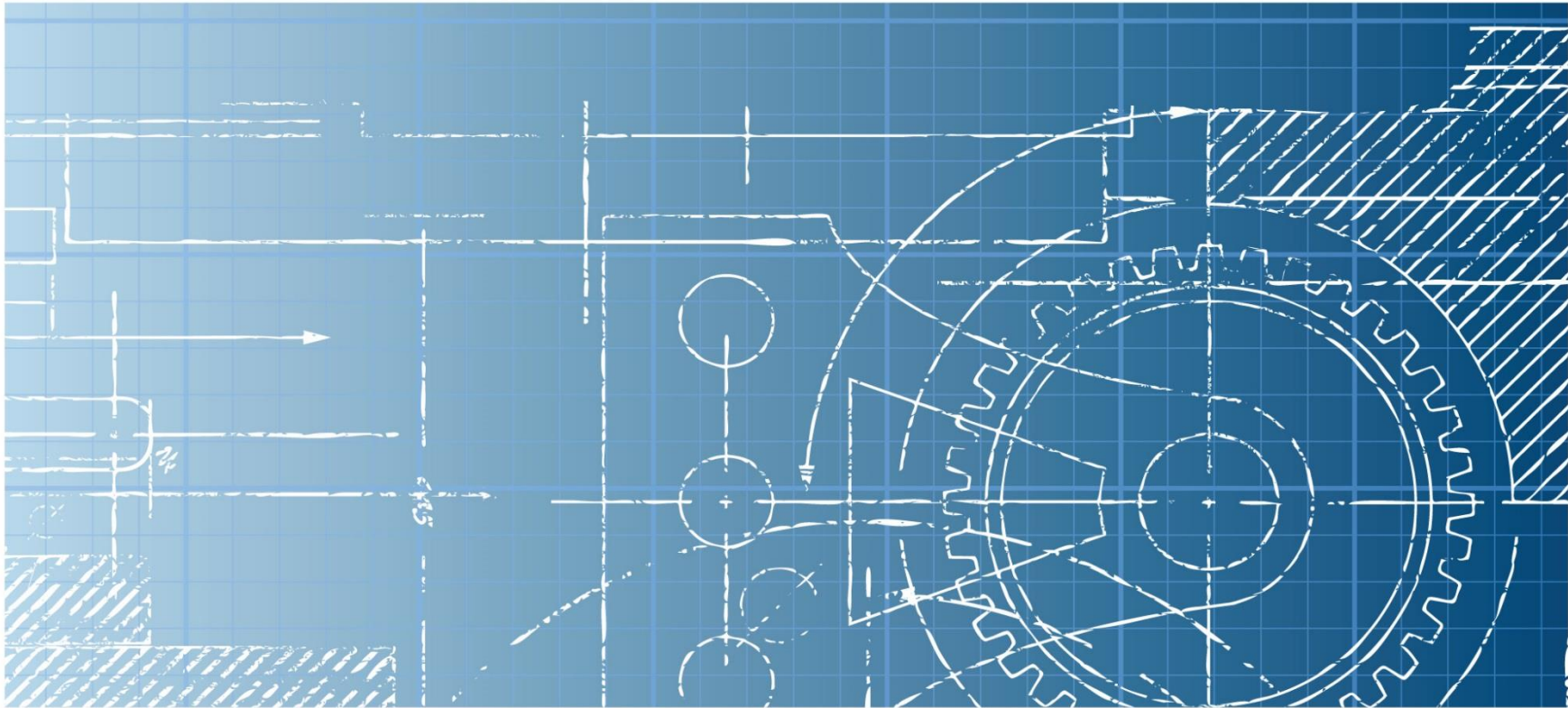


Better Identity in America: A Blueprint for Policymakers



THE BETTER IDENTITY COALITION

About the Better Identity Coalition

- Focus: developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication.
- Launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity.
- As government contemplates new policies to improve the quality of digital identity, the Better Identity Coalition is bringing together leading companies to help develop innovative ideas that improve security, privacy, and convenience for all Americans.

Some background

Equifax reveals vast scale of 2017 consumer data breach

Some 145 million customers' Social Security numbers were stolen, company says

Jeremy B White San Francisco | Tuesday 8 May 2018 18:24 | [0 comments](#)



Security

IRS breach highlights weakness of 'knowledge-based' security

By Zach Noble May 27, 2015

The compromise of 100,000 taxpayer accounts through the Get Transcript application on the IRS website were not random hacks, but the exploits of an already-publicized vulnerability -- known to security experts since at least March.

And, in order to gain access, hackers already had a good deal of information on the affected taxpayers.

Hackers already had the keys



Some background



The screenshot shows a Bloomberg Politics article. The header includes the Bloomberg Politics logo and navigation links for Markets, Tech, Pursuits, Politics, Opinion, and Businessweek. The article title is "The White House and Equifax Agree: Social Security Numbers Should Go". The byline is "By Nafeesa Syeed and Elizabeth Dexheimer". The date and time are "October 3, 2017, 2:50 PM EDT" and "Updated on October 3, 2017, 7:15 PM EDT". Below the article title, there are two bullet points: "→ Administration exploring new tech for personal identifiers" and "→ Ex-Equifax CEO tells Congress relying on numbers outdated".

The White House and Equifax Agree: Social Security Numbers Should Go

By **Nafeesa Syeed** and **Elizabeth Dexheimer**
October 3, 2017, 2:50 PM EDT Updated on October 3, 2017, 7:15 PM EDT

- Administration exploring new tech for personal identifiers
- Ex-Equifax CEO tells Congress relying on numbers outdated

McHenry Introduces the PROTECT Act in Response to Equifax Breach

Washington, October 12, 2017 | 0 comments



Today, Chief Deputy Whip Patrick McHenry (R, NC-10), the Vice Chairman of the House Financial Services Committee introduced **H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017, or the PROTECT Act.**

Following the data breach at Equifax that exposed the personal data of over 140 million Americans, this bill would require the federal government to create uniform cybersecurity standards for credit bureaus and submit them to onsite examinations. The bill would also create a national framework for credit freezes so that victims of identity theft, active military personnel, people over 65 years of age, and children are protected. Finally, the bill would stop the credit bureaus from using Americans' Social Security Numbers as a basis for identification by 2020.

"The Equifax data breach has harmed my constituents in western North Carolina and Americans across the country," said McHenry. "It exposed a major shortcoming in our nation's cybersecurity laws and Congress must act. The bill I've introduced today takes an important first step in providing meaningful reforms to help Americans who have been impacted by this breach. It is focused on prevention, protection, and prohibition.

"It prevents future harm to all Americans by requiring the largest credit reporting agencies to be subjected to the same standards and supervision as the rest of the financial industry," McHenry continued. "It protects Americans by creating a national credit freeze that actually works. Finally, it prohibits the largest credit reporting agencies from continuing to rely upon the most sensitive of Americans' personal information: our Social Security Numbers."

BETTER IDENTITY IN AMERICA:
A BLUEPRINT *for* POLICYMAKERS

Members

aetna



DISCOVER

EQUIFAX



JPMORGAN
CHASE & CO.



**Quicken
Loans**



usbank.



Framing the Challenge

Security

Compliance

Privacy

Transaction
Costs

Customer
Experience

Trust



"On the Internet, nobody knows you're a dog."

Trust

is hard to get right.

Identity

(when done right)

enables Trust

Identity

as

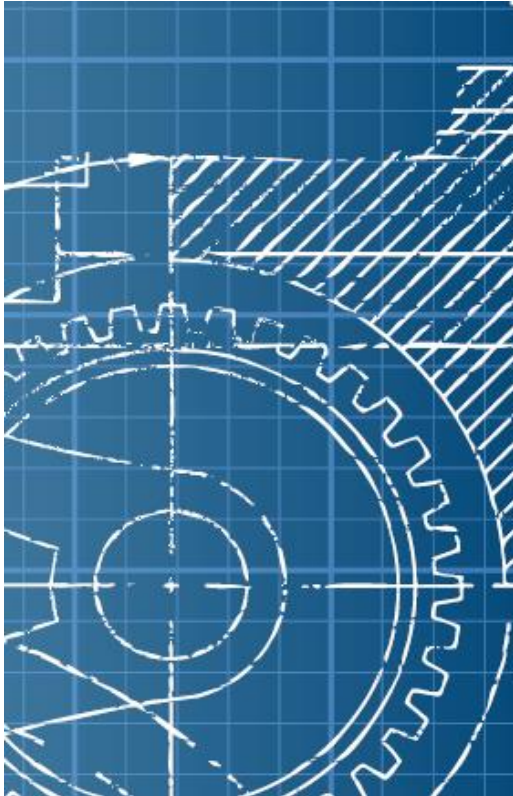
“the great enabler”

Identity as the Great Enabler

Providing a foundation for digital transactions and online experiences that are:

- Secure
- Easy to Use
- Protect Privacy

The challenge



“Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network...”

“The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.”

- National Institute of Standards and Technology (NIST)

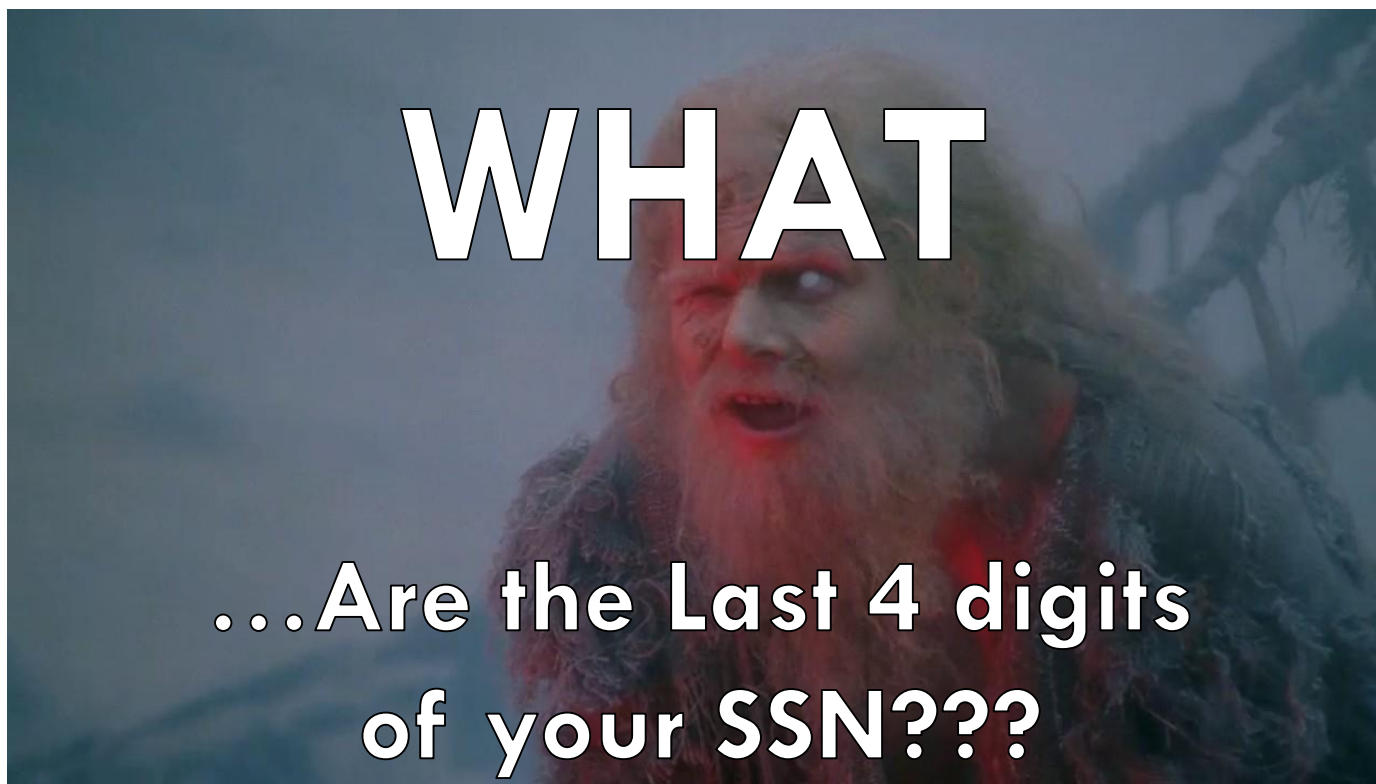
Our approach (to date)



Which has proven to be very practical



Especially when adversaries already know the answer



This has not worked well

**Nobody can actually
manage this for one
password – let alone
20-30**

**Any password that
meets this criteria is
still susceptible to
phishing, malware
and password reuse**

**Makes your
employees and
customers hate you**

STRONG PASSWORD CRITERIA:

Users of critical systems are required to use a strong password; a strong password must conform to all of the following:

- Your password must contain at least one uppercase letter.
- Your password must contain at least one lowercase letter.
- Your password must contain at least one number or punctuation mark.
- Your password cannot contain any common words or proper names of five or more characters, regardless of the case (upper or lower) of the letter.
- Your password cannot contain invalid characters (spaces, tabs, accented letters, etc.).
- Your password must be between eight and fifteen characters in length.
- Your password cannot contain forward or reverse fragments of five or more characters of your first name, middle name, or last name, regardless of the case (upper or lower) of the letter.
- Your password cannot contain forward or reverse fragments of five or more characters of your NetID/EnterpriseID, regardless of the case (upper or lower) of the letter.
- Your password cannot contain forward or reverse alphabetic sequences of five or more letters, regardless of the case (upper or lower) of the letter.
- Your password cannot contain forward or reverse numeric sequences of five or more numbers.
- Your password cannot be changed to any of your twelve previous passwords.
- Your password cannot be changed more than once in a twenty-four-hour time period.
- Your password must be changed annually.

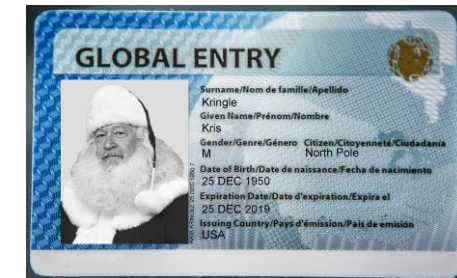
The cost of outdated identity solutions

- › **16.7 million** victims of identity fraud in 2017.
 - › **\$16.8 billion** stolen as a result of identity fraud in 2017.
 - › **44.7%** - the increase in U.S. data breaches from 2016 to 2017.
 - › **179 million** records containing personal information were exposed in 2017 breaches – a 389% increase over 2016.
 - › **69%** of 2017 data breaches were identity theft incidents.
 - › **30%** - the rate in which Online shopping fraud attacks rose in 2017, with criminals leveraging holes in e-Commerce identity services to perpetrate fraud.
- 

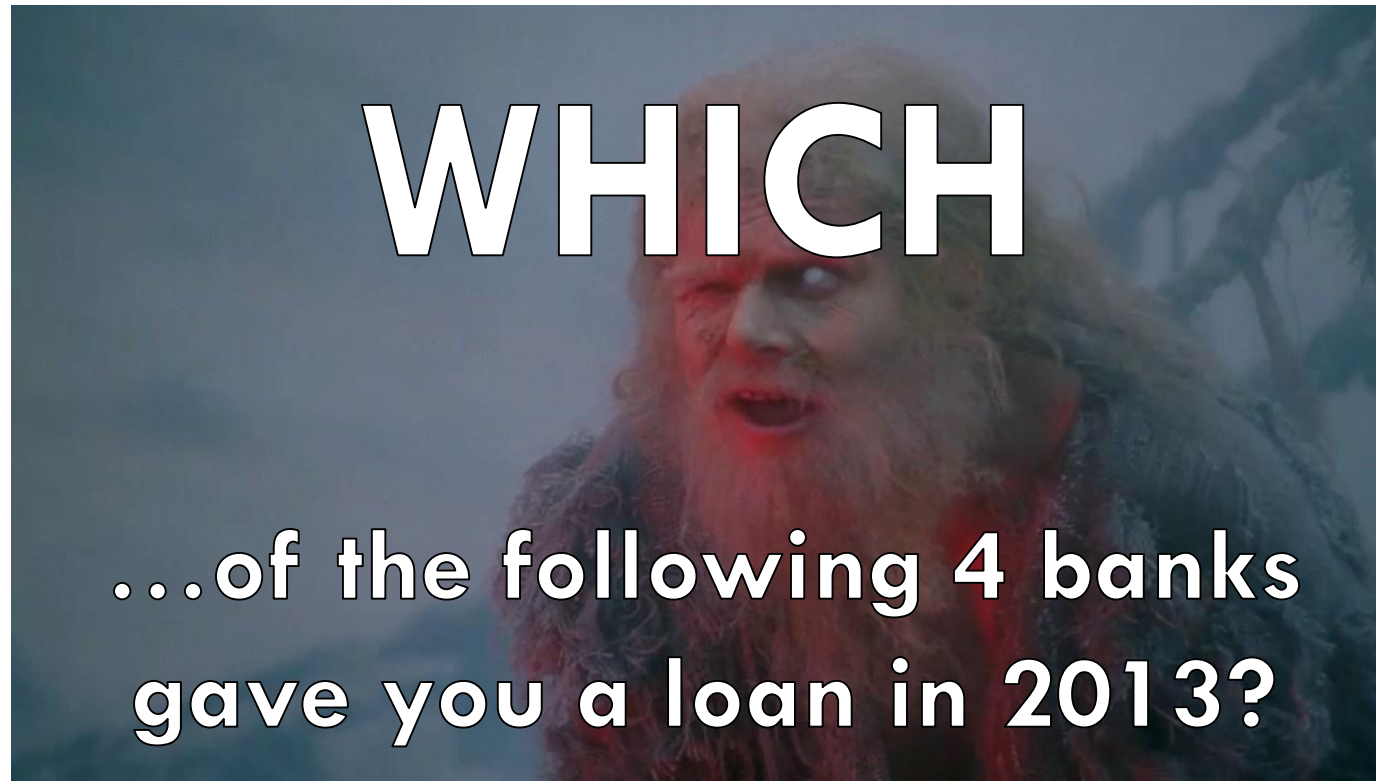
- › **81% of 2016 breaches** that exploited identity as an attack vector – using weak or stolen passwords to access systems and steal data.
- › **69%** of online shopping carts are “abandoned,” meaning that consumers fail to complete a purchase online after beginning the process; 37% of those abandonments had to do with consumer frustrations about the account creation process.
- › **\$150 million** is spent by the largest financial institutions each year to comply with Anti Money Laundering (AML), Know Your Customer (KYC), and other identity-related compliance requirements.
- › **81%** of Americans say they would stop using a service that allowed their profile information to be stolen and leaked online.

Why has this been so hard to solve?

- The “identity gap” – the U.S. has many nationally recognized, authoritative identity systems
- All are trapped in the paper world



This was an attempt to get around the “identity gap”



Industry needed something to enable trusted digital commerce – this was the best solution out there

It worked for a while

- But today, attackers have caught up
- “Out of wallet” questions are not as secret as they used to be



Security IRS breach highlights weakness of 'knowledge-based' security

By Zach Noble May 27, 2015

The compromise of 100,000 taxpayer accounts through the Get Transcript application on the IRS website were not random hacks, but the exploits of an already-publicized vulnerability -- known to security experts since at least March.

And, in order to gain access, hackers already had a good deal of information on the affected taxpayers.

Hackers already had the keys



at the IRS was first realized. More than numbers and tion may have

ranscript" you to check

BETTER IDENTITY IN AMERICA: A BLUEPRINT *for* POLICYMAKERS

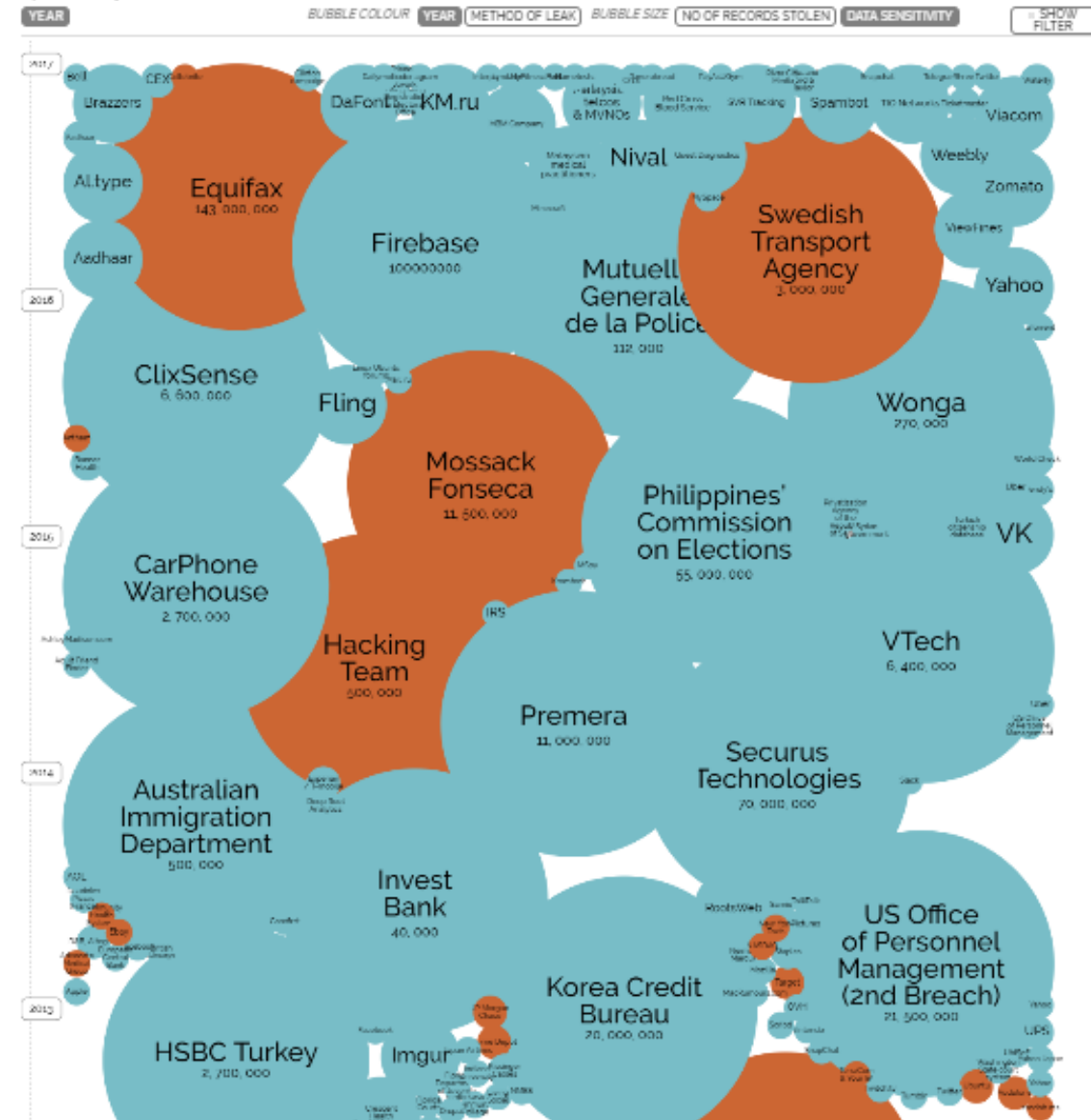
While any one of these breaches on its own creates serious policy issues, there now exists the potential for malicious actors to combine multiple stolen data sets into one, thereby enabling them to obtain more complete “packages” of identity information.

-House Energy & Commerce Committee, 2017

World's Biggest Data Breaches

Selected losses greater than 30,000 records
updated 4th July 2018

Interesting story



SSNs are no longer “secrets”



USA - PERSONAL INFO | 2016 FRESH SSN + DOB FULLZ

...FULLZ COMES IN THIS FORMAT FIRST:LAST:ADDRESS:CITY:STATE:ZIP:MAIL:DOB:IP:P
ST | CITY: | STATE: | ZIP: | DOB: |

Sold by - 9681 sold since Feb 24, 2016

Vendor Level 5

Trust Level 5

	Features
Product class	Digital goods
Quantity left	Unlimited
Ends in	Never

	Bulk Discounts		
Bulk Discount	From qty 9 to 19	USD 0.98	0.0008 BTC
Bulk Discount	From qty 20 to 49	USD 0.97	0.0008 BTC
Bulk Discount	From qty 50 to 99	USD 0.95	0.0008 BTC
Bulk Discount	From qty 100 to 999	USD 0.90	0.0008 BTC

SEE MY STORE FOR MORE - 1 days - USD +0.00 / item

Purchase price: USD 0.99

Qty: 1

Buy Now

Buy Now

Queue

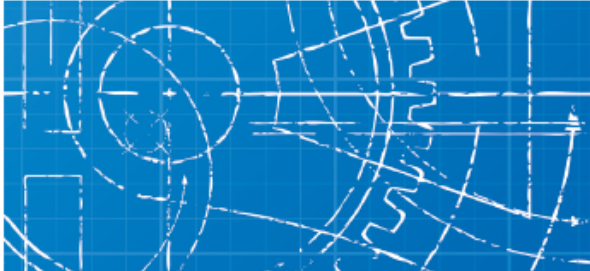
0.0009 BTC / 0.0945 XMR

Summary: Where we are today

- In an era where transactions are increasingly digital, our authoritative identity systems are stuck in the paper world
- Solutions that “papered over” that fact helped for a while – but now attackers have caught up
- “Shared secrets” like SSNs and passwords are no longer secret
- Industry innovation is helping to develop better, next-generation identity solutions such as passwordless authentication and identity proofing tools that scan and validate ID documents
- But – government remains the one authoritative issuer of identity. In this next phase of making identity “Better,” the government also has a role to play

What does “Better” look like?

- **Better Security – with Less Fraud and Identity Theft**
 - Embracing the recommendation of the 2016 Commission on Enhancing National Cybersecurity that *“Compromises of identity will be eliminated as a major attack vector by 2021.”*
- **Better Convenience for Consumers**
 - Allowing consumers to open new accounts online with ease, without having to go through duplicative, burdensome enrollment processes.
- **Better Confidence for Both Consumers and Service Providers**
 - That identities asserted online are reliable and trustworthy.
- **Better Privacy**
 - Shifting the predominant model for identity verification from one based on firms aggregating personal data without opt-in consent, to one where consumers proactively request that their identity be validated by parties with whom they already have a trusted relationship

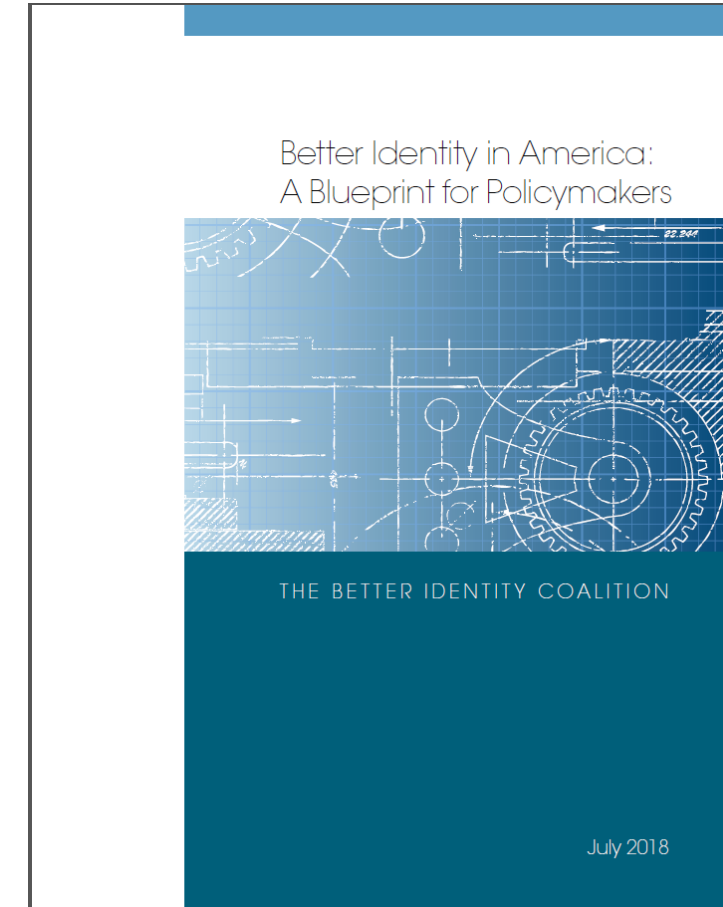


“The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021.”

- 2016 Report from the
Bipartisan Commission
on Enhancing
National Cybersecurity

How to Get There: A Policy Blueprint

- Five core areas where government can and should help
- A specific action plan detailing “who needs to do what” in Congress and the Executive Branch
- No single action or initiative can “solve” identity
- But: taken as a package, if this Policy Blueprint is enacted and funded, it will make identity better



A Policy Blueprint

Our Blueprint for Policymakers contains five key initiatives:

- 1. Prioritize the development of next-generation remote identity proofing and verification systems**
- 2. Change the way America uses the Social Security Number (SSN)**
- 3. Promote and prioritize the use of strong authentication**
- 4. Pursue international coordination and harmonization**
- 5. Educate consumers and businesses about better identity**

1. Prioritize the development of next-generation remote identity proofing and verification systems

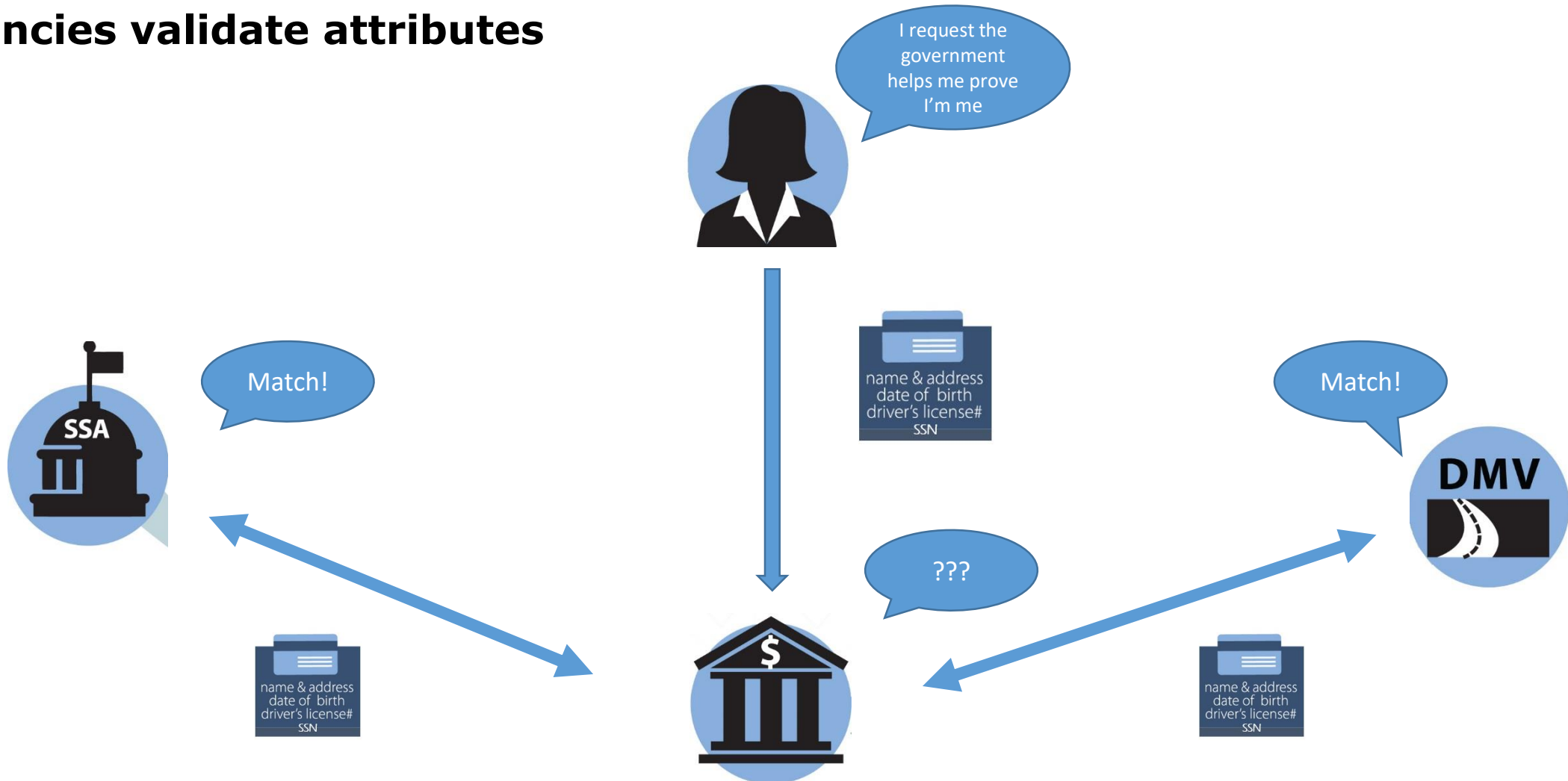
In simple terms:

If I've gone through the process of having an agency vet my identity once – can I ask that agency to vouch for me when I need to prove who I am to another party?

America's legacy paper-based systems should be modernized around a privacy-protecting, consumer-centric model that allows consumers to ask the government agency that issued a credential to stand behind it in the online world – by validating the information from the credential.

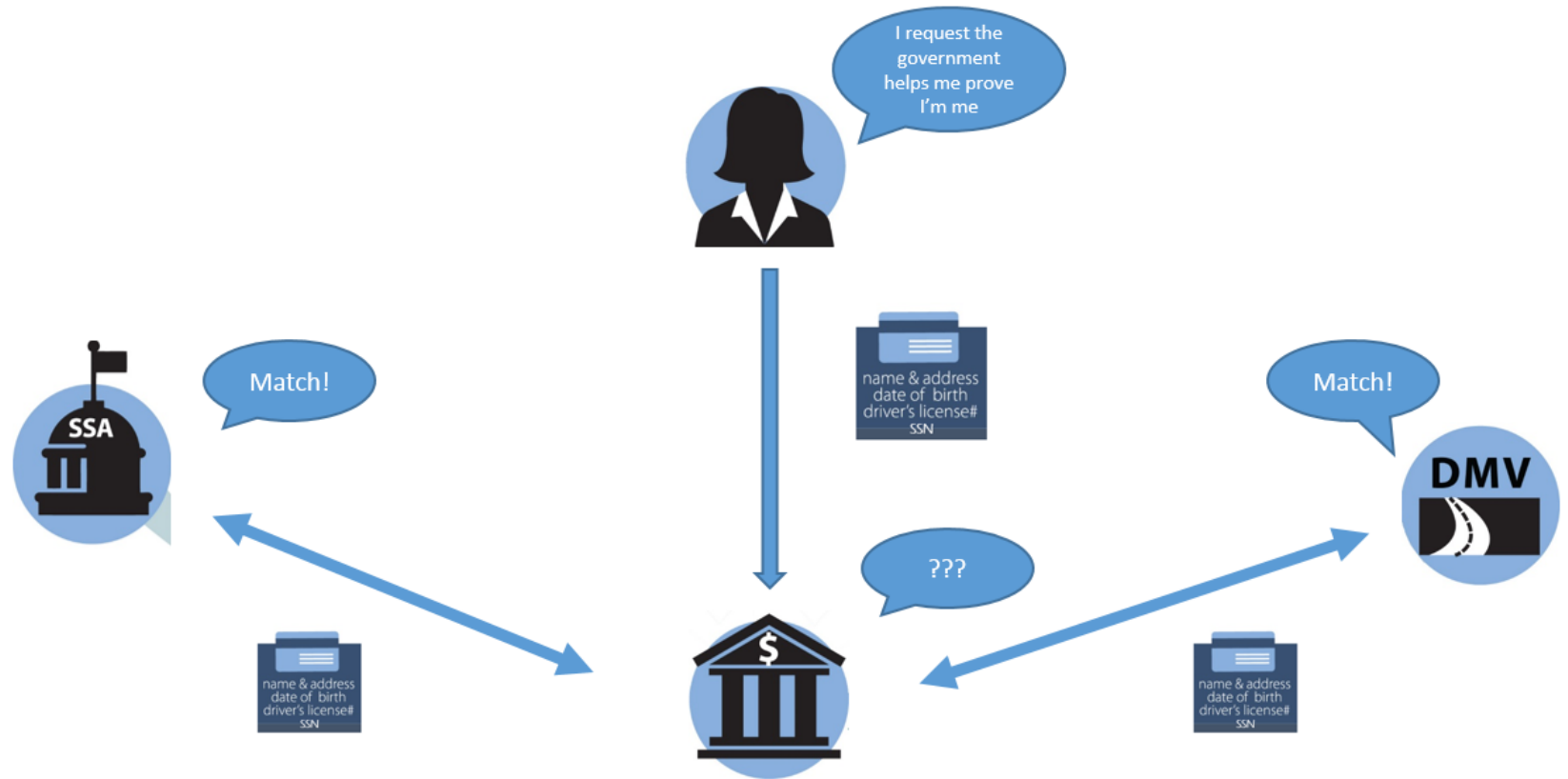
How this could work

1. Agencies validate attributes



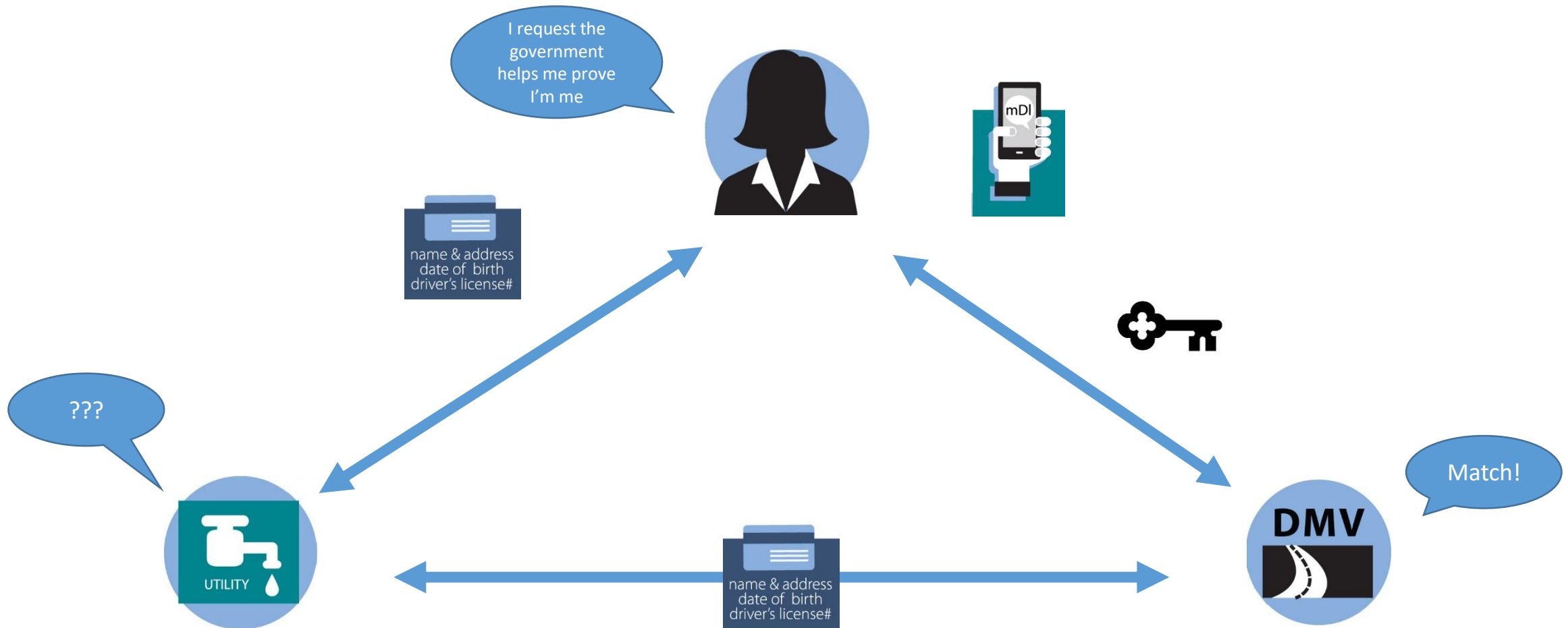
Of note...

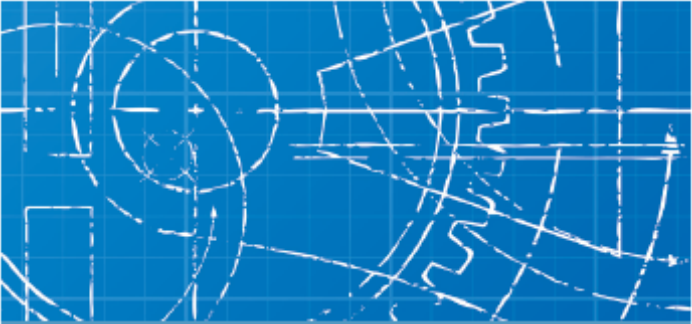
- Sec. 215 of the “Economic Growth, Regulatory Relief, and Consumer Protection Act” directs SSA to establish this service for transactions covered under the Fair Credit Reporting Act (FCRA)
- One idea: expand beyond FCRA



How this could work

2. Apps enable consumers to easily prove their identity





“The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021.”

- 2016 Report from the
Bipartisan Commission
on Enhancing
National Cybersecurity

1. Prioritize the development of next-generation remote identity proofing and verification systems

Action Item 1.3.3: *The government should serve as a source to validate identity attributes to address online identity challenges.*
(MEDIUM TERM)

The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.

As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers’ licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is key. Industry and government each have much to gain from strengthened online identity proofing.

The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes.

1. Prioritize the development of next-generation remote identity proofing and verification systems

Improving Identity While Protecting Privacy

- Inadequate identity solutions have impacted the privacy of millions of Americans – through an epidemic of breaches. Better Identity is key to improving privacy protections.
- New identity solutions backed by the government should embrace a “Privacy by Design” approach ensures that any new solutions are architected from the start to address privacy risks; protections are embedded in the solution architecture
- Government should only validate data should when consumers request it, and only for the purpose specified.
- Consumers should be able to choose to share or validate only certain attributes about themselves without revealing all their identifying data.
- To ensure that new systems are secure and privacy-preserving, NIST should be funded to lead development of a framework of standards and operating rules that will apply to any new government attribute validation services.

1. Prioritize the development of next-generation remote identity proofing and verification systems

Helping states embrace Better Identity

- States are ideally suited to drive Better Identity
 - The driver's license is the document most commonly used to prove identity, and it's backed today by a robust, in-person identity proofing process
- In practice, most state DMV systems are not built to support modern identity services
 - Many states are running DMVs off infrastructure that is 20-30 years old
 - States are not incented on their own to invest in DMV modernization to support digital identity



Helping states embrace Better Identity

- \$2.5-3 billion in unaddressed funding needs for DMV modernization that can support Better Identity
 - Based on an analysis of recent DMV modernization efforts
- Federal assistance can help catalyze activity in state governments: A five-year, \$200 million-per-year grant program
 - Provide seed money to incent states to invest their own resources in modernizing DMVs to support digital identity
 - “Strings attached” – grants can only be used for systems that follow Federal (NIST) framework for security and privacy

Prioritize R&D and Standards

- Government investment in identity R&D and standards work has waned
- The Federal government should develop a new, forward-looking investment strategy for R&D and standards work in identity that
 - 1) Ensures alignment in priorities across agencies, and
 - 2) Ensures necessary work around identity is adequately funded
- Focus areas:
 - Active partnership with private sector standards efforts
 - Augmenting private sector-led R&D and standards work to fill critical gaps
 - Research and standards for privacy-preserving technologies in identity systems

R&D and Standards – where are there gaps?

- We have solid standards for
 - Identity proofing
 - Authentication
 - Federation
- Gaps
 - Attribute exchange
 - Use of identity analytics tools
 - Privacy and consent (including privacy-preserving technologies in identity systems)
 - “Mobile driver’s licenses” – work underway
 - DMV security

Summary

1. **Prioritize the development of next-generation remote identity proofing and verification systems**

- a. Governments should offer new digital services to validate attributes – modernizing legacy paper-based identity systems around a privacy-protecting, consumer-centric digital model that allows consumers to ask the agency that issued a credential to stand behind it in the online world – by validating the information from the credential
- b. Create a five-year, \$200 million-per-year grant program to provide seed funding to states enabling DMVs to modernize and become digital identity providers
- c. Develop a forward-looking investment strategy for R&D and standards work in identity
- d. Address policy and regulatory barriers that inhibit private sector entities from innovating around identity – and create incentives that promote adoption of innovations

2. Change the way America uses the Social Security Number (SSN)

The Equifax breach spurred some proposals



The screenshot shows a Bloomberg Politics article. The header includes the Bloomberg Politics logo and navigation links for Markets, Tech, Pursuits, Politics, Opinion, and Businessweek. The article title is "The White House and Equifax Agree: Social Security Numbers Should Go". The byline is "By Nafeesa Syeed and Elizabeth Dexheimer" with a timestamp of "October 3, 2017, 2:50 PM EDT" and an update timestamp of "Updated on October 3, 2017, 7:15 PM EDT". Below the title, there are two bullet points: "→ Administration exploring new tech for personal identifiers" and "→ Ex-Equifax CEO tells Congress relying on numbers outdated".

The White House and Equifax Agree: Social Security Numbers Should Go

By **Nafeesa Syeed** and **Elizabeth Dexheimer**
October 3, 2017, 2:50 PM EDT Updated on October 3, 2017, 7:15 PM EDT

- Administration exploring new tech for personal identifiers
- Ex-Equifax CEO tells Congress relying on numbers outdated

McHenry Introduces the PROTECT Act in Response to Equifax Breach

Washington, October 12, 2017 | 0 comments



Today, Chief Deputy Whip Patrick McHenry (R, NC-10), the Vice Chairman of the House Financial Services Committee introduced **H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017, or the PROTECT Act.**

Following the data breach at Equifax that exposed the personal data of over 140 million Americans, this bill would require the federal government to create uniform cybersecurity standards for credit bureaus and submit them to onsite examinations. The bill would also create a national framework for credit freezes so that victims of identity theft, active military personnel, people over 65 years of age, and children are protected. Finally, the bill would stop the credit bureaus from using Americans' Social Security Numbers as a basis for identification by 2020.

"The Equifax data breach has harmed my constituents in western North Carolina and Americans across the country," said McHenry. "It exposed a major shortcoming in our nation's cybersecurity laws and Congress must act. The bill I've introduced today takes an important first step in providing meaningful reforms to help Americans who have been impacted by this breach. It is focused on prevention, protection, and prohibition.

"It prevents future harm to all Americans by requiring the largest credit reporting agencies to be subjected to the same standards and supervision as the rest of the financial industry," McHenry continued. "It protects Americans by creating a national credit freeze that actually works. Finally, it prohibits the largest credit reporting agencies from continuing to rely upon the most sensitive of Americans' personal information: our Social Security Numbers."

2. Change the way America uses the Social Security Number (SSN)

The SSN is not just one thing

2. Change the way America uses the Social Security Number (SSN)

The SSN is not just one thing

Identifier

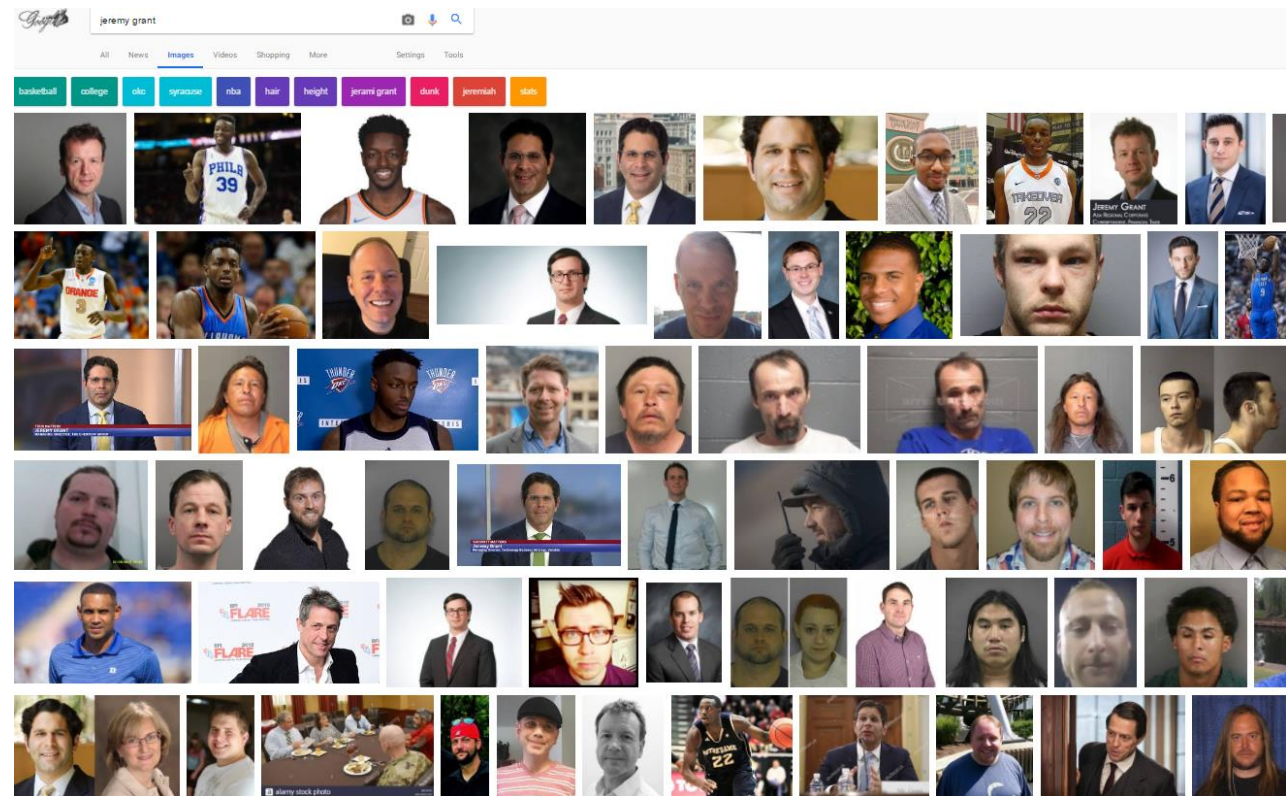
Used to determine which of the 3,847 Jordan Pooles are a “particular Jordan Poole”

999-99-XXXX

jordanp@foo.org

@JordanPooleMI

Typically, this is a username or number. It may be widely known, but it is unique, and linked to a particular individual.



2. Change the way America uses the Social Security Number (SSN)

The SSN is not just one thing

Identifier

Used to determine which of the 3,847 Jordan Pooles are a “particular Jordan Poole”

999-99-XXXX

jordanp@foo.org

@JordanPooleMI

Typically, this is a username or number. It may be widely known, but it is unique, and linked to a particular individual.

Authenticator

Used to determine whether the person claiming to be a “particular Jordan Poole” is in fact that person

Passw00rd



Typically, this is something a person possesses and controls (such as a password, a biometric, or a cryptographic key). It should not be widely known.

2. Change the way America uses the Social Security Number (SSN)

IDENTIFIERS

Used to determine which of the 3,847 Jordan Pooles are a “particular Jordan Poole”

999-99-XXXX

jordanp@foo.org

@JordanPooleMI

Typically, this is a username or number. It may be widely known, but it is unique, and linked to a particular individual.

AUTHENTICATORS

Used to determine whether the person claiming to be a “particular Jordan Poole” is in fact that person

Passw00rd



Typically, this is something a person possesses and controls (such as a password, a biometric, or a cryptographic key). It should not be widely known.

- Frame proposals about the “future of the SSN” on the basis of its use as an authenticator, and identifier, or both
- Stop using the SSN as an authenticator
- Preserve its use as an identifier – but look to reduce its use wherever feasible

Don't: Seek to replace the SSN with a new government-issued identifier

- It would cost billions of dollars and create confusion for millions of Americans
 - while offering very little security benefit
- Introduction of a new identifier would require both government and industry to map back to the old SSN
 - Chaos due to errors in mapping and matching

2. Change the way America uses the Social Security Number (SSN)

Do:

- Executive Order or legislation banning agencies from using SSN as an authenticator
- Launch a task force charged with reviewing existing laws and regulations that require the use of the SSN and identifying whether any can be changed
- Acknowledge that SSA plays a role in the identity ecosystem

Questions?

Jeremy Grant

Coordinator

Better Identity Coalition

info@betteridentity.org

jeremy.grant@venable.com