Caudle Crisis & Communication Counsel

DRAFT 3.4 7/17/18

Thank you Jeremy.

I am the Chief Security Officer at PNC. I and my team of 700 professionals spend all day on the front lines of the cyber and information security battle.

That's the work we do every day.

The job we are challenged with is building trust. [**Trust]** that every financial transaction is secure. [**Trust**] that every person we interact with is who they say they are.

Building **trust** in a world where in 2017 alone there were 16.7 million victims of identity fraud and 170 million records containing personal information exposed in last year's breaches is a very difficult job.

How do we build **trust** in a world where our adversaries have caught up with the Knowledge Based Verification systems and can answer those once secret questions to prove our identity?

Commented [JM1]: Minister emphasis on TRUST at start of each paragraph

Why should consumers trust us when we ask for personal Information and why should we trust them to be who they say they are when they communicate with us online?

When parents of a new baby do the right thing and establish a social security number for their infant child, should they have to worry that their child's identity will be stolen and wake up 18 years from now only to learn their credit history is destroyed?

When your grandmother goes online to make a purchase to send you a special gift for your birthday and is greeted by a lengthy account creation process, 37% of the time she gives up. It's too hard and she's afraid to give so much information. Instead you get a birthday card in the mail, two days late with a check for $10.

When the retiree in Phoenix wants to open a checking account and line of credit with us at PNC, how can I prove he is who he says he is? I have no branches in Arizona for him to walk into. Is he a real estate baron with millions of dollars or someone posing as that recently born baby? We won't know without a lot of checking.

I believe that the proposal we will share today from The Better Identity Coalition will help all of us regain trust in our collective need to securely verify and authenticate an individual's identity.

What the Coalition will propose is not moonshot. What the Coalition proposes are both significant in impact and most importantly achievable.

Can the private industry develop and advance consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication alone?

Simply answered, NO.

Identity verification and authentication is a societal issue. Only with cooperation and guidance from private industry And policy makers may we rebuild consumer confidence and therefore trust in any transaction that takes place online.

America is a retail economy. We cannot continue to operate in an online world where online shopping fraud attacks increase at an annual rate of 30% as they did in 2017.

We cannot grow an online economy where 69% of online shopping carts are abandoned due to consumer frustration or mistrust.

We must come together, do our part, and solve this problem.

So what can we do?

As corporations we must do our job to protect customer's data. As the Chief Security Officer for a financial institution I see this as my most important job. Without the trust that my customer's data is safe, my customer would never allow me to provide them any other service. That's why America's largest financial institutions spend hundreds of millions of dollars each year to comply with Anti Money Laundering, Know your Customer and other identity-related compliance requirements.

That's also why my team at PNC works hard every day to find better solutions to keep customer data safe. Unfortunately, the solutions that will work for the heavily regulated financial industry may not work for those in the healthcare, technology, telecom, and manufacturing industries, just to name a few..

What you will see today from the Coalition is a recommendation that can work for all.

There are two more partners in this triumvirate, Policymakers and Law Enforcement.

To secure digital privacy, Policymakers at both the federal and state level must lay a structural foundation and establish expectations for all involved. This is achieved by creating the laws that define systems and standards we can all uphold to achieve and enforce safe business transactions.

None of this works without the diligent enforcement of laws. Without enforcement there is **no** accountability, **no** fear of wrong doing and **no** societal trust that things will be done right. At PNC, we work every day with the FBI and the US Attorney's office as they seek to enforce the laws That hold criminals accountable [pause] Until the price of getting caught is greater than the reward of doing wrong, our problem of identity fraud will continue to grow at a startling rate.

Commented [JM2]: Minister emphasis on "No"s

Commented [JM3]: Thoughtful inflection

Is it possible for corporations, policymakers and law enforcement to come together to develop systems and standards that balance security, accessibility and privacy? Is it possible to be open but secure, private but accessible?

As a participant in the development of the Coalition's recommendations: **this IS a**chievable.

As government contemplates new policies to improve the quality of digital identity in the United States, The Better Identity Coalition has brought together leading companies to help develop innovative ideas that improve security, privacy, and convenience for all Americans.

What you will see today is a solution that works for all Americans.

A solution that will help us all rebuild the trust we seek in those who hold our personal information.

[Pause]

But a solution that works for all Americans must be built through a public-private partnership. That's why we're here today.

Many of the most glaring problems in digital identity are ones that can be addressed through active partnership between the public and private sector.

Before defining a plan of action, it is important to first lay out a high level vision of what "**Better**" means.

Better identity in America means that the following outcomes have been achieved:

1. **Better** Security. The 2016 Commission on Enhancing National Cybersecurity asked that compromises of identity be eliminated as a major attack vector by 2021. We believe our public private partnership blueprint will achieve that goal.
2. **Better** Convenience for Consumers. Allow consumers to open new accounts with ease, without having to go through duplicative, burdensome enrollment processes. We believe our blueprint achieves this goal. And maybe grandma won't give up on the purchase of that awesome gift for your birthday.
3. **Better** Confidence for both Consumers and Service Providers. An ecosystem where identities asserted online are reliable and trustworthy.
4. **Better** Privacy. Shifting the predominant model for identity verification from one based on private industry aggregating personal data without opt-in consent to one where Consumers proactively request that their data be shared for the sole purpose of verifying identity.

Commented [JM4]: Emphasis on BETTER
Louder better and a slight pause

So, if the private sector can't do this alone, what do we need from our Policymakers?

The Coalition's blueprint for Policymakers contains five key initiatives:

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

   America's 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.

   We see the creation of a Government Attribute Validation Service that will transform legacy identity verification processes and help consumers and businesses alike trust online.

6. Change the way America uses the Social Security Number

   Every time there has been a breach where Social Security Numbers are targeted industry and government leaders call for a wholesale replacement for the Social Security Number.

There is little risk of using a Social to distinguish between Debbie Guild of Pennsylvania and Debbie Guild of California – however, when you start to depend upon it for authentication – to do things like transfer money – that is where the issues begin.

Effective use of Socials as an authenticator requires that the number be secret.

That, however, is no longer the case. The Equifax breach alone--where 55% of Americans 18 or older had their data compromised--is reason enough to stop using the Social Security Number as an authentication tool.

In short, government and industry alike need to move away from using Socials as an authentication factor and migrate to alternative solutions that can more securely authenticate consumers.

Today we ask that the Federal government launch a task force charged with reviewing existing laws and regulations that actually require the use of the Social Security Number and identify whether any can be changed.

7. Promote and prioritize the use of strong authentication

   We must recognize the problem is not just with Socials, but also with passwords and other "shared secrets."

   Verizon's 2017 data breach investigations report found that 81% of all breaches were enabled by compromised passwords. That number means it is an anomaly when a breach occurs and identity is not the attack vector. There is no such thing as a strong password or secret Social in 2018 and America should stop trying to pretend otherwise. We must move to stronger forms of authentication based on multiple factors that are not vulnerable to these common attacks.

   The good news is that industry and government have recognized the problems with old authenticators like passwords and Socials and worked together these past few years to make strong authentication easier.

   Multi-stakeholder efforts like Fast Identity Online (FIDO), the World Wide Web Consortium (W3C) and the GSMA have developed standards for the next-generation authentication. These are now being embedded in most devices, operating systems and browsers, and allow the use of biometrics and patterns in singular security enclaves in ways that enhance security, privacy and the user experience. These security enclaves on personal devices eliminate the creation of vast honey-pots of sensitive data ripe for attack.

   To the Federal Government we say…continue promoting strong authentication for industries like mine in banking, for healthcare and other government and consumer applications. Also let's modernize the rules that govern use of strong authentication and reduce the barriers to its adoption.

8. International Coordination and harmonization

   We are not alone.

Consumers and businesses operate in environments beyond America's borders. As other countries contemplate new approaches to making identity better, we should look for ways to coordinate and harmonize requirements, standards and frameworks where feasible and compatible with our values.

Coordination and harmonization is *particularly* relevant in my industry where the shift to digital banking and the emergence of fintech startups is disrupting traditional business practices. Coordination and harmonization is also critical for managing the risks associated with the Customer Identification Program requirements of the Bank Secrecy Act, as well as the related Know Your Customer and Anti-Money Laundering rules.

In the U.S., consumers are pushing for Open Banking where they are allowed to ask their bank to share their data with other firms, such as account aggregation services, or enable third parties to make payments from their account. Robust identity solutions are at the heart of these applications, as they require us to ensure that those authorization requests are coming from the right person or system, as well as comply with Know Your Customer rules for any new account openings.

All that said, we also must explore how we can be aligned with global efforts in this area, such as Europe's eIDAS initiative and ongoing work in the Financial Action Task Force. Doing so will help streamline the ability of Americans to more easily transact business on the global stage.

9. Educate consumers and business about better identity.

We've got to tell people that we are addressing this difficult problem. Government must partner with industry to educate both consumers and businesses, with an eye toward promoting modern approaches and best practices.

The National Cyber Security Alliance, which has a strong record of driving public-private partnerships to educate the public on cybersecurity, should be leveraged to promote better identity outcomes.

All that said, with any societal issue, there are macro-economic forces at play.

We must seek a proper balance between legislative action and market pressures.

We must identify easier and more effective ways to authenticate and verify.

We must provide clear and simple guidance on how we conduct business.

And the Government must create and enforce the laws created to enable stronger identity protections.

Let me conclude by asking for a show of hands of everyone who has a Social Security Number. Okay that's a good start.

Now let me ask everyone to reach into their wallets and purses and hold up their driver's license.

That's a pretty good showing.

Jeremy, they're all yours.