

The “Policy Layer” of Digital Identity



Jeremy Grant

Coordinator

Better Identity Coalition

info@betteridentity.org

jeremy.grant@venable.com

Who am I?

- Managing Director in Venable's Cybersecurity and Privacy practice
- Identity: 25+ years experience across government and industry

Government:

- Led National Strategy for Trusted Identities in Cyberspace (NSTIC)
- Senior Executive Advisor for Identity Management at NIST, built out the NIST Trusted Identities Group
- U.S. Senate staff – covering health and technology issues (Senate Finance Committee & Joint Economic Committee)

Industry:

- Five years building and delivering identity solutions (ID proofing, PKI, smart card, biometrics, federation)
- Three years as a market analyst covering the identity space
- Seven years consulting with identity vendors, end-users, investors and governments on how to best position in the identity market

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.

Members



How we got started: The Equifax breach spurred some proposals



- 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- Ex-Equifax CEO tells Congress relying on numbers outdated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."*

HOUSE COMMITTEE ON ENERGY & COMMERCE

HEARING ON "IDENTITY VERIFICATION IN A POST-BREACH WORLD," SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS (NOVEMBER 30, 2017)

Date: Thursday, November 30, 2017 - 10:15am
Location: 2322 Rayburn House Office Building
Subcommittees: Oversight and Investigations (115th Congress)

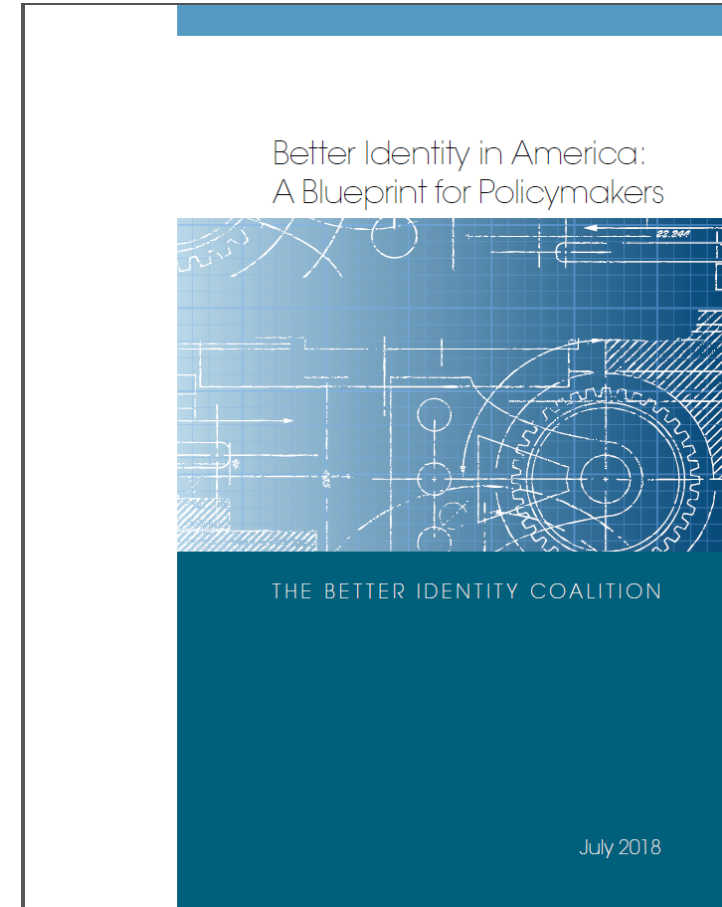
The Subcommittee on Oversight and Investigations held a hearing on Thursday, November 30, 2017, at 10:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled "Identity Verification in a Post-Breach World."

Livestream



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

Framing the Challenge

Security

Privacy

Customer
Experience

Compliance

Transaction
Costs

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

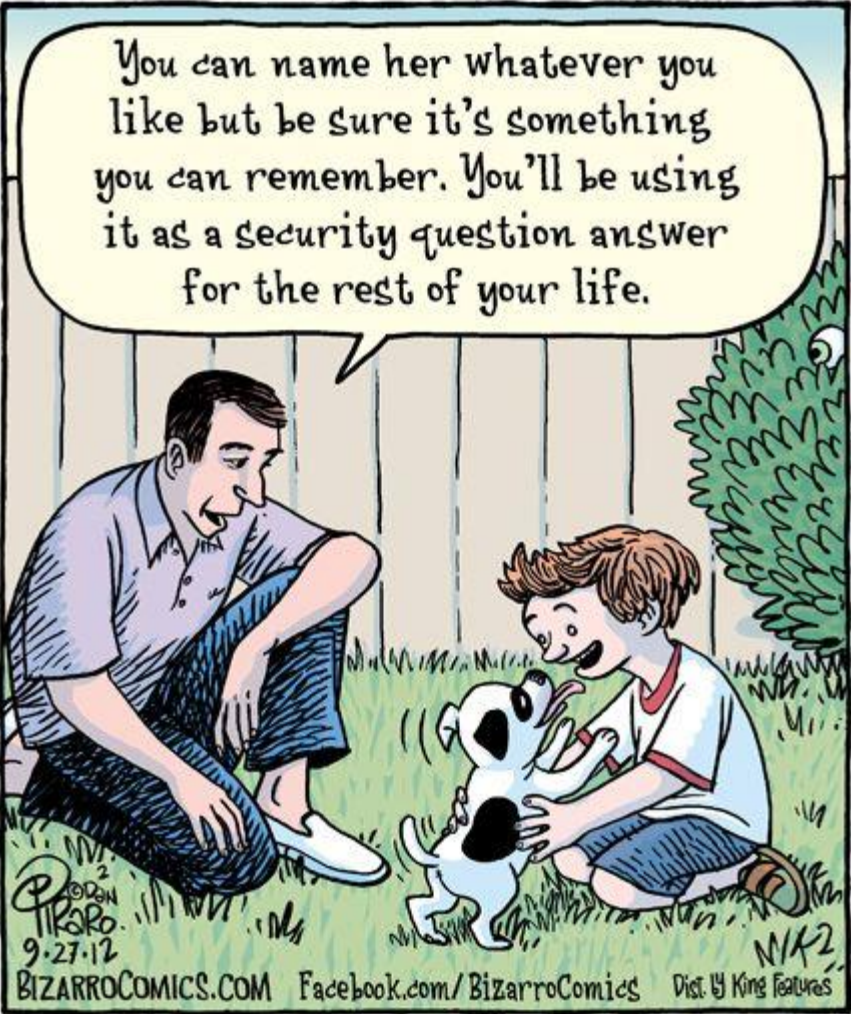


“Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network...”

“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)

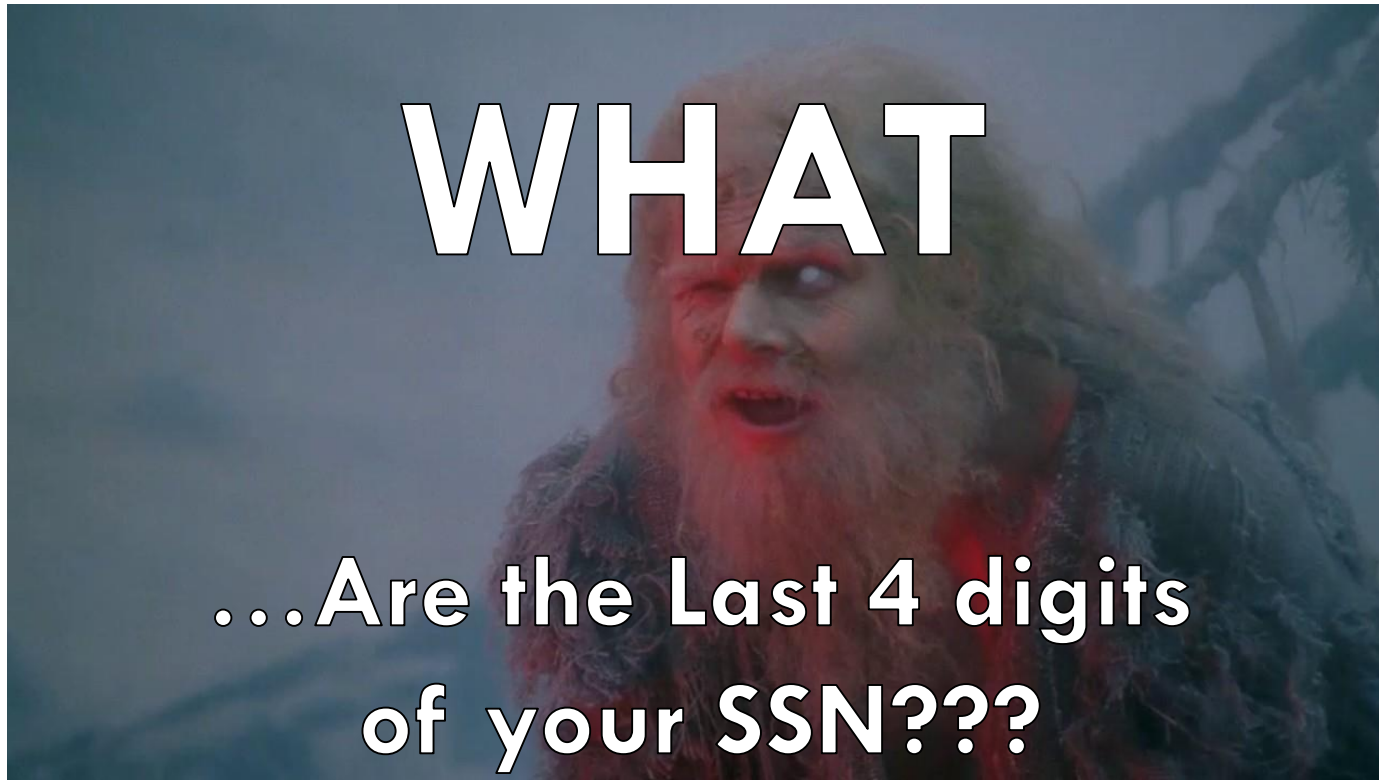
Our approach (to date)



Which has proven to be very practical



Especially when adversaries already know the answer



And it all just got worse



April 19, 2021

Identity Thieves Target Pandemic Unemployment Programs in Record Numbers

The Federal Trade Commission reports that “of the identity theft reports received in 2020, over 394,000 came from people who said their information was misused to apply for a government benefit. This represents a staggering increase of nearly 3000% from 2019.”

[Read the Federal Trade Commission's report.](#)

A bar chart with a blue line graph showing an overall upward trend in identity theft reports. The bars represent data points for different periods, and the line connects them, showing a significant peak and then a dip followed by another rise.

Identity Theft Impacts Nearly Half of U.S. Consumers, Aite Group Report Finds

Underwritten by GIACT, Aite Group Report Discovers Alarming Percentages of U.S. Consumers Impacted by Identity Theft, Application Fraud and Account Takeover



NEWS PROVIDED BY
GIACT →
Mar 09, 2021, 08:00 ET




DALLAS, March 9, 2021 /PRNewswire/ -- GIACT®, the leader in helping companies positively identify and authenticate customers, today announced a new report, *U.S. Identity Theft: The Stark Reality*, developed by Aite Group, and underwritten by GIACT, that uncovers the striking pervasiveness of identity theft perpetrated against U.S. consumers and tracks shifts in banking behaviors adopted as a result of the pandemic.

[Click here to download the report](#)

According to the report, from 2019 to 2020, almost half (47%) of U.S. consumers surveyed experienced identity theft; well over one-third (37%) experienced application fraud (i.e., the unauthorized use of one's identity to apply for an account), and over one-third (38%) of consumers experienced account takeover over (i.e., unauthorized access to a consumer's existing account) over the past two years.

What FinCEN says


“Analysis of the over 3 million Suspicious Activity Reports that financial institutions filed with us in 2021 shows that the majority include reference to potential breakdowns in the identity verification process—verification, impersonation, and compromise.”

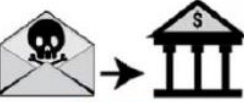
 **Threat Environment: Identity as a High Value Target**


Common fraud and cybercrime typologies rely on identity theft, compromise or other exploitation – key contributor to trillions of dollars in cybercrime

- **Identity Theft and Synthetic Identity Fraud:** 3,077 suspicious activity reports (SARs)/\$256 million per month
- **Account takeovers (ATO):** 5,200 SARs/\$350 million per month
- **Business Email Compromise (BEC):** 1,200 SARs/\$433 million per month
- **Pandemic Exploitation:** Over 60,000 SARs since February, many involving compromise of identity and trust between counterparties in financial relationships, supply chains, and across remote systems (e.g., impostor fraud, medical scams, stimulus fraud, credential stuffing)
- **Identity Crime Enables Other Crime:** Significant money laundering and terrorism financing (ML/TF) activity occurs exploiting simpler criminal fraud and anonymization methods to obscure involved parties

EXAMPLE: BEC Schemes Targeting Weaknesses in Identity

 **STAGE 1**
Compromising Victim Information and Email

 **STAGE 2**
Transmitting Fraudulent Transaction Instructions

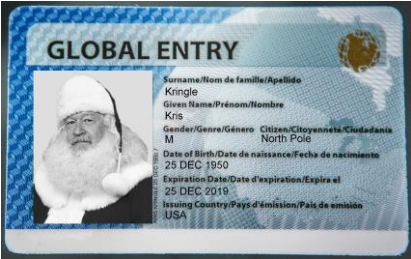
 **STAGE 3**
Executing Unauthorized Transactions



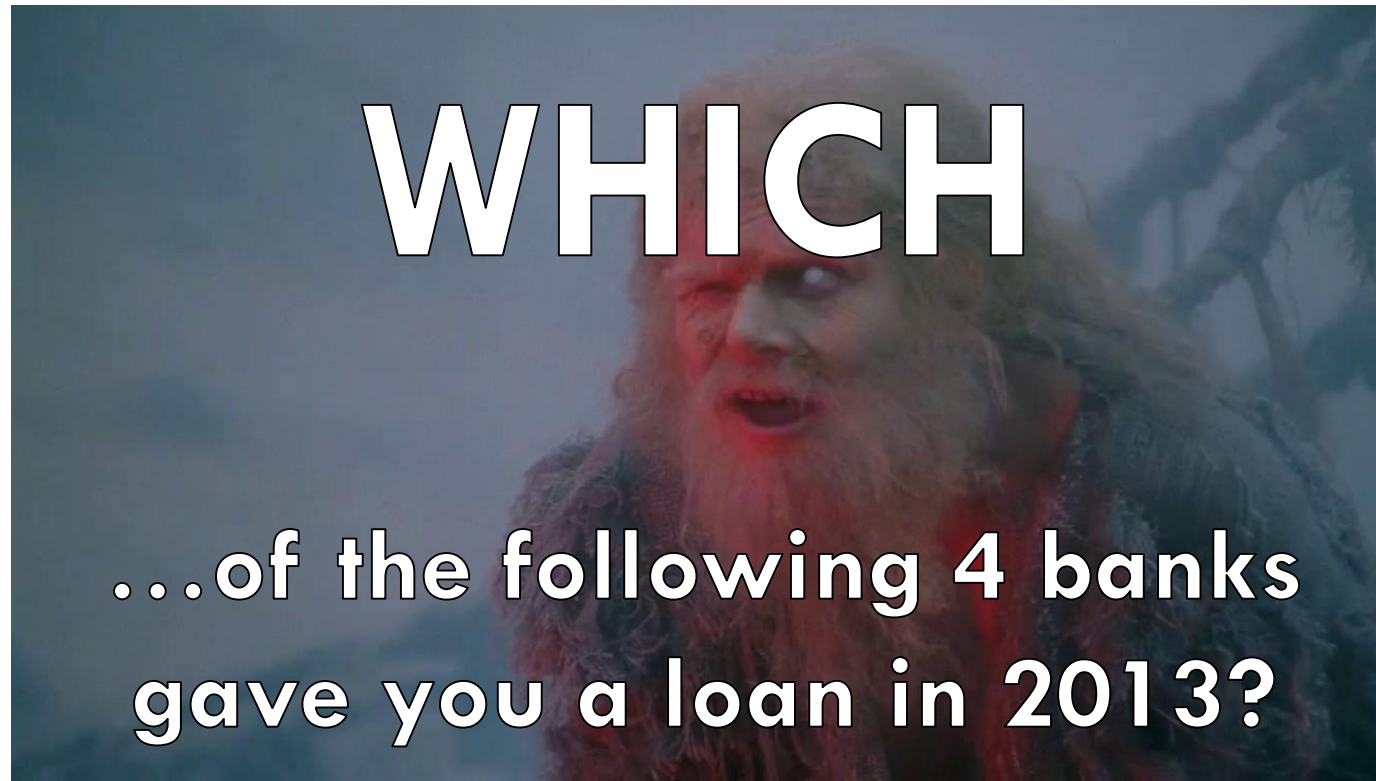
<https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-deputy-director-jimmy-kirby-during-2022-federal>

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 information may have been accessed. "Get Transcript" you to check



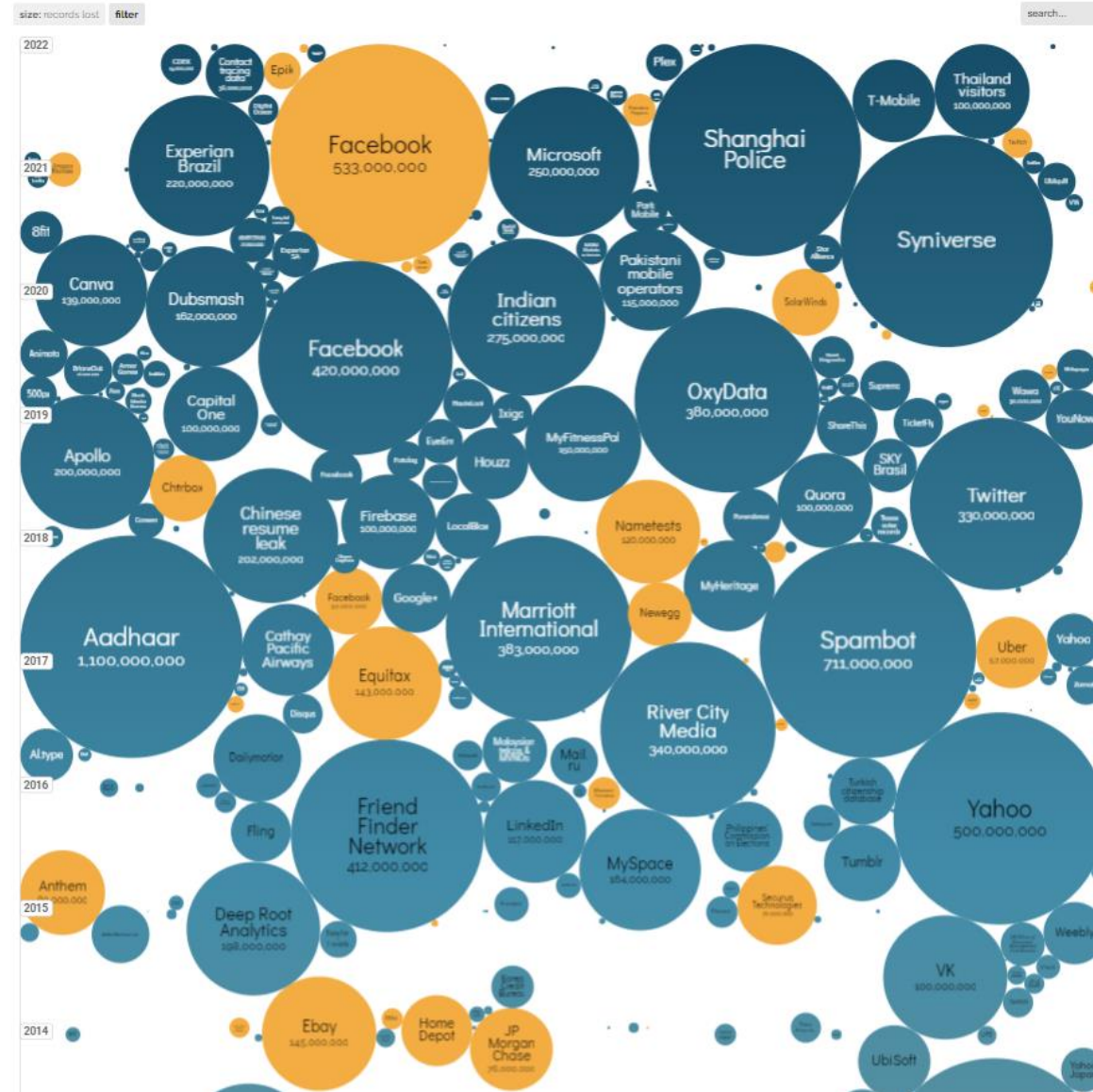
While any one of these breaches on its own creates serious policy issues, there now exists the potential for malicious actors to combine multiple stolen data sets into one, thereby enabling them to obtain more complete “packages” of identity information.

-House Energy & Commerce Committee, 2017

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022



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

Summary: Where we are today

Cutting to the point:

The Private Sector Cannot Solve Identity Alone.

Doing So Will Require Better Access to Government Data.

The Challenge:

How to do This in a Way That's Good for Security + Privacy?

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.

Early Progress

eCBSV moving forward @SSA

- Launched in June 2020
- Available to banks and their service providers (per P.L. 115-174)
- Will validate “Yes/No” match of Name/DOB/SSN combo along with indicator if the person is dead
- We are working with SSA to provide industry feedback on standards, electronic consent best practices, API design, etc.

Friday, September 6, 2019
For Immediate Release



Mark Hinkle, Acting Press Officer
press.office@ssa.gov

News Release

SOCIAL SECURITY

Social Security Announces First Potential Group of Participants for New Electronic Social Security Number Verification Service Service to Begin in 2020

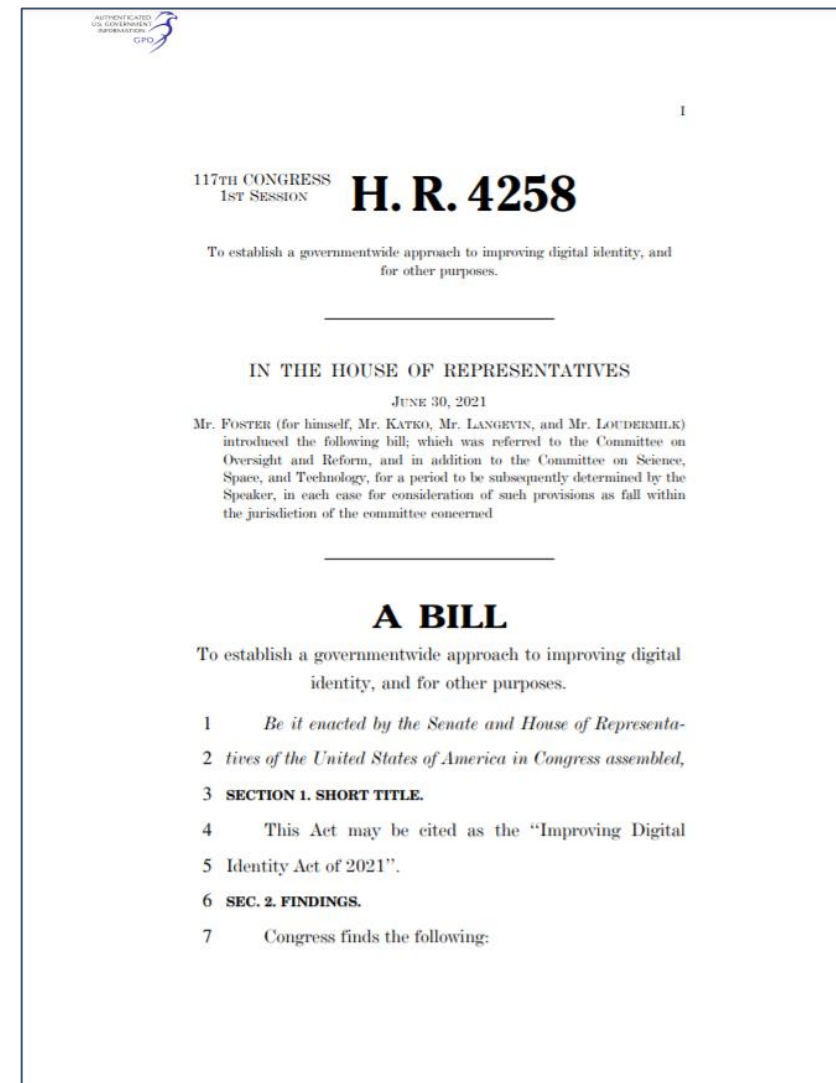
The Social Security Administration today announced the first potential group of selected participants for its new electronic Consent Based Social Security Number (SSN) Verification (eCBSV) service. The agency will roll out the service to these users in June 2020, and plans on expanding the number of users within approximately six months of the initial rollout.

“Our new electronic SSN verification service will help to reduce synthetic identity fraud by comparing data provided electronically by approved participants with the agency’s records,” said Andrew Saul, Commissioner of Social Security. “This will provide fast, secure, and more efficient SSN verifications for the financial services industry and customers using their services.”

Social Security is creating eCBSV, a fee-based electronic SSN verification service, to allow select financial institutions and service providers, called “permitted entities” and including subsidiaries, affiliates, agents, subcontractors, or assignees of a financial institution, to verify if a person’s SSN, name, and date of birth combination matches Social Security records. Social Security needs the person’s written consent and will accept an electronic signature in order to disclose the SSN verification to the permitted entity. eCBSV returns a match verification of “Yes” or “No.” eCBSV does not verify a person’s identity.

H.R. 4258 – The Improving Digital Identity Act of 2021

- New bipartisan digital ID legislation introduced to coordinate a government-wide approach to identity validation services
- Marked up in House Oversight Committee July 20th; revised language tracks a Senate counterpart S. 4528
- Senate HSGAC marked up today!



A “whole of government” approach – covering Federal, State & Local

NIST Framework of standards, policies, and rules – that any agency can use to create interoperable services that set a high bar for security and privacy*

Grant dollars to states to modernize legacy ID systems to support digital ID

H.R. 4258 - Three Pillars to Better Identity

Why Government Needs to Act

- Government is the only authoritative issuer of identity – but those issuers are split between the Federal, state and local level
- Without a coordinated approach that involves all issuers:
 - Progress will lag another 15 years – and identity theft and identity-related cybercrime will continue to thrive.
 - Solutions that do roll out won't be standards-based, making them hard for many to use
 - We will miss an opportunity to set a high bar for security and privacy – making sure this is done right

Questions?

Jeremy Grant

Coordinator

Better Identity Coalition

info@betteridentity.org

jeremy.grant@venable.com