THE FUTURE OF IDENTITY IN FINANCIAL SERVICES: THREATS, CHALLENGES, AND OPPORTUNITIES

HEARING

BEFORE THE

TASK FORCE ON ARTIFICIAL INTELLIGENCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 12, 2019

Printed for the use of the Committee on Financial Services

Serial No. 116–49

U.S. GOVERNMENT PUBLISHING OFFICE

42–317 PDF WASHINGTON : 2020

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
WM. LACY CLAY, Missouri
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
BEN MCADAMS, Utah
ALEXANDRIA OCASIO-CORTEZ, New York
JENNIFER WEXTON, Virginia
STEPHEN F. LYNCH, Massachusetts
TULSI GABBARD, Hawaii
ALMA ADAMS, North Carolina
MADELEINE DEAN, Pennsylvania
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
DEAN PHILLIPS, Minnesota

PATRICK MCHENRY, North Carolina, *Ranking Member*
PETER T. KING, New York
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
ANN WAGNER, Missouri
ANDY BARR, Kentucky
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
DENVER RIGGLEMAN, Virginia

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON ARTIFICIAL INTELLIGENCE

BILL FOSTER, Illinois, *Chairman*

EMANUEL CLEAVER, Missouri
KATIE PORTER, California
SEAN CASTEN, Illinois
ALMA ADAMS, North Carolina
SYLVIA GARCIA, Texas
DEAN PHILLIPS, Minnesota

HILL, FRENCH, Arkansas, *Ranking Member*
BARRY LOUDERMILK, Georgia
TED BUDD, North Carolina
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
DENVER RIGGLEMAN, Virginia

CONTENTS

THE FUTURE OF IDENTITY IN FINANCIAL SERVICES: THREATS, CHALLENGES, AND OPPORTUNITIES

Thursday, September 12, 2019

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE ON ARTIFICIAL INTELLIGENCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 9:32 a.m., in room 2128, Rayburn House Office Building, Hon. Bill Foster [chairman of the task force] presiding.

Members present: Representatives Foster, Phillips; Hill, Loudermilk, Budd, Hollingsworth, Gonzalez of Ohio, and Riggleman.

Ex officio present: Representative McHenry.

Also present: Representative Himes.

Chairman FOSTER. The Task Force on Artificial Intelligence will now come to order.

Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of the task force are authorized to participate in today's hearing.

Today's hearing is entitled, "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities."

The Chair will now recognize himself for 4 minutes for an opening statement.

Thank you, everyone, for joining us today for what should be a very interesting hearing of the task force to explore the dangerous threats of identity fraud, how artificial intelligence (AI) is making it easier for criminals to engage in these activities, and how we can safeguard one of the most important things to have in our digital economy, and that is our identity.

Identity fraud is a hugely important problem in financial services. In 2018 alone, almost $15 billion is estimated to have been stolen from U.S. consumers online. This doesn't include the more indirect future costs of having a compromised identity.

Today, criminals have lots of tools at their disposal to get at sensitive consumer financial data. And there is a complicated situation that a Member of Congress finds themselves in, where we get briefings like the one I just received from Ms. Walraven where you go through just how massive the problem is and the techniques that are available, and we realize that mentioning them in public is not a wise thing to do. And so, this puts us in a tough situation.

But I urge all of the members on the committee here and their staff who are interested to get those briefings from members who are testifying today to just see how big of a problem this is, because it is costing us probably a lot more than that $15 billion.

There is a large number of tools that criminals are using today, things like phishing, ransomware, and malware attacks, that are already rife within financial services, and these cyber intrusions are only becoming more sophisticated.

In the news this week, there was the story of a voice synthesizer, an AI-enabled voice synthesizer that was used to generate fake instructions from what an employee thought was his boss to move money somewhere where it shouldn't have been moved. And that sort of attack is going to accelerate as the technology gets more advanced and more widely deployed.

And the stakes in this are enormous. With simply a name, address, and Social Security number, criminals use stolen identities to steal credit card numbers and bank account numbers, and to obtain fraudulent IRS and Medicare refunds. And the list goes on and on.

The financial services industry is on the frontlines of this attack. More than 25 percent of all malware attacks hit banks and other financial services organizations, which is more than any other industry.

In addition to the billions of dollars that financial institutions spend a year on cybersecurity, they also spend over $25 billion a year on anti-money-laundering and know-your-customer compliance, with large institutions spending up to $500 million annually.

Artificial intelligence is only enhancing the cyber criminal's arsenal. AI can be used more quickly to find vulnerabilities in a bank's software that can be used to impersonate someone's voice or face in a phishing scam, much like those deepfakes of which everyone is aware.

It can also be used for something that is called synthetic identity fraud. That is where criminals make up fake online identities by combining real and fake data from lots of different people, along with the Social Security number of a person, often a child, which they can buy very cheaply off the dark web or even the non-dark web.

These fake identities look completely real, and the criminals can use them to open new bank accounts and a record of new financial transactions that make the synthetic identity look more and more real.

And at the end of this, the unfortunate common practice is the so-called "breakout," where criminals simply take out a massive loan they never repay, or buy a car that they ship offshore. This sort of scam happens using these synthetic identities.

There are a number of things that we can do. I was very impressed by the roadmap produced by Jeremy Grant, one of our witnesses here, and his organization, the Better Identity Coalition.

So if someone only has time to read one document in this space, that is the one that I personally have found most useful. It provides a roadmap for what government can do to help, because I think that government has a unique role in provisioning the ID, that we ultimately should take a responsibility for maintaining a valid list of our citizens.

And I think that there has been a lot of motion, both by governments and motion in terms of the public perception of what is needed here.

This is one of the reasons why I am really eager to hear more from the witnesses in this hearing. And I guess, in light of the fact that we are unlikely to have a large amount of time because of votes maybe intervening, I think I will just cut off my comments here and turn it over to the ranking member of the task force, Representative Hill.

Mr. HILL. Thank you, Mr. Chairman, for convening the hearing today as a part of our Task Force on Artificial Intelligence. I know this is a topic that you particularly care deeply about. I am very interested in learning how our identity systems can be modernized in such a way that protects the privacy and personal information of all of our citizens, and I look forward to hearing from the panel today.

When we anticipate a digital world where we are distributing financial services products digitally through banks and nonbanks across the country, obviously, whether it is a mobile app or through the internet, through the web, this issue of authenticating someone truly that you are doing business with and that they, in turn, then are just granting you, the financial services company, access to their information for a particular purpose, all of this relates to how we identify people, how we authenticate people in the space.

And, of course, we have had Gramm-Leach-Bliley for many years now, but a lot of people who aren't banks or financial services players are not covered by Gramm-Leach Bliley. And so, this issue of how do we improve that and offer innovation is so important.

If we think about a digital world, you can't really have a completely digital process in 50 States in this country or internationally if you don't have not only the cyber protections that we are talking about in terms of the data being protected, but also that authentication process, so that individual user's identity.

That is why I think this hearing is so important to the work we are doing in the Financial Technology Task Force, and it is so important for our private sector players, and, I think, our regulators on how we enhance the robustness of identity. How do we do it, how do we authenticate people in a more effective way, and move way beyond the user name and password that has spent the last 20 years of repeating our pet's names and 1, 2, 3, et cetera, as a way to get into systems as helpful as maybe just a sharing app or as important as reviewing our financial lives online.

Also, the issue of data breaches is critical. And here the Federal Government doesn't have any better track record than the private sector. We have been in, this committee—I have been in Congress for 4½ years, and we have spent a lot of hours in this room talking about the incompetence of the Federal Government in protecting people's privacy and our data. So obviously, this is a key issue for both the public and the private sector.

Financial services companies, as Dr. Foster noted, are victim more to this kind of attack, 300 times more frequently than nonfinancial businesses, purely for really, though, obviously, for Willie Sutton's admonition that that is where the money is. But also, if

you are a state actor, that is where the disruption is a very vulnerable point in the Western world.

But thanks to advances in technology such as artificial intelligence and machine-learning, it is becoming increasingly easier to authenticate individuals and mitigate that kind of fraud. But we must be vigilant as policymakers to ensure that all of our sensitive information remains private.

I look forward to having the witnesses help us to understand these issues and what we might consider either legislatively or regulatorily to improve this process. And I look forward to the discussion.

With that, Mr. Chairman, I yield back.

Chairman FOSTER. Thank you.

And I would like to now yield 1 minute to Mr. McHenry, the ranking member of the full Financial Services Committee.

Mr. MCHENRY. Thank you.

Equifax, Capital One, what is next? How many breaches is it going to take before Congress takes appropriate action to view cybersecurity as a top priority and combating identity fraud as a top priority?

Only a few months ago, we had the world's biggest bank executives right here before us, and they identified cybersecurity as the chief threat to the financial system, not productivity, not growth at home, not political upheaval in Europe, not the slowdown in China, but cybersecurity.

What I appreciate about this panel, and I appreciate the work Mr. Foster has brought to the table here, because we begin with a bipartisan challenge, a challenge that we can then seek bipartisan solutions for here in Congress, and a new, innovative approach to this really cumbersome "dumb-passwords user-name" situation that we are currently in, and a new type of thinking that is occurring in the private sector, but to ensure the policymakers keep pace with what is happening in the private sector and further enable it and move this along much faster.

Thanks so much. And I look forward to your testimony.

Chairman FOSTER. Thank you.

Today, we welcome the testimony of Anne Washington, assistant professor of data policy, NYU Steinhardt School; Valerie Abend, managing director of Accenture Security; Jeremy Grant, coordinator of the Better Identity Coalition; Amy Walraven, president and founder, Turnkey Risk Solutions; and Andre Boysen, chief identity officer, SecureKey Technologies.

Witnesses are reminded that your oral testimony will be limited to 5 minutes. And without objection, your full written statements will be made a part of the record.

Ms. Washington, you are now recognized for 5 minutes.

STATEMENT OF ANNE WASHINGTON, ASSISTANT PROFESSOR OF DATA POLICY, NYU STEINHARDT SCHOOL

Ms. WASHINGTON. Chairman Foster, Ranking Member Hill, and members of the Task Force on Artificial Intelligence, I am grateful for this opportunity to speak.

Before I became a professor, I spent 8 years in financial services, in addition to many years working in support of this Chamber.

My name is Anne Washington. Now, why did I give my name? I gave you my name because it is an identifier, and digital financial services rests on its ability to guess who you are through identifiers like your name. Artificial intelligence goes further by taking actions based on a presumed identity, and those actions have serious consequences.

Today, I am going to explain why identity is important, why AI makes mistakes, because they are inevitable, and what we might do about it.

Consider a firm with an AI system that works 99 percent of the time. That is great, right? But actually, in a business of 10 million people, clients, that means it fails on 100,000 people: 100,000 people who cannot get credit in an emergency; 100,000 families who cannot get a home mortgage and build wealth; 100,000 entrepreneurs who cannot get a start in a small business.

My examples focus on individuals, but let's not forget that owner-operators who are individuals with their own business face even greater financial risks.

Much of the data technology today was originally designed for marketing purposes. So if I get a wrong coupon or a useless ad, it is cute. It is a momentary curiosity. In financial services, the stakes are higher. A digital mistake is detrimental, and it is ongoing.

A few items from the news. Jennifer Norris of Boston routinely was in danger of losing her job because of an inability to resolve a dispute about her identity. A teacher in Maryland had to give up her livelihood because she was in a profession that required continuous recertification.

As depicted on this slide, this New York novelist sees herself in all of her daily roles—an author, a parent, a friend. She probably does not see herself primarily as a New York driver. The next slide shows you how a computer sees her. She is just the information on this slide, primarily a name and a birth date. Yet, someone else in New York has the exact same name and the exact same birth date.

The "Lisas" have no recourse to resolve this confusion. No organization can fathom the likelihood of this coincidence. A data double is what the scholar, Evelyn Ruppert, calls them, and that is somebody who has the same identifiers, but it is not you.

Now, I am a computer scientist with a degree in business. I am going to tell you that I think this stuff works. But I can also tell you that there is little financial incentive to fix these mistakes, because mistakes will happen. It is mathematically certain, in fact.

You can just go to the final slide.

What are the chances that you are going to meet someone who has the same birthday? Actually, it is really high. It only takes 23 people in the same room. Probably in the members of this committee and your staff, there are two people who have the same birthday. If you go up to at least 75 people—I don't think we have that many here—it is 99.9 percent certain. Coincidences are not as rare as we perceive them to be.

So, what can be done? Artificial intelligence identifiers built for a global audience need to scale. That means we have to respect naming practices that come from different religious traditions or different cultural traditions, or even non-Latin characters.

Finally, I am going to argue that we need a way to get feedback back into identity systems. As a technologist, I want to know how I can improve and also incrementally make these systems better. It could also help lead towards procedures for handling errors and exceptions.

One example is the MiDAS system in Michigan which accused jobless people of fraud without recourse. And that is one example of the way that AI systems need a feedback mechanism.

Now, I argue that the authority of human experience must balance the authority of data. Why? Because stats happen.

And experience matters. Each of you has someone in your district office who does case work. Why is that? That is a recognition that institutions sometimes obscure the needs of individuals.

What will be the resolution process for identity disputes in artificial intelligence?

[The prepared statement of Dr. Washington can be found on page 79 of the appendix.]

Chairman FOSTER. Thank you.

Ms. Abend, you are now recognized for 5 minutes to present your testimony.

STATEMENT OF VALERIE ABEND, MANAGING DIRECTOR, ACCENTURE SECURITY

Ms. ABEND. Chairman Foster, Ranking Member Hill, and members of the task force, my name is Valerie Abend, and I lead Accenture's security practice for our North American financial services clients. Thank you for the opportunity to join you here today. I really commend this task force for holding a hearing to explore the importance of digital identity and its intersection with artificial intelligence.

Innovation in digital identity and access management is incredibly important to cybersecurity, to enhancing privacy, and to ensuring trust in financial transactions. We live in a digitally connected world where customers' demand for efficient and accurate transactions continues to increase.

From taking out a loan or paying my child's babysitter, most of these happen online. And key to these transactions is trust, trust that the individual we are conducting business with online is whom they say they are.

However, the information we use to validate our identities now is widely available through dark web forums and social media postings, making us more vulnerable to spearphishing campaigns.

Simply put, identifying yourself online through passwords, usernames, and security questions is no longer working.

I would like to draw the members' attention to the slide on the screen that lists five global cyber threats to financial services as outlined in a recent report that we published.

Credential and identity theft is first, because it is at the root of almost every breach. Not only are cyber criminals really good at fooling people through spearphishing to gain access into enterprises, but once they are inside these networks, they compromise other access credentials, moving throughout the company, learning how they operate, and ultimately gaining access to privileged data

and systems. I like to call this access inside of systems the "mushy middle."

One of the best known examples is the 2016 cyber heist from the Bangladesh Central Bank, where attackers stole $81 million. That was more than 3 years ago, and hackers are building new capabilities to commit their attacks in ways we haven't even thought of yet.

This is why we must use innovations, including AI, to thwart them at the speed that cyber attacks occur. Attacks leveraging credential theft, as we saw in Bangladesh, will remain possible until we fundamentally change the way enterprises manage employee and customer access and how they detect and respond at machine speed when they sense that something is amiss.

Today, we can use AI to enable financial institutions to have a more accurate picture of employee access across a complex enterprise. Through these tools, managers can make better decisions of who should have access, to what systems, and to what data in real time, thus managing this mushy middle.

On the customer-facing side, leading organizations are leveraging biometrics, AI behavioral-based analytics, and multifactor authentication to make real-time risk-based authentication decisions to approve transactions and set limits around those transactions. In the blink of an eye, a financial institution can make complex risk management decisions about whether a person using their mobile apps is, in fact, their actual customer.

This customer risk management approach is not just in use in the United States and other developed countries, but also in emerging economies where these new tools are providing secure online identities.

For example, we at Accenture are part of the ID2020 Digital Identity Alliance, which was formed to develop a reliable digital identity for people in developing countries so they can confidently receive government services and validate their identities to employers, schools, and other service providers.

These digital identity advances provide individuals with more security and control over their data, giving them the ability to decide who to share their personal information with, what to share, and for how long it can be shared.

Congress' help would greatly benefit our nation's ability to improve digital identity as a cornerstone for better and safer online transactions.

First, Congress needs to pass a national privacy law, which will build consumer confidence and trust in the digital economy while enabling the private sector to gain wider adoption for more secure products and services. A good starting point for this is the framework released by the Business Roundtable last year under the leadership of our CEO, Julie Sweet.

Second, Congress should help foster an environment for digital identity innovation through proofs of concept that enable the testing of new capabilities and their ability to scale.

And, third, I encourage you to ensure that any new laws designed to advance digital identity or cybersecurity be technology-neutral and interoperable with other sectors.

So in conclusion, Mr. Chairman, there is much work to be done to build a digital identity ecosystem that thwarts cybersecurity attacks, improves privacy, and ensures trust.

I want to thank you again for the opportunity to discuss these issues, and I look forward to your questions.

[The prepared statement of Ms. Abend can be found on page 34 of the appendix.]

Chairman FOSTER. Thank you.

And now, Mr. Grant, you are recognized for 5 minutes.

STATEMENT OF JEREMY GRANT, COORDINATOR, BETTER IDENTIFY COALITION

Mr. GRANT. Chairman Foster, Ranking Member Hill, members of the task force, thank you for the opportunity to testify today. I am here on behalf of the Better Identity Coalition, an organization that was launched last year, focused on bringing together leading firms from different sectors to work with policymakers to improve the way that Americans establish, protect, and verify their identities when they are online. Our members include recognized leaders from financial services, health, technology, FinTech, payments, and security.

Our 22 members are united by a common recognition that the way we handle identity today in the U.S. is broken, and by a common desire to see both the public and private sectors each take steps to make identity systems work better.

Let me say up front that I am grateful to this task force for calling the hearing today. The way we handle identity in America impacts our security, our privacy, and our liberty. And from an economic standpoint, particularly as we move to high-value transactions in the digital world, identity can be the great enabler, providing the foundation for digital transactions and online experiences that are more secure, more enjoyable for the user, and ideally, more respectful of their privacy.

But when we don't get identity right, we enable a great set of attack points for criminals and other adversaries. A whopping 81 percent of cyber attacks are executed by taking advantage of weak or stolen passwords. Eighty-one percent is an enormous number. It basically means that it is an anomaly today when a breach happens and identity did not provide the attack vector.

And outside of passwords, we have seen adversaries seek to steal massive datasets of Americans. In large part, they can have an easier time compromising the questions that are used in identity verification tools, like knowledge-based verification (KBV) solutions.

A key takeaway for this committee to understand today is that attackers have caught up with many of the first-generation tools that we have been using to protect, verify, and authenticate identity. Now, there are a lot of reasons for this, and there is certainly blame to allocate. But the most important question is, what do government and industry do about it now?

That is a key point, government and industry. If there is one message I think this task force should take away from the hearing today, it is that industry has said they cannot solve this alone. We are at a juncture where the government will need to step up and

play a bigger role to help address critical vulnerabilities in our digital identity fabric.

Last year, the Better Identity Coalition published a policy blueprint which outlined a set of key initiatives that the government should launch to improve identity that are both meaningful in impact and practical to implement. A few highlights:

First, when talking about the future of the Social Security number (SSN), it is essential to understand the difference between the SSN's role as an identifier, essentially a number that is used to sort out which Jeremy Grant I am among the hundreds of us in the U.S., and its use as an authenticator, which is something that is used to prove I am really me, this particular Jeremy.

SSNs should no longer be used as authenticators. This means that, as a country, we stop pretending the number is a secret or that the knowledge of an SSN can actually be used to prove that someone is who they claim to be.

But that doesn't mean we need to replace them as identifiers. Instead, let's start to build systems that treat them like the widely available numbers that they are today. I have yet to see any replacement proposal around SSNs that does not involve spending tens of billions of dollars confusing hundreds of millions of people and not really giving us much security benefit.

Second, on the authentication topic, there is good news here. Multi-stakeholder efforts, like the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium, have developed standards for next-generation authentication that are now being embedded in most devices, operating systems, and browsers in a way that enhances security, privacy, and user experience. The passwordless era is near, and government can play a role in accelerating the pace of adoption.

Third, government will need to take a more active role in working with industry to deliver next-generation remote ID proofing solutions. Now, this is not about a national ID, and we are not recommending that one be created. We already have a number of nationally recognized authoritative government ID systems: the driver's license; the passport; the SSN.

Our challenge here is what I call the identity gap, that all of these systems are stuck in the paper world while commerce is increasingly moving online. So to fix this, America's paper-based system should be modernized around a privacy-protecting consumer-centric model that allows a consumer to ask a government agency that issued a credential to stand behind it in the online world by validating the information from that credential.

So, how would this work? As the animation that is up on the screen from our policy blueprint demonstrates, it is about creating a new paradigm for digital identity that starts with the needs of the consumer.

Here, we will start with someone named Stacy who is trying to open a bank account online. She provides some basic identify information. But since she is not there in person with a physical ID, the bank doesn't really know if it is her or, for that matter, whether she is a real person at all.

So, Stacy will ask somebody who already knows her, the DMV, to help her prove that she is who she claims to be. She will launch

a mobile driver's license app on her smartphone. She will unlock it with an on-device biometric match, say, touch ID, which then unlocks a cryptographic key that is in the phone that can securely log her into the DMV to make this request.

Now, because that app was securely issued to her phone at the time she got her driver's license, and because she unlocked it with her biometric on the device, there is now a chain of trust in place which allows that DMV to know it was Stacy who was actually making the request. With that secure authentication and authorization, the DMV and the bank can then set up a secure connection, and the DMV can validate her identity.

Note that this concept was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity, as well as a recent White House OMB memo published in May.

I appreciate the opportunity to testify today. Note that I have submitted lengthier testimony for the record as well as a copy of our policy blueprint.

Thank you.

[The prepared statement of Mr. Grant can be found on page 49 of the appendix.]

Chairman FOSTER. Thank you.

Ms. Walraven, you are now recognized for 5 minutes.

STATEMENT OF AMY WALRAVEN, PRESIDENT AND FOUNDER, TURNKEY RISK SOLUTIONS

Ms. WALRAVEN. Thank you, Chairman Foster, Ranking Member Hill, and members of the task force, for the opportunity to appear before you and provide my testimony today to help inform discussions on the future of identity in the financial services sector: threats, challenges, and opportunities.

I am the founder and president of Turnkey Risk Solutions, and prior to starting that company I spent 20 years in the financial services sector at a lot of large institutions. The last 10 years of my career, I was at JPMorgan Chase, where I was responsible for establishing the business practices specifically focused around proactive identification, mitigation, and remediation of various fraud threats that included credit bust-outs, synthetic identities, identity manipulation, and credit abuse.

As we consider how to utilize artificial intelligence and machine-learning to navigate big data to identify consumers, it is important that we clarify our target by gaining a more comprehensive understanding of what synthetic identities are. I have been asked to provide the committee a brief overview of the factors that contributed significantly to their emergence in order to better frame the threats and challenges that we are facing.

For the purposes of my discussion, Chairman Foster, you covered that a synthetic identity in its basic form is a Social Security number, a name, a date of birth. But it is important to note that creating a synthetic identity is materially different than traditional identity theft.

In cases of traditional identify theft, the criminal impersonates a real person to open an account or take over an existing relationship. But in cases of synthetic identity, the criminal is using just a limited amount of elements of a true person's identity, for exam-

ple, just their Social Security number, and then they pair that with a name, a different date of birth, and an address that they can control, and create a completely separate and distinct persona. And that is intentional. They do not want to commingle with an existing person.

Once that synthetic has been created, you can use it for just about anything you can use a conventional identity for. Obviously, products in the banking service, but you can also create a social media account, insurance products, rent an apartment, obtain utilities, or enroll in benefits programs. You can basically use it for any purpose that the creator intended and whatever they are controlling it for.

To better understand the threat of synthetic identities, I think it is important to understand the landscape that is influencing them.

Technology plays a huge role. Advances in technology have created speed and convenience, but at the same time, they have created anonymity for the fraudsters. We are also asking an infrastructure that was built a long time ago to do more and more things that it wasn't intended to do, without really being able to keep up with the technology and the threats that are in the landscape today.

Consumer awareness. Consumers are a lot more educated on understanding the importance of their credit, understanding the different ways to be able to protect their identifiers, and being able to stay away from compromising their information. That information has been put out to help protect consumers, but it has also been used by organized criminals and different criminal actors to be able to understand how the infrastructure works and to be able to design their attacks specifically to exploit those types of avenues.

Regulations and new controls have done a lot to protect identity theft victims and have done a lot to make sure that they have ways to remediate when they have been victimized. We have seen those same protections, however, exploited, leveraged, and abused by criminals.

We have done a lot to try to make sure that we can erase and eradicate anything that has been related to an identity thief. But when it comes down to actually having a synthetic identity, those same protections have been leveraged by them.

Data breaches were originally focused on compromising credit and debit data. And once we put the chips in the cards, that information was then as useful as it had been in the past. So now, they had started to move to PII, more static information, people's names, people's Social Security numbers, people's dates of birth.

All of these factors played a major role in an emergence of use of synthetic identities. This fraud threat was specifically engineered to evade existing controls while exploiting vulnerabilities in the financial services system and beyond, impacting other verticals.

Many of the groups committing this type of fraud are highly organized, extremely sophisticated, and tend to be transnational in nature. These adversaries are focused, committed, well-funded, and have access to the same technological advances as we do.

As an industry, we must be proactive in our actions, unified in our defenses, and more effective in our application of evolving technologies, including artificial intelligence.

As we seek to deliver unprecedented speed and convenience to increasingly mobile and technology-dependent consumers and businesses, we must remain vigilant in understanding the threats to our interests and to our infrastructure.

Synthetic identity fraud in the United States and around the world is widespread and inconceivably pervasive. It is being amplified by increased digitalization of products and processes. And when you couple that with a proliferation of available data, synthetic identity fraud readily operates across all delivery channels, providing the perpetrators with potentially unfettered access to our nation's financial system and Federal programs, making it essential that we act in a unified and collaborative manner to protect the integrity of our infrastructure.

In order to do so, we must recognize the complexity of these next-generation frauds and be fully informed of their severity and their scope. Advances in technology alone cannot identify and resolve these issues. Mitigation efforts from industry and government must be fluid and nimble to ensure we have the ability to effectively address these issues with the urgency they deserve.

Our control framework needs to be updated to specifically address synthetic identity fraud. It needs to be universally defined in order for institutions to be able to detect, report, and remediate it.

Thank you very much. I appreciate the opportunity, and I look forward to any questions you may have.

[The prepared statement of Ms. Walraven can be found on page 76 of the appendix.]

Chairman FOSTER. Thank you.

And, Mr. Boysen, you are now recognized for 5 minutes.

STATEMENT OF ANDRE BOYSEN, CHIEF IDENTITY OFFICER, SECUREKEY TECHNOLOGIES

Mr. BOYSEN. Chairman Foster, Ranking Member Hill, and members of the task force, thank you for the opportunity to discuss the future of digital identity with you today.

I am Andre Boysen, the chief identity officer at SecureKey Technologies, and I look forward to sharing our experiences in building a nationwide privacy-based digital identity network for Canadian consumers that works across the economy.

SecureKey is a Canadian company that is a world leader in providing technology solutions to enable citizens to easily access high-value digital services. We focus on the intersection of the citizen, the public and private sectors, privacy, and consent.

Digital identity is not just about citizen expectations. Companies, governments, and other organizations have strong incentives to move transactions online to realize cost savings, enhance customer experiences, and increase business integrity. An organization's ability to do this hinges on a single question: Can I trust the person or the digital identity at the other end of this transaction?

As Jeremy has already said, identity is broken and it is equally problematic for citizens and for business. To recognize clients and provide trusted access to services online, organizations typically deploy a mix of analog and digital measures to confirm identity and mitigate risk. As we have seen, however, these solutions tend to be complex and are not fully effective.

On the other side, citizens are asked to navigate a continuously changing kaleidoscope of identification methods to satisfy the onboarding needs of the organizations from which they seek services. All the while, we all read newspaper stories every single day about data breaches and online impersonators.

There is reason to be concerned. Fraudsters are collecting information to know as much, sometimes more, than the citizens that they are impersonating. Standard physical cards for a paper-based world are easily counterfeited and it's often impossible to check the document validity with the issuing sources.

Even biometric methods, which have been presented as a digital solution to digital fraud, are increasingly being targeted by hackers. Unlike passwords, you can't change your biometrics. You can easily be tricked out of a selfie.

Our collection of siloed systems are too hard for consumers to use. It is not solving the problem, and it is too expensive to be sustained. It is every web service for itself.

Consider the CEOs of Twitter and Facebook, Jack Dorsey and Mark Zuckerberg. These two digital leaders know how the system works, understand digital identity best practices, and have all the resources in the world at their fingertips. Yet, even they have problems controlling and managing fraudulent access to their digital identities.

Mr. Zuckerberg's problem was self-inflicted, while Mr. Dorsey was failed by the telco he relied on when he became the victim of SIM swap fraud.

If they can't manage and be protected in the current digital landscape, how are the rest of us supposed to manage?

Urging greater online security vigilance has passed the point of diminishing returns. It needs to be said that there is no organization on the planet that can solve digital identity on its own. It takes a village to make digital identity work, each player playing to their strengths and combining to create trust greater than the sum of the parts.

The Canadian model is a public-private partnership between financial institutions, telcos, governments, and other trusted partners. It is a give-to-get model.

For example, governments are the foundational issuers of identity documents in the form of birth registries and immigration documents. Governments also link their records with a photo to a living person by issuing a driver's license or a passport.

But governments aren't as adept as the commercial sector at knowing if the person actually is at the end of a given digital transaction. The IRS has a file on everyone in this room, but they would be hard-pressed to point any of us out in a crowd. That is why they use knowledge-based authentication (KBA).

This brings us to financial institutions who complete billions of authentications per year. Compared to other organizations, citizens only rarely interact with government during their daily lives. They may renew their driver's license or passport every 5 years. But they will log into their bank account several times per week. This increases the integrity in their transactions for banks.

And our mobile devices are always within reach. The carriers have some security features that are important and that are tied

to subscriber accounts. Verified.Me is a service that is offered by SecureKey Technologies, that is built on open standards. Verified.Me was developed in cooperation with seven major financial institutions in Canada. It is a first-of-its-kind service that takes a village approach to solving the digital identity problems we have been talking about today with greater simplicity, higher integrity, greater cost efficiency, and better privacy.

With the information and resources already available, we have helped to solve the digital identity problem in Canada, and have developed a model we think will work around the world. Some of our leadership and collaboration partners include Global Privacy and Security By Design developed by Ann Cavoukian, the U.S. Department of Homeland Security, the Science and Technology Directorate under Anil John, and the Digital ID and Authentication Council of Canada.

Thank you for the opportunity to share my comments with you today.

[The prepared statement of Mr. Boysen can be found on page 45 of the appendix.]

Chairman FOSTER. Thank you.

I will now recognize myself for 5 minutes for questions.

Mr. Grant, one of the things that impressed me in your testimony is the bipartisan nature of the support for this. You were very involved in the Obama Administration's initiative on secure online digital ID. And it appears as though OMB and the current Administration is actually strengthening those initiatives.

Could you just sort of briefly outline what the recent history of government involvement is in strengthening citizens' ability to authenticate themselves online?

Mr. GRANT. Sure. As you mentioned, I spent several years in government leading an Obama Administration initiative, the National Strategy for Trusted Identities in Cyberspace (NSTIC), although I was a civil servant when I was there and stationed up at NIST, up the road, where I served as their senior adviser for identity management and ran the program.

This has never been a partisan issue, as you point out, and it is great to see that tradition continuing today in this task force hearing.

Much of what the NSTIC program, as it was known, was focused on was how to basically catalyze a marketplace. The idea was that the government's role, the way things are in the U.S. should be limited, but government should play a role where there might be gaps to fill. And there was a lot of good work that was done then that I would say is now flowing into the work that we are driving in the Better Identify Coalition in terms of looking to carve out an appropriate role for the government without one where there is too much of a role for the government.

As I mentioned in my written statement and opening statement, in May the Office of Management and Budget signed Memorandum 19–17 into effect, it is about 13 pages, updating a lot of the government's cybersecurity policy as it impacts identity. And we were really excited to see that they took one of our key recommendations, basically calling for agencies to create, I think the language was privacy-enhanced APIs, which would allow consumers to ask

that an agency validate identity information about themselves either for public or private sector applications.

I think now that that is in place, there is a good policy foundation in place for the first time in the U.S. to actually start to bring government into play more of this role for consumers and businesses.

Chairman FOSTER. Thank you.

And, Ms. Washington, Ms. Abend, you both touched on in your testimony the fact that the lack of a way to authenticate yourself falls most heavily on those who are not wealthy, in developing countries, that one of the real improvements in the quality of a citizen's life comes from having a way to authenticate themselves and prove who are they are. This sounds sort of counterintuitive, and I was wondering if you could add a little bit about why this is.

Ms. ABEND. It is interesting what we found, if you look at some of the things that even the Chair of the FDIC has said recently in some of her public comments about how individuals who are unbanked or underbanked have cell phones and they use those phones to conduct their financial transactions.

And so, if we could establish the kind of confidence by having, as I put in the recommendations, a national privacy law, I think we would go a long way to engender trust so that they have certain protections through that national privacy law and a much less complex way of understanding what those protections are while also being able to use the tool that is in their hand to be able to validate themselves for financial transactions. And through that process, would give them access to financial transactions in a safe and sound manner.

Chairman FOSTER. Ms. Washington, do you have anything to add?

Ms. WASHINGTON. I just want to say that right now, without a standard way and a standard procedure for disputing authentication issues, people who feel powerless in society are probably not going to figure out how to dispute it. So by default, we are not going to have equal access to resolving disputes.

Chairman FOSTER. I think there is probably also a tendency for wealthy people to have a more established financial transaction record that can be used in a sort of secondary way to make sure that the person is real and so on.

Ms. Walraven, do you have anything to add there?

Ms. WALRAVEN. I think we also have to take into consideration that for all the things that we are putting in place to protect consumers, and they are all very valid, there are much easier ways to take a step back and go through and negotiate the system.

I think all the controls that we are putting on for artificial intelligence and authentication, it starts at the front. You need to know who that person is, and then you go through and do the authentication. So we need to go further up the chain and make sure that identity is actually factual first, and then you can build a lot of controls behind it.

But we need to get to the root of the issue instead of just addressing, in some cases, the symptoms. I think that is really how we can get much more collaborative between industry and government. And I definitely think we need to do that, because the cur-

rent infrastructure is doing a good job with what it can, but we need to reshape the issue and look at it from a different lens.

Chairman FOSTER. All right. Thank you.

The gentleman from Arkansas, Mr. Hill, the ranking member of the task force, is recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman.

Before I begin my questions, I would like to ask that something be submitted for the record. One area that has been concerning to our title industries across the country is business email compromise, which is just another commercial form of fraud. And in that regard, I would like to submit a letter from Chairman Powell, as well as the response he had on this issue and how important it is. I would like to submit that for the record.

Chairman FOSTER. Without objection, it is so ordered.

Mr. HILL. This has been a really good panel. And as I said, we are trying to correct the world we live in and prepare for the world in the future. And we can't do that without this strict privacy standard and the ability to authenticate whom it is that we are doing business with. I thought each of you had great opening comments, and I am grateful for that.

And I was pleased to hear, Mr. Grant, you talk a little bit about OMB's issue, because one thing this panel has heard, and our FinTech Task Force has heard consistently is the dangers of data scraping and that that is not a best practice out in the FinTech world for accessing customer data.

Can you reflect, will OMB's policy impact that in the government sector? And is it a good standard for the private sector to adopt?

Mr. GRANT. I think the new OMB policy, assuming that there is some follow-up to actually get more agencies to start providing that to validation services online, will help to contribute to some of the challenges we have seen in open banking where you have different FinTechs who might want to scrape financial data.

But there, I have been really impressed by the work of the Financial Data Exchange. It is a group that was incubated in the FS-ISAC, the Financial Services ISAC, that does a lot of cybersecurity work. And they brought together banks and FinTech firms to work on essentially coming up with a standard API that leverages well-known standards like FIDO, OAuth, and OpenID Connect, that will allow a consumer to decide to essentially securely grant certain access rights to some of their financial data.

Because identity is that core control that is there, if we are able to enhance some of the ways we do identity verification through that API with some of the things that the government can provide, I think we are going to have more robust solutions all across-the-board.

Mr. HILL. That is very helpful.

And, Ms. Walraven, this issue of synthetic identity, could you explain that a little more? I looked at your testimony and listened to you. But are you suggesting that people are just aggregating a good cell number, a good address with a different name and a different Social Security number, so they are not imitating the exact person, they are creating a new synthetic individual, and so they are just using all validated information? Is that what you are suggesting?

Ms. WALRAVEN. Similar. So, basically, a synthetic can use someone's real information, let's say, a Social Security number, either yours, or a child's Social Security number. And then, what they will do is they will take that, add a name that is different than the real person's name, and add a date of birth. And if they are going to go in person somewhere, they probably would make it closer to probably what is more likely for them. And then put at an address that they can control. And basically from there, they create a completely separate and distinct identity.

So it is not real per se as far as it has been a real person. It is a real person doing it, potentially, but it is not a real identity. But it functions, especially in a digital and in a paperless area, exactly like a real identity.

And when they create that, they know their mother's maiden name, they know the user ID and password, they know the different security questions, because they created them. So when you go to do the authentication afterwards, you are not going to catch them in the existing infrastructure that we have, because those credentials are known to them.

Mr. HILL. Thanks for your contribution to that.

Mr. Grant, I read recently about the beginning of the implementation of the California statute. And for the 4½ years I have been in Congress, we have debated privacy and data breach notification here and witnessed the battle between retailers and the financial services industry, which grows tiresome here on this committee, and the desire to have a 50-State solution, which would be great in a digital world if we could do that.

So now, California has acted. I am interested in your views. Is the California Consumer Privacy Act (CCPA) a net positive for the consumer? Is it a decent basis in terms of the definitions they struck, the approach they took, for the Federal Government to consider?

Mr. GRANT. I think CCPA writ large, I guess we will have to see how its implementation goes and whether it is a positive for the consumer.

There is a couple of things on the identity side that I have been very concerned about, including the fact that it took kind of an ambiguous approach to whether you can use data for security and fraud prevention.

As background, the General Data Protection Regulation (GDPR) over in Europe did, I thought, a pretty good job saying, look, if you are using data for marketing purposes or other things, all of these rules apply. But if I am analyzing data I am able to capture about the way you are interacting with a device, well, that is for security or fraud presentation only, so that is okay.

In California, they took a little bit of a different approach. And I think part of this might have been because the law was written in about a week. I think the history of it was they were trying to head off a ballot initiative. They said that a consumer cannot go to a company that has information on them that is being used for security and fraud prevention and ask that that information be deleted, which is good. But they did not go ahead, you couldn't actually go to a company and opt out of that information being used at all.

And so the concern there is that if, say, even 2 percent of people go to companies and basically tell them to turn off the security analytics controls that are some of the best tools we have today to prevent things like credential stuffing attacks or other spoofed identities, it is going to put people at risk, consumers at risk, and businesses at risk.

Mr. HILL. Thank you very much.

I appreciate it, Mr. Chairman.

We will come back to it. Thank you.

Chairman FOSTER. The gentleman from North Carolina, the ranking member of the full Financial Services Committee, Mr. McHenry, is recognized for 5 minutes.

Mr. MCHENRY. Thank you.

This has been great testimony, an informative panel, and I think it is quite constructive, again, quite constructive for what has been, as Mr. Hill outlined, a rather tiresome debate between retailers and banks on who holds the bag, without talking about progress or fixing the problem. They want Congress to intervene and make the decision on who gets sued.

So, let's get beyond that. Let's get to the solution.

Mr. Boysen, I would like to hear the story of what your company is doing in Canada to verify identity and the undertaking that you and your company have had.

Mr. BOYSEN. Thank you.

There have been two generations of services that we have launched in Canada. The first one was in 2012, and that we did with the Government of Canada. It was designed to be a safe replacement for multiple user IDs and passwords.

In 2012, the problem the Government of Canada had is every time I, as a Canadian, went to our tax authority, every single time, I forgot the password. And so, their challenge was how to authenticate me. They can't do what Amazon does. They can't do an email password reset. They have to send secure mail to my house.

Being a busy Canadian, I solved my tax problem with them another way. And they sent me this thing 2 weeks later. I don't send it back in, and I come back here next year and do the same thing. That cost them 40 bucks a shot.

Between the period 2004 to 2012, they spent $970 million authenticating 5 million Canadians. For the subsequent period, from 2012 to 2018, their costs have come down to roughly $200 million in order of magnitude in savings. The reason is that Canadians now are able to use their bank account to get to the government. This has been transformational.

The reason this works better is because Canadians are in their bank account every single week, so they are not going to forget the password. More importantly, if they do forget the password, like, if they can't get in, they are on DEFCON 5, they are going to run down to the bank right now because they are terrified their money is going to be lost, and it is that self-interest that has actually increased the integrity of the transactions.

The challenge with that service, however, is that it was authentication only. It didn't solve the identity problem. So in May of this year, with all of the major banks in Canada and several other trusted partners, we launched an identity service. It allows me to

prove my identity in a trustworthy way based on bank, telco, and government data that I authenticate with each of those providers myself. And then I am able to, under my control, give that to someone else when I want sign up for a new service.

So this actually increases integrity for all of those end points and takes their cost down and gets them better results, too.

Mr. MCHENRY. Okay. So, verify me. I use blockchain technology. Walk us through that.

Mr. BOYSEN. We didn't start off saying, blockchain is cool, let's use it. We came at it from a very different point of view. If any organization is consuming data from a network to confirm my data, they have three requirements that need to be met.

Requirement number one is they want to know the data came from an authoritative source, somebody they would know and trust today, like a government-issued ID.

The second requirement that they want to know is they want to know the data has not been altered since it was written by that authoritative source; the crook didn't take my driver's license, take all my data, scratch my photo, and stick their photo on it.

The third requirement they have is they want to know that the data belongs to the person presenting it.

So, let me answer your question about, why blockchain? Blockchain does three very specific things. The first thing is it allowed us to implement this thing we call triple blind privacy. In Canada today, when I use my bank account to get to the government, the bank account does not get to see my online destination. The government in its place knows that I came from a tier one bank in Canada but not which one. And our company, which operates the network, we don't know who you are. Triple blind privacy says not the bank, not the government, not SecureKey got a complete picture of the user journey.

When we tried to go do that with identity, the problem is, with us in the middle, we were going to get to see a lot, and we wanted to figure out a way to do triple blind identity so I could send my data from Wells Fargo to the IRS without Wells Fargo knowing it went to the IRS, without the IRS knowing it came from Wells Fargo, and without us seeing anything in between.

So, it gave us a method to implement triple-blind privacy. The second thing is, it allowed us to meet the integrity challenge to verify and meet those three requirements that I talked about. And the third side benefit is we get resiliency because there are so many nodes it is harder to mount a denial-of-service attack.

Mr. MCHENRY. So broadly, that cryptography, the blockchain cryptography, is this leap forward in order to ensure that you can have that movement of data.

But here is a different question. Is there a different cultural assumption between folks in the United States versus folks in Canada about their digital identity and that willingness to share that data?

Mr. BOYSEN. I would say the stance of Canadians and Americans is very similar on this front. I would say that the privacy regulations in Canada are generally better, and so that gives Canadians confidence when they are doing this. They have recourse. If some-

thing negative happens, they have somewhere to go and get it sorted. So, I would say the model would work here, too, is my sense.

Mr. MCHENRY. Excellent. Well, let's get at it, right? Pitter patter, let's get at her. Let's make some progress here.

Thank you for a great panel. It was highly informative. I have 3 hours more of questions, but every one of you are top notch.

Thank you for being here.

Chairman FOSTER. Thank you.

And the gentleman from Georgia, Mr. Loudermilk, is recognized for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

Thank you to all of you on the panel here. This is intriguing, coming from an IT background. I have been dealing with cyber issues for quite some time from my time in the Air Force dealing with intelligence data all the way up through even protecting businesses and school systems with internet accesses.

It is an ongoing challenge. And transactions that happen, especially in the financial services sector, happen at incredible speeds. Therefore, verification for those who use this has to be done at the same speed.

I am one of those guys who likes using cash. I like reading a printed book. I like going to a store and putting my hands on what I am going to buy. I am unique in the world today, as I found out the younger you are, the more you are relying on the technology. So, we have to be exploring these areas.

Before I get to my questions, though, Mr. Chairman, I would like to submit for the record a letter from the Consumer First Coalition addressing concerns and congressional oversight over the electronic consent-based Social Security verification system as they move forward.

Chairman FOSTER. Without objection, it is so ordered.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

Ms. Washington brought up a very interesting scenario at the beginning of this, which I think illustrates some of the challenges that we do face. But I have one that I found quite unique.

I was taking a group to the White House. And if you have ever visited the White House, they have quite a verification system to go through. If there is one thing wrong, you are going to get pulled out and put in a holding area.

A young lady I was with, who was probably in her early thirties, was pulled out and put in a holding area. It kind of surprised me, and so I went to talk to her.

She said: "Oh, this happens all the time."

"Really?"

"Yes. I have an identical twin sister. My mom didn't realize that she was going to have twins, and she had already chosen the name, so she gave us both the exact same name."

And I am going to use a different name, but it was Elizabeth Grace Smith. One was called Liz, the other was called Grace. They have the same name, the same birthday, the same birth location, the same hair, the same height, the same weight. What triggered the Secret Service was their Social Security numbers were off by one digit.

So. there was this delineator. This is a real illustration of the type of thing that we are going to encounter, as Ms. Washington had brought up, but we have to find a path to get there.

And one of the things—I am big on innovation. I am big on sandboxes so we can go out and explore ways to do this, but it has to be done in a controlled environment to protect consumers but yet have the ability to do these things.

Ms. Abend, it took us a while to adopt the chip payment system. Traveling in Europe, they had it a long time before we were able to adopt it here. But from what I understand, it has reduced the counterfeit fraud by about 87 percent.

But the bad players, the criminals now focus on digital payments, which involve digital identities. We need cybersecurity solutions to combat these digital payment frauds.

Are we heading in the right direction? Do we have the sandbox available to develop these?

Ms. ABEND. Congressman, that is an excellent question. And I remember distinctly, when I was actually back working at the Office of the Comptroller of the Currency, when the deadline was approaching for a chip and pin and the conversations, because we had just faced the breach with Target and actually had to appear before Congress to testify on cybersecurity at that moment in time as well, and I remember distinctly having this conversation about what it would do and what it would not do.

And as we have seen overseas, the card-not-present fraud goes through the roof, right? Bad guys know. And all of these online transactions, they are card not present, and that means they are missing that authentication aspect of being present with that chip and pin.

And I think that, while it was a step in the right direction and it was just a layer, the fact that most of our transactions are increasingly online and need to happen at the speed that we have discussed here, we do need to create an environment that fosters more innovation, that figures out a way to improve the state of synthetic IDs, as my colleague here has talked about, that creates that more trust that we have talked about here, and do it in a way where people can protect all consumers and everyone can get bought into that system.

And I think that is why my colleague, Jeremy, and the Business Roundtable that I mentioned earlier that has over 200 CEOs, have a lot of alignment around what needs to be done to create that transparency for consumers with privacy, a national privacy law, while also creating a better ecosystem where we proof people to enable them for online transactions.

Mr. LOUDERMILK. Thank you. I agree with Ranking Member McHenry; I also have tons of questions. This is intriguing. But I am already out of time. I will submit the others for the record.

I agree with Ms. Washington on her concerns, but I think the solution, because those with low income are using electronic transactions as much or more as some others are, and we have to be able to find the way to positively protect them as well.

Thank you, Mr. Chairman.

Chairman FOSTER. Thank you.

The gentleman from Ohio, Mr. Gonzalez, is recognized for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman.

And thank you to the panel for your outstanding testimonies and participation today. I think this has been a great hearing so far.

Mr. Boysen, I want to kind of drill down on some of Mr. McHenry's questions around blockchain specifically. So, I will spend some time there, if you don't mind.

As you were innovating in the space, what legal impediments existed in Canada that prevented you from developing the blockchain, and what has had to change? Just kind of walk me through what it was like as you were innovating, and then how did you get there?

Mr. BOYSEN. Sure. One of the biggest challenges, in fact, is when you look all across the economy, the most rigorous process we go through as consumers when we get identity proofed is when we go through a bank, and it is a regulated process. They have know-your-customer (KYC) and anti-money-laundering (AML).

In Canada, our organization for managing that is called FINTRAC, and they have a set of interpretation bulletins that they use to interpret the legislation to say what banks can and cannot do.

The problem when we started this process is it didn't include digital methods, so it took a long time to talk about the advantages of doing digital methods.

And I want to pick up on Valerie's comments around this card-present/card-not-present concept. One of the things we were able to convince the regulators is what we were doing with our service is actually creating card-present identity. Today, when I take my driver's license to the counter, if it is a fake driver's license, the bank is defenseless against that attack because they can't check against the issuer. With our service, all of the data is checked in real time.

So that, getting the regulators and the community to understand this was actually better than what we could do in person, took a long time, but once we got there, they said this was more powerful.

Mr. GONZALEZ OF OHIO. And was that a regulatory fix or a legislative fix?

Mr. BOYSEN. The interpretation bulletins for the FINTRAC and KYC and AML were updated to include digital methods.

Mr. GONZALEZ OF OHIO. Legislatively?

Mr. BOYSEN. Yes.

Mr. GONZALEZ OF OHIO. Okay. So, your legislature had to act.

And then as you look at the U.S., where do you see similar holes where we should be legislating to enable the technology?

Mr. BOYSEN. Canada had an advantage in trying to get a scheme like this going because we have a small set of banks, we have a small set of provinces, and a small set of telcos. So we could kind of get everything in the room.

Your economic construction here is a little bit different. You have 3,000 banks. You have 50 States. Luckily, you have a small set of telcos.

I do think the learnings in Canada can be applied to the U.S. model. So I will say that there is a lot of work being done with U.S.

organizations to launch a similar service to the one we have in Canada, here in the United States. That is down the track. More work needs to be done. But I think there will be similar changes where the regulatory updates are going to be required to support it.

Mr. GONZALEZ OF OHIO. Okay. And do you have any specifics in mind on, hey, here is how the SEC is interpreting this, and this needs to change?

Or anybody else, frankly?

Mr. Grant, you are kind of nodding.

Mr. BOYSEN. Yes. I can provide it as follow-up testimony for the record. I could get our legal counsel, who has actually done a lot of work here, and I will submit that for the record and you can review that after.

Mr. GONZALEZ OF OHIO. That would be fantastic.

Mr. Grant?

Mr. GRANT. I would say, if you look at our membership, about half of them are firms in banks or payments or FinTech. And one of the things we specifically called for was for was for Treasury and the regulators to do more here.

I will say they have been really receptive to discussions with us. The message we have gotten is, if you are seeing a barrier to digital identity innovation, please let us know. Marshall Billingslea, whom I think is Assistant Secretary for Terrorist Financing at Treasury, announced that Treasury wants to do a text print, working with industry in the next year to try and help bring regulators and innovators together.

I continue to ask my members every month, are we running into things that are precluding innovation, particularly at the intersection of identity and financial services? And I think the biggest answer we get is, sometimes there is a regulation where there is just ambiguity. And then, the compliance people kind of have their freak-out and it is hard to move forward. But I am actually bullish there.

I think where we need a little more effort—we talked before about the Office of Management and Budget (OMB) memo, which is a nice start, but policy memos come out all the time from OMB and get ignored. So I think we need more of a formal government-wide initiative, hopefully convened by the White House, to try and look at how to bring agencies together, potentially within the industry, to figure out how to take this to the next step.

I think more work needs to be done at my old agency, at NIST, on a framework of standards to help put a foundation in place. And I think agencies could benefit from a center of excellence in government as well, that could actually help.

The Social Security Administration right now is developing an attribute validation service. Congress told them to do so last year, in fact, thanks in part to the work of this committee. But in getting other agencies to do that, they will need some technical help.

These are little steps around the edges that can make a big difference to solving this problem.

Mr. GONZALEZ OF OHIO. Thank you.

And, again, I want to thank everybody for the time and energy on this.

Mr. Boysen, we will follow up.

And I yield back.

Chairman FOSTER. Thank you.

The gentleman from Virginia, Mr. Riggleman, is recognized for 5 minutes.

Mr. RIGGLEMAN. Thank you, Mr. Chairman. I hope I can have 60 minutes to question the panel, please. Thank you.

It is good to be here.

And, Ms. Washington, thanks for your—at the beginning when you talked about birthdays, my birthday is March 17th, a show of hands for St. Patrick's Day birthdays? Well, look at that. No one. My goodness.

I want to give my background really quickly because I actually get excited about this stuff. My background was in military intelligence, about 26 years combined in the military and doing this, was tracking people and finding their identities without them volunteering their information. So I might cover this a little bit differently. But it is also sort of the bridge between technology and operations and how this would happen. So my questions might be a little more esoteric and a little bit more fun, I would hope.

Right now, I have about 50 questions I had written down, so I am going to try to go quickly. I always have too many to go quickly. But Ms. Abend had said something beforehand, and I will start the line of questioning there.

I am going to start with sort of the bottom line upfront, and then go backwards with technology. And, here we go.

It does sound like the use of AI will be a critical part of ensuring security in digital identity. I want to know, should we be concerned that this kind of technology could be cost-prohibitive—and I am starting at the back—or otherwise unavailable to smaller financial institutions or even companies? Do you think that is something we have to worry about?

Ms. ABEND. I think that any time you deal with innovation, it is actually interesting, some of the smaller companies of the world are really creative, and they partner with Accenture to actually make those possible and to make them scale. But I do think we need to find ways to actually help smaller companies be able to leverage some of these capabilities that you are pointing out, AI being one of them.

And to that end, I would commend the ranking member's effort in his own district, in Little Rock, Arkansas, to actually create an innovation hub where community institutions can actually learn how to take advantage of these things.

And I think the other way to actually help them scale to the benefit particularly of smaller entities and in this case community institutions is to actually help them do that through the partnerships with their third parties, their large-scale technology service providers.

Mr. RIGGLEMAN. This is why I get excited about this, because we all are sort of creating our own unique identifiers, our own "UIDs." But a refrigerator has one also, and I don't want to be mistaken for that.

So as we go forward, do you see private companies—and here my questions get a little esoteric—rejecting individual or business

transactions with other entities based on insufficient authentication of identity?

And when I look at how people are going back and forth and utilizing sort of their own signatures, my question is, are we going to get to a point—and this is where I get a little bit excited and my head starts to explode a little bit—where we are going to see private companies actually creating their own unique ID sort of set of criteria? And then, do you see them ensuring that criteria or ensuring that identity is doing transactional issues with other companies and then rejecting those companies?

That is the thing that—and I know Mr. Grant, and I listened to what you are doing in Canada—I am almost wondering if we are going to get to a point where companies are going to be judged based on their criteria for how they protect our identity and other companies rejecting that identity based on UIDs. Do you guys see that happening in the future?

Mr. Grant, go ahead?

Mr. GRANT. For years, one of the things we have been trying to do here in the U.S. and really in a lot of countries abroad has been looking at whether we could have certification programs for private issuers of identity.

I talked today about the role of government, but my bank knows me. In fact, that is sort of the foundation of what is happening in Canada, as well as what I think we will see in the U.S., because they have to figure out who I am before they open an account. So could they then vouch for me other places? Could I log in with my bank somewhere, perhaps at the Social Security Administration?

There are certification programs in place today from organizations. The one that is most well-known is called Kantara. That has actually been recognized by the General Services Administration as what they call a trust framework provider to certify the way that a private sector entity issues an identity.

Going forward, I talked about a lot about the concept of an identity ecosystem. There are components that industry is going to provide, and there are components that the government is going to provide. And I think we are going to be able to create some hybrid solutions that can really bring in, frankly, the best innovation the private sector can deliver, but that access to the authoritative data sources that only government has. Government is the only entity that authoritatively confers identity. If you can merge those together, you can give people something that is portable that they can use everyplace they go.

Mr. RIGGLEMAN. Well, geez, you are in my head.

So do you believe, if we are creating, say, this identity token, and you are talking about these standards, do you think we are dealing with unstructured data? We are dealing with new things like natural language processing, things like that. Do you believe there is ever a time where we are going to be able to customize our token where the only way we can find our identity or make our identity known is the stuff that we actually customize with that information? Do you think that is the future, where we own our identity by customizing our own information within the token?

Mr. GRANT. There is a lot of focus these days on how you can allow people to only reveal certain things about themselves without

revealing everything, and I think there are some great models that are in place these days that will give people very granular choices about what they share about themselves online.

When we talk about the privacy debate in this country—and it is getting a lot of attention on the Hill—so much of it is tied to identity. What information is collected on me? What do I want to be collected? Why do I want these companies to know these four things but not these seven things?

So, having a really strong tool that you can use to manage that and in some cases go back and maybe revoke certain things, I think is going to be a key enabler here.

Mr. RIGGLEMAN. Thank you so much. It was already 5 minutes and 30 seconds. So, I do apologize for how quick that was. But thank you so much. You guys are fantastic. I appreciate it.

Chairman FOSTER. Thank you.

And without objection, the ranking member and I will each have an additional 5 minutes for questions and closing statements.

So with that, I would like to recognize Mr. Hill.

Mr. HILL. Thank you again, Dr. Foster, for holding this hearing. And, again, I think we have heard a good discussion and the panel has been very appreciated.

I wanted to go back, Mr. Grant, and just kind of finish our conversation about the California proposed statute. And I may broaden that to the panel as well to compare, as you said, a rushed law, a set of parameters with the more thoughtful approach the EU took and just have a compare and contrast.

The Wall Street Journal last week reported that private businesses could face a half a billion dollar compliance burden trying to comply with the California law. So, talk about that.

And then finish your thought I think you were trying to make on it was rushed, you have some concerns, you outlined a couple. But did you have something else you wanted to finish up on, on that?

Mr. GRANT. The main point I was making, from what I could tell with California, it might be a drafting error. And there have actually been some proposals to try and clarify that.

Mr. HILL. This is the information to be used for fraud investigation, better customer service?,

Mr. GRANT. Right. The backdrop on this is that identity analytic solutions, many of them that are using AI, are one of the most powerful tools that we have today to actually prevent fraud.

So just to give you a number on that, Microsoft started talking about this publicly. So in Azure they manage billions of log-ins a day.

Two years ago, they were seeing about 10 million attacks a day. A year ago they were seeing 100 million attacks a day. This year, they are seeing 300 million attacks a day, trying to compromise log-in systems to get in and do all sorts of bad things. That is a 30 times increase in 2 years.

The way that they are actually combating this is with database analytic systems, some of which might be collecting things that would fall under the definition of personal data under GDPR or CCPA or other proposals.

So long as you have a carve-out that says that is okay if you are worried about security and fraud protection, you just can't take that data and use it someplace else, we are good. In fact, in Europe, because GDPR is clear on this, the European Banking Authority is actually actively promoting the use of what they call transaction risk analysis to secure payments under the PSD 2 directive over there for open banking.

So I think the concern here is if it is more ambiguous, or certainly if we are concerned that Federal privacy legislation that doesn't say it as clearly, if 2 percent of people start calling up Microsoft, to give the example I suggested, and say, don't use those systems, turn that off, what are they supposed to do at a time when attacks might go up another 10 times next year? That is my concern.

Mr. HILL. Very helpful. And you mentioned open banking in the U.K. for example, and Canada as well. So I might ask Mr. Boysen this.

First of all, does anybody else want to add to that comment on California? Anybody have a comment on California?

Okay. Mr. Boysen, on the privacy directives in Europe and what you have done in Canada, have Europe and the U.K., to your knowledge, solved this password authentication process in order to make open banking be a safe activity? Because clearly here that would be an open question I would think about open banking.

Mr. BOYSEN. Yes, open banking is a singular term, but the way it manifests in each country turns out to be a little different. In some countries, it is compulsory. In other countries, it is optional. In some places, it includes the ability to do push payments. In others, it doesn't. So, it is not a uniform application of how it works.

What I will say, however, is one of the fears of open banking is it is going to cause asset stripping. What is going to happen is the banks are forced to open up their APIs and give out the data at no cost, and then the consumer is going to give this to some new startup who doesn't have the same control as the bank does. That FinTech is going to get breached. And then, the consumer is going to come back to the bank and say, "How did you let this happen?"

So rather than giving away the data, what we should give away is trusted data so consumers can give it away at a granular level, rather than giving it all. So that is kind of the approach that we are looking at in Canada.

It's interesting that in Australia, they took the approach that it is reciprocal. If you are going to participate in open banking, if you want to be able to get data from the network, you also have to agree in advance to share data back with the network. And that solves part of the asset stripping issue that is in some other jurisdictions.

Mr. HILL. I think I am interested in what we need to do regulatorily, again, limiting our conversation here to financial services, about how we handle this requirement of an API approach and a discrete approach, instead of just allowing scraping.

I hear from start-up entrepreneurs in the FinTech environment: "Well, you are disturbing the customer experience by doing that." But I would argue that customers' experiences get really messed up

when everything is stolen from them. So, that is not a good idea, either.

Is there something specific one of our regulatory agencies could do in this area?

Mr. BOYSEN. I would submit that you can't do open banking without a good digital identity infrastructure; it just can't be done.

This is the problem. I am the consumer, you are the bank that is trying to represent me, and Jeremy is the startup that wants my data. How is Jeremy supposed to present to you that he has my permission to get my data?

So, you have this three-way triangle of authentication trying to go on and it is very complex and the consumer is never going to get it.

The only way to solve this is by allowing the consumer to have a digital identity infrastructure, and then see line by line, what is going to go.

Mr. HILL. Thank you very much.

And I yield to you, Mr. Chairman. Thank you.

Chairman FOSTER. Thank you.

That business of this three-way conversation is fascinating, for which I think there are technological solutions with a properly designed app on your cell phone. So I think that probably the future of this is not an identity dongle but probably an advanced cell phone that has things like the secure enclave on an iPhone which can store the private keys and is resistant, it is my impression, even against having your cell phone completely hacked, that you may be able to capture the screen and see passwords being transmitted but you cannot actually steal from the secure enclave in these, the private key, which is a tremendous advantage of that approach, and that you can still have this three-way conversation under the control of a properly designed app. So, I think there has been, I believe, great progress there.

Now, as it relates to the use of blockchain, one of the great advantages of blockchain is it provides a non-falsifiable ledger. Is there a solution in that context to developing, say, a witness protection program which is essentially government-sponsored synthetic identity fraud? Is that something that people have thought about and come up with solutions to?

Mr. BOYSEN. I don't have a great answer here. I will say one of the challenges that what we are getting with these longitudinal records is that you can't go back in time and insert a person for the purposes of witness protection. It is very difficult to do. So, you are going to have find some other method to bring that identity along.

Chairman FOSTER. If it is a publicly visible blockchain—

Mr. BOYSEN. Ours is not. Ours is a private blockchain. So, there is that protection. But still, going back and altering the records in the past is hard.

What the government could do perhaps is have a set of identities on standby to use for the future so they have the longevity that would be required to pass the muster, but that has its own pitfalls.

Chairman FOSTER. That is tough because this has to pass all sorts of secondary verifications but it is really—anyway, you should

put that on your to-do list when we come up with the perfect example here.

Now, it also seems to me that to come up with the ultimate solution here, there has to be a role of government, almost certainly government. At some point in your life you have to go and authenticate yourself and be uniquely identified using biometrics. At that point you can then be issued a security dongle or the cell phone equivalent of one that you can use for many, many purposes in very streamlined and low-friction transactions.

Is there any logical alternative other than having every citizen who wants this to be able to authenticate themselves security, knowing that there is not synthetic identity fraud or other people using their credentials and the alternative to having them present themselves in front of a trusted government authority?

Mr. BOYSEN. I would say we need to learn from payment systems when we try to do identity. David Birch has this famous phrase that identity is the new money, and comparing identity to money, there are a lot of things we can learn.

When you look at the global payment system with EMV cards, we have six billion cards in circulation and they have never been compromised. What is good about this model is you can have your favorite bank and I can have my favorite bank and we can go to any merchant on the planet with no prior relationship and get what we want.

More importantly, when we lose the card, we call the bank right away because we are terrified we are going to be responsible for the results if we don't. So, that integrity is what makes the process works.

In payment systems, these three things make the global payment system work. The first thing is we made it super simple for the consumer and we hid the complexity away so they don't have to understand anything. We don't have to train users how to use credit cards.

Thing number two is we have a trusted network operator. Crooks can't pop up in the middle and say, "Hey, I am a crook. I take Visa." Right? You have to apply to get in the network, and you have to behave well to stay in the network.

The third most important thing that keeps the global payment system safe is user behavior. When I look at my wallet and see my card is gone, I am going to be on DEFCON 5, I am going to run down to the bank to turn the thing off, because I am terrified I am going to be responsible.

Chairman FOSTER. Yes. I think Ms. Walraven would feel—well, I don't want to put words in your mouth. But this system is not perfect that he just described. Synthetic identity fraud can still permeate such a system.

Ms. WALRAVEN. Agreed, I think, but I think that is when it comes down to understanding, knowing your real customer, because we do have controls in place that are supposed to do that, and we all assume that banks know who their customers are, and I know, coming from the banking industry, that everybody is trying to do that.

But considering the fact that synthetics are as prolific as they are, considering that they are as widespread as they are, consid-

ering that they are growing in a force multiplier, I would contend that they don't actually know their customer.

So I feel like if you have an issue that is not right at the root and then you compound on top of that, you actually just make the issue later worse because you get this false sense of trust, you get this false sense of security, and it doesn't allow you to actually really be able to contend with those types of individuals.

And that actually bodes to exactly what they are looking for. They want to be seen as a regular, traditional customer. They don't want to send that many red flags because they don't want to get caught. They want to be able to continue to navigate through the system, and currently they are navigating pretty well unfettered for the most part.

Chairman FOSTER. But if you think of the example that Mr. Loudermilk gave of the identical twins with identical names, they differ only in their fingerprints. So at some point in their lives, it seems like they have to present themselves to some organization, almost certainly a government, who has to go and look and de-dupe all the people who claim to have that name.

I think there is no alternative to very advanced biometrics of some kind. And this can be an optional system, but if you are going to provide citizens who want one with a secure means of authenticating themselves, you have to have this moment in their lives.

Mr. Grant, do you have any comments on that?

Mr. GRANT. Yes. I would say biometrics can play a role. I worry about saying they are the solution. In part, I tend to get very nervous when we talk about creating new central databases and biometrics, in part, because if there is one thing we have learned, it is that like any other type of valuable data, we are not really good at protecting them.

And Exhibit A for that was the OPM breach of 2015, where I have a top secret clearance, and all of that information from my SF–86 and the images of my fingerprints are now in China—and I think at least two-thirds of this room probably has the same thing, understanding who is here today—which means that I would never want to use a centrally matched fingerprint system online where they didn't know I was there to protect anything of value because a nation-state can spoof a fingerprint based off those images.

That said, there are some really helpful tools. Most DMVs are using face recognition for de-duping. So if I were to go in as Jeremy Grant to the DMV, and then show up 3 months later under a different name, they are able to say, "Oh, it looks like you were here before, let's at least"—and, mind you, the face recognition is not perfect, but they can toss that to a fraud investigator to figure out if they should issue a second credential.

Leveraging that process, I think is really important. One of the things we point out in our policy blueprint is that the driver's license is the one thing that most Americans get in their lifetime where they have a robust in-person identity-proofing process. That is really valuable, and we think people should be able to reuse it. The DMVs will play a role.

But I will flag that only 87 percent of adults have a driver's license. And in fact, one thing we are seeing these days is that it is harder to get one thanks to things like the REAL ID Act from

2005 which, on one hand, look, there were good security reasons for it and it has put a very robust Federal standard in place for in-person identity proofing.

The flip side is, if you are on the margins of society, let's say you have been in and out of homelessness, let's say you were evicted and your license and your birth certificate and your Social Security card were left in a box by the side of the road that was soaked in rain and lost, it is really hard for people to restart their identity lives again because they are just lacking what they used to have, to the point that we are seeing in many places—in fact, in D.C., there are a couple of churches, like the ID Ministry at the Foundry United Methodist Church up the street, that work with people.

Chairman FOSTER. I am afraid I am going to have to gavel myself; my time is up. Votes have been called.

Without objection, I would like the report from the Better Identity Coalition to be included in the record.

Without objection, it is so ordered.

And I just want to thank the witnesses for their testimony. This is, I think, at the root of so many problems that we have, that we are going to be facing.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

Thank you again. The hearing is now adjourned.

[Whereupon, at 10:56 a.m., the hearing was adjourned.]

A P P E N D I X

September 12, 2019

**"The Future of Identity in Financial Services:
Threats, Challenges, and Opportunities"**

Testimony of

**Valerie Abend
Managing Director
Accenture**

Before the

**Task Force on Artificial Intelligence
Committee on Financial Services
U.S. House of Representatives**

September 12, 2019

Chairman Foster, Ranking Member Hill, and members of the Task Force, my name is Valerie Abend and I am a Managing Director with Accenture, where I lead the North America Financial Services Security practice, and serve as the Global Cyber Policy & Regulatory Lead. On behalf of all my colleagues at Accenture, a leading global professional services and technology company, serving 95 of the Fortune 100 and 75 percent of the Fortune 500, thank you for the opportunity to appear before the Task Force to discuss cyber threats and how innovations in digital identity and access management are improving financial institutions' and customers' ability to mitigate cyber attacks, enhance privacy, and ensure trust in financial transactions, and what more needs to be done. My comments today will cover three areas:

1. The increasing volume and sophistication of cyber threats that specifically focus on credential theft and exploit privileged access;
2. The significant advances in digital identity systems to combat fraud and provide true needs-based access, while also enhancing customer experience and privacy; and
3. How artificial intelligence is being used to manage cyber risk both for internal access within financial institutions and for customers.

Credential Theft and Privileged Access

First, let me address the increased volume of cyber threats, particularly credential theft and the growing trend of bad actors exploiting privileged access. In our recently published paper entitled, "Future Cyber Threats: Extreme but Plausible Threat Scenarios in Financial Services,"[1]

[1] https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf#zoom=50

which I have provided to the Task Force for inclusion in the hearing record, we explore how current cyber threats will be increasingly directed across multiple institutions and third parties simultaneously, potentially causing extreme impacts. The five key themes in the paper are: 1) credential and identity theft, 2) data theft and manipulation, 3) destructive and disruptive malware, 4) emerging technologies, and 5) disinformation. While my remarks before the Task Force today focus largely on credential and identity theft, the paper describes how all five threat themes may come together in the future to impact financial services. Credential theft was our first theme because this is how most attackers initiate a financial institution breach.

Phishing and spear phishing have been problems for more than a decade because it works. Malicious cyber actors can cheaply target large volumes of people and entice users to click on links or open attachments that imbed malicious software that enables the attacker to scrape a user's log in information. For attackers, it also helps that people put vast amounts of information about themselves online, making it even easier for bad guys to identify specific targets and construct a social engineering campaign to steal a particular individual's login credentials.

Securing credentials is a key challenge for both retail and wholesale financial services.

Today, sophisticated attackers don't just go after one bank, they go after the end to end process, which includes the customers, deposit institutions, clearing banks and central banks. They identify vulnerabilities in the processes, leverage countries with weak money laundering enforcement, and target specific employees and third-party employees' credentials. We call these multi-party attacks and they are becoming more common.

One well-known example of this is the 2016 cyber heist from the Bangladesh Central Bank, where attackers successfully stole more than $81 million. The attack started in 2015, when

attackers set up seemingly legitimate bank accounts, using fraudulent identities at several institutions. They then targeted the specific identities of employees at the Central Bank who were part of the wholesale payment transactions value chain. The attackers knew the systems they had to effect and the credentials they needed to control to carry out the attack unnoticed and transfer stolen funds to accounts they set up with fake identities. This was four years ago, and adversaries are continuously learning.

Advances in Digital Identity

Fortunately, while the bad guys have gotten smarter, the good guys have too. Financial institutions are making investments to thwart these types of attacks and manage risks more effectively. These include people, process and technology. Cyber threat intelligence teams both internally within institutions, along with external providers, are helping companies build more effective defenses. Advanced security operations centers are enabling companies to identify attacks sooner and take mitigation measures more quickly. Robust awareness and training initiatives are helping employees better understand social engineering attacks and know what to look out for. Information sharing about threats and vulnerabilities is also more robust than ever before through the Financial Services Information Sharing and Analysis Center (FS-ISAC). And to the topic of today's hearing, the financial services industry is an early adopter of digital identity innovations. These innovations provide better risk engines to make it harder for fraudsters to gain access to customer accounts while enhancing customer experiences.

Consumers expect seamless and easy to navigate online services, and institutions are working to meet that demand by growing their online products and services. Online and mobile banking are

now table stakes in a digital economy. To stand these operations up quickly and efficiently, commercial entities initially rolled out platforms that relied heavily on customers setting passwords and answering security questions to authenticate their identities online. Unfortunately, today a large percentage of Americans' names, addresses, birthdays, social security numbers, and other information, used by fraudsters and state-based cyber actors to guess passwords and answers to personal questions, is available on the dark web. The days of the username, password, and security questions as tools to manage risk are numbered.

This is where the concept of customer digital identity comes in.

Increasingly, financial institutions are implementing an array of products and services - such as biometrics, behavioral analytics, and multi-factor authentication - to help them make real-time, risk-based decisions about whether to authenticate a customer, approve a transaction, and what limits to set around a transaction.

Because of these new tools and techniques, individuals can be digitally authenticated anywhere in the world, in real-time. For example, I was recently traveling overseas and could log into my banking app on my mobile device using my thumbprint. The bank would have used the identifier from the phone, my location information, and many other factors to determine if I was actually Valerie Abend. If, at the time, the bank noticed anomalous activity in my account, its algorithms would have decided whether and what additional information it needed from me to provide me access to my account. Of course, as with any new process and technology in this highly-interconnected digital age, there could be other implications, and in this case, depending on the types of information that is gathered or that I share with the institution, there could be privacy implications for an effective risk management approach. Ultimately, the digital identity ecosystem I've outlined above will not just be limited to financial services but will also spread to

other parts of the economy. That is why Accenture believes Congress must pass a national privacy law that provides consumers with rights for transparency, control, access, correction and deletion with respect to their data. A robust and secure digital identity ecosystem depends on privacy to build trust and will not thrive without it.

The Role of Emerging Technologies in Managing Risk

One of the most ubiquitous new technologies being discussed today is artificial intelligence (AI). Not a day goes by without some mention of the promise of AI in all sorts of business settings, and cybersecurity is no different. The unfortunate reality is that bad guys will use AI as part of cyber attacks. While that can be scary, it should also give us some comfort to know that agile and forward leaning organizations will also leverage AI to defend themselves. AI will enable automated detection, response, and mitigation in security operations centers, intercepting attacks faster than humans can today, and stopping suspicious events before they become actual, harmful incidents.

AI is also increasingly being used to help ensure needs-based access management internally to financial institutions. Within many financial institutions there is a significant amount of attention and resources paid to identity and access management. Identity access and management includes policies, technologies, and processes that are meant to ensure that customers, employees, and even contractors only have access to systems and information necessary to perform their transactions or do their job.

Most institutions use a principle called role-based access control (RBAC) to manage their identity and access management. For example, when an employee starts her job at an

institution, she needs access to certain systems. We call this day-1 access—things like email, human resource systems to select and receive health benefits, and payroll systems so she can get paid. All of that day-1 access is put into something called a role. In addition, the new employee likely is joining a particular group within that institution and that means she probably needs access to certain applications and datasets to do her job. That's another role. She likely needs access to more than just one role because her job requires her to work with information across different groups at the institution. Let's say she does a great job and gets promoted. She even gets transferred to a new group and gets additional roles. Over time, she accumulates a lot of roles with the access that goes well beyond what she needs to do her job at any one time. Some of these access rights might include privileged access to sensitive data or systems including the ability to not just see information and systems but to copy them or make changes. Let's take a step back now and multiply this one woman's access across thousands of people and thousands of systems inside a single institution and you have a very complex risk management challenge. Today this process is manual, inefficient, and hard to maintain in alignment with current risk management principles.

This is why institutions are starting to use AI to have a more accurate, real-time understanding of access enables supervisors to make better access management decisions. This is really important. Most breaches involve some type of gap in the identity access and management process—either from the customer or employee or both. Innovative approaches, such as AI, can deal with complex and highly vulnerable processes and will increasingly be essential to thwarting cyber attacks.

From a customer perspective, we are helping to spearhead important innovations using emerging technologies such as blockchain, biometrics, and encryption, to enable large numbers of

customers to verifiably identify themselves with an audit trail to their bank, while still being in control of their own identities in a virtual world. The best example is the ID2020 project. As a Founding Alliance Partner of the public/private alliance called ID2020, Accenture built the decentralized ID prototype and launched it in June 2017. This blockchain identification system was designed to provide reliable digital identity to refugees so they can confidently receive government services, and validate their identity to employers, schools, and other service providers. Additionally, it gives users control over who has access to their information and for what period of time. As innovations like this progress, it is likely they will leverage AI to further enhance both risk management scoring of customer identities and their customer experience.

Imagine a world where we broadly apply these kinds of techniques across financial services. Americans will have the opportunity to exert real control over their data. They would share what they want, when they want, with whom they want. Instead of filling out long application forms, repeating the same information over and over—users can populate those forms with a simple click of the mouse or touch of the thumb, saving millions of hours of time while simultaneously and dramatically increasing security and privacy. Of course, as I noted earlier, new processes and technologies also introduce new challenges. In the case of AI, there are four key areas where we need to manage risk:

1. The security and quality of the data informing the algorithms.

2. The security of the algorithms.

3. The quality and accuracy of the outputs—looking for disparate impact, bias, and malicious compromise or manipulation of data.

4. Effective and responsible AI governance approaches.

Looking forward

There is a lot of work to be done to make these emerging technologies work in favor of customers. From where I and others sit, based on the industry's long history of being heavily regulated and the importance of safety and soundness of the industry, financial institutions are best positioned to leverage these new technologies as early adopters while managing the risks to enhance the financial lives of Americans. The World Economic Forum's January 2018 report, *On the Threshold of a Digital Identity Revolution,* noted that people and legal entities in many countries already leverage documents from financial institutions as a form of identity to gain access to other services. This positions the sector as a prime candidate to act as a trusted identity provider.[2] Proofs of concepts should be encouraged, and their ability to scale should be assessed. Interoperability is essential, as any new tools or techniques should work with not just one company's systems, but also with those in other industries. And financial services should lead the way in moving away from the Social Security number as a key authenticator. The role of the Social Security number has moved well beyond its original intent, giving it unintended power and value that ultimately has made it possible for bad guys to commit a myriad of fraudulent activities. The time has come to find a way to diversify off the Social Security number so that it is no longer a proof of who you are in an online environment.

Broadening and scaling the use of digital identity across the economy will require new levels of cooperation and collaboration between the private and public sectors. This was a key conclusion reached in a white paper, *Building Trusted and Resilient Digital Identity,* recently released by Business Roundtable, a trade association consisting of more than 200 CEOs of leading U.S.

---

[2] World Economic Forum, *Digital Identity On the Threshold of a Digital Identity Revolution*, January 2018 http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf

companies. The paper, developed under the leadership of Accenture CEO Julie Sweet, made eight recommendations to advance private and public development and use of digital identity, including:

- Reducing our dependency on passwords in favor of more intuitive and secure authentication;
- Increasing customer awareness, digital literacy, and confidence;
- Improving multiple sector participation in a digital identity ecosystem that enables trust in each other's attestations of identity—so users can continue to transact business even when an individual organization's digital identity system has been breached; and
- Ensuring transparency and choice to customers, empowering them with customer rights. A national privacy law would go a long way to achieving this goal.[3]

What does all of this mean for Congress? As this Task Force and Congress as a whole, considers legislation and other avenues in the areas of digital identity and cybersecurity in the financial services sector, I would encourage three things specifically:

- Ensure legislation is truly technology neutral and does not effectively choose winners and losers in the marketplace;
- Pursue policies that will protect and advance innovation, which is essential for our financial institutions to stay a step ahead of the bad guys; and
- Pass a national privacy law, which as I noted earlier, is essential to effective, robust digital identity ecosystem.

[3] Business Roundtable, *Building Trusted and Resilient Digital Identity* July 2019 https://s3.amazonaws.com/brt.org/BRT-DigitalIDReportJuly2019.pdf

Conclusion

In sum, the financial services industry is facing significant changes on the cybersecurity front. Credential theft and abusing privileged access has long been a successful approach for cyber attackers, but their tactics are getting more sophisticated. Fortunately, the industry has made significant advances in digital identity systems to improve user experience, combat fraud, and to limit access to only those who truly need it, which gets at the heart of what our adversaries have used so successfully. And emerging technologies like AI are increasingly needed and becoming part of financial institutions' cyber resilience strategies.

Customers trust financial institutions with vast amounts of their data they are highly regulated. These regulations include cybersecurity supervision, and identity and access management. As such, financial institutions will play an important role as part of the foundation of the digital identity ecosystem today and will help shape its growth in the future. For the sake of the safety and soundness of the financial system, we must create a policy environment that encourages innovation and scaling of digital identity solutions to mitigate cyber attacks, enhance privacy, and help to ensure trust in financial transactions.

Again, I would like to thank the Task Force for the opportunity to discuss these issues today and I look forward to your questions.

Andre Boysen
Chief Identity Officer, SecureKey Technologies

U.S. House Financial Services Committee
Task Force on Artificial Intelligence

"The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"

September 12, 2019

Chairman Foster, Ranking Member Hill and members of the Financial Services Committee and Task Force on Artificial Intelligence, thank you for the opportunity to discuss the future of digital identity in financial services with you today.

I am Andre Boysen, Chief Identity Officer at SecureKey Technologies. I look forward to sharing our experiences in building a privacy-based digital identity verification network for Canadian consumers, in the hopes that my testimony will help inform this committee and task force as to what possibilities robust digital identity schemes can offer to citizens, governments and the services with which they choose to interact.

SecureKey is a Canadian company that is a world leader in providing technology solutions that enable citizens to efficiently access high-value digital services, while guaranteeing the security and privacy of their personal information. We do this by building highly secure networks that span and merge the strengths of the public and private sectors.

SecureKey's expertise lies in building tools that realize the possibilities of digital identity in the modern digital economy. To build identity verification tools, we focus on the intersection of the citizen, public and private sectors, privacy and consent, rather than leveraging AI and big data.

As we know, the digital age has ushered in a host of new services, business models and opportunities to participate in the world. Not long ago, it would be unimaginable to order a shared ride from a device in your pocket, or to access sensitive government services from your home. Today, we take these things for granted and often get irritated when we come across a task that can't be done online.

It's not just about citizen expectations. Companies, governments and other organizations have strong incentives to move services and transactions online to realize cost savings, enhance

client experiences and increase business surety. An organization's ability to do this hinges on a single question: "Can I trust the person, or digital identity, at the other end of the transaction?"

This digital identity challenge is equally problematic on both sides.

To recognize clients and provide trusted access to services online, organizations typically deploy a mix of analogue and digital measures to confirm identity and mitigate risk. As we have seen, however, these solutions tend to be complex and not fully effective. As such, confidence in them has suffered.

On the other side, citizens are asked to navigate a myriad of identification methods and challenges to satisfy the identity proofing requirements of the organizations they seek services from, without knowing where the information is going, and in the face of a steady stream of news about data breaches and online impersonators.

These concerns are well-founded.

Fraudsters are collecting information to know as much, and sometimes more, about the citizens they are impersonating. Standard physical cards are easily counterfeited, and it is often impossible to check their validity with the issuing sources. Even biometric methods, which have often been touted as the solution to digital fraud, are increasingly being targeted by hackers, elevating the risk that biometric data may be compromised.

These factors are driving complexity up, trust in the system down, and adversely affecting privacy; exactly the opposite of what needs to happen.

Our siloed system is too hard for consumers to use and too expensive to be sustained.

Consider the reality of Twitter and Facebook's chief executive officers, Jack Dorsey and Mark Zuckerberg. These two individuals know how the system works, understand digital identity best practices and have all the resources in the world at their fingertips. Yet, even *they* have problems controlling and managing fraudulent access to their own digital identities. If they cannot manage in the current digital identity landscape, how can an everyday citizen be expected to navigate the pitfalls?

The problem we face is not simply a matter of finding the best technology, the right skills, or enough money to fix it; rather, everyone with a stake in the system needs to focus on solving the digital identity problem that underpins all digital services, bringing data and identity information back under the control of the citizen.

To solve the digital identity challenge, we must find ways to combine the prime factors of identity. These are the unique things we know, like shared secrets; the unique things we have, like existing trusted relationships, mobile devices or government-issued identification; and, the unique things we are, like our fingerprints or facial scans.

By combining these factors, we can resolve identity and give organizations confidence that their clients are who they say they are. All experience to date proves that single methods are not up to the task. This means that trusted networks and models are needed. All participants must be involved in the solution, including, and perhaps especially, citizens, whose control over their own data and privacy, will underpin its security.

Only by combining the best aspects of each system can we solve the digital identity problem and rebuild the trust that is equally required by both organization and citizen. The Canadian model is a public-private-partnership between banks, telcos, governments and other trusted partners. Each participant has a unique contribution to make to the ecosystem, and they each also desire services from other participants in the network. It is give to get.

For example, governments are the initial issuers of individual identities, including birth registries, immigration documents, and permits and licences. Governments also can link their records to a living person, by issuing a driver's license or a passport. But governments are not as adept as the commercial sector at knowing if that person is actually at the end of a given digital transaction.

This brings us to financial institutions, who complete billions of authentications per year. Compared to other organizations, citizens only rarely interact with governments during their daily lives. They may renew a license or passport every five years but will log into their bank account several times a week, which gives a higher level of trust and immediacy to that interaction. Then think about mobile devices, which are always within reach, and which are both identifiable within a cellular network and are tied to subscriber accounts.

All parts have something valuable to offer within a successful network.

Imagine a scenario where a citizen can choose to share information securely within a network made up of organizations that they trust already. This citizen would need to access the network using their trusted online banking login and, because he or she is using a device that the telecommunications operator knows and can validate, reliable information – like their age of majority – can be shared to an online seller for a regulated sale, like alcohol, for example. The citizen has complete control over the interaction to share with knowledgeable consent.

In this scenario, the online seller does not need to know the actual issuer of the information, only that it comes from a trusted source. The seller doesn't need to know the citizen's actual birthday, only that the trusted source confirms that they are above the age of majority. Moreover, companies or organizations using the network would have no access or visibility to the data transiting the network. We call this Triple Blind Privacy®.

This scenario is not part of the distant future. All of the pieces are already in place to allow the providers of data to enable a system that has authoritative information, that provides receivers of information with confidence in the transaction, and for the citizen to fully trust the system as they control their own data in a privacy-enhanced way. This type of arrangement is the cutting edge and is happening now in Canada, with our Verified.Me digital identity verification network.

Verified.Me is a service offered by SecureKey Technologies Inc. The Verified.Me service was developed in cooperation with seven of Canada's major financial institutions – BMO, CIBC,

Desjardins, National Bank of Canada, RBC, Scotiabank and TD. It is a first-of-its-kind and blockchain-based network that takes an ecosystem approach to solve the problems associated with digital identity today. Working closely to develop the network with Canada's financial institutions was a natural foundation, as ours is a highly banked population and the number of financial institutions is far more concentrated.

With the information and resources already available, we had the opportunity to solve the digital identity problem and develop a replicable model for the world. These include cooperative jurisdictions, technologically advanced telecommunications, and world-leadership in developing new approaches, such as Global Privacy and Security by Design developed by Dr. Ann Cavoukian; the U.S. Department of Homeland Security Science and Technology Directorate; IBM Blockchain; the Linux Foundation's open source Hyperledger projects; and the Pan Canadian Trust Framework, championed by the Digital Identity and Authentication Council of Canada.

We had, and continue to have, the opportunity to build services that can provide identity validation claims from multiple parties in a single transaction, while ensuring complete privacy and control for the citizen. Key factors for any solution to be successful will be citizen acceptance, trust and the potential to reach a large user base quickly.

The responsibility to guarantee and protect privacy, and to provide a sense of security to citizens, are fundamental factors in the success of any solution. It is critical that any approach to solve the problem with digital identity connects together the trusted parts of the digital economy such as finance, telecommunications, government, and commerce. Only this will provide citizens with confidence they demand, to use the providers that they already trust and to have access to the information that they want to securely share.

The cyber risk around digital identity is high. Any solution that does not involve both the private and public sectors will be of limited success. It will perpetuate the siloed approach that is currently under strain and will not have the security or public trust to enable the digital economy of tomorrow.

Fortunately, there are options and many brilliant minds around the world who are dedicated to solving this problem on behalf on the everyday citizens everywhere. We have the privilege of being the custodians of citizens' digital futures. As such, we have the obligation to act responsibly and with the highest degree of collaboration, commitment to open standards and world-leading privacy and consent technologies. I am thankful for the opportunity to share my expertise in this public forum today, and I welcome your questions.

Thank you,

Andre Boysen
Chief Identity Officer
SecureKey Technologies Inc.

Jeremy Grant
Coordinator, The Better Identity Coalition

U.S. House Financial Services Committee
Task Force on Artificial Intelligence

"The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"
September 12, 2019

Chairman Foster, Ranking Member Hill and members of the committee, thank you for the opportunity to discuss the future of identity in financial services with you today.

I am here today on behalf of the Better Identity Coalition[1] – an organization launched last year focused on bringing together leading firms from different sectors to develop a set of consensus, cross-sector policy recommendations that promote the adoption of better solutions for identity verification and authentication. The Coalition's founding members include recognized leaders from diverse sectors of the economy, including financial services, health care, technology, FinTech, payments, and security.

As our name would suggest, the Better Identity Coalition is not seeking to push the interests of any one technology or industry. Instead, our members are united by a common recognition that the way we handle identity today in the U.S. is broken – and by a common desire to see both the public and private sectors each take steps to make identity systems work better. Last year we published "Better Identity in America: A Blueprint for Policymakers" – laying out five key

[1] More on the Better Identity Coalition can be found at https://www.betteridentity.org

initiatives that government should launch around identity that are both meaningful in impact and practical to implement.

As background, I've worked for more than 20 years at the intersection of identity and cybersecurity. Over the course of my career, I've been a Senate staffer, led a business unit at a technology company architecting and building digital identity systems, and done stints at two investment banks helping investors understand the identity market – cutting through what works and what doesn't, and where they should put capital. In 2011, I was selected to lead the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative focused on improving security, privacy, choice and innovation online through better approaches to digital identity. In that role I worked with industry and government to tackle major challenges in identity, built out what is now the Trusted Identities Group at the National Institute of Standards and Technology (NIST), and also served as NIST's Senior Executive Advisor for Identity Management. I left government in 2015 and now lead the Technology Business Strategy practice at Venable, a law firm with the country's leading privacy and cybersecurity practice. In that role at Venable I serve as the Coordinator of the Better Identity Coalition.

Setting the stage

Let me say up front that I am grateful to the Committee for calling this hearing today. Identity is a topic that impacts every American, but it's only recently that identity has started to get proper attention from policymakers in the U.S. At a high level, the way we handle identity in America impacts our security, our privacy, and our liberty. And from an economic standpoint, particularly as we move high-value transactions into the digital world, identity can be the great

enabler – providing a foundation for digital transactions and online experiences that are more secure, more enjoyable for the user, and ideally, more respectful of their privacy.

But when we don't get identity right, we enable a set of great attack points for criminals and other adversaries looking to execute attacks in cyberspace. And unfortunately, we have not been doing well here. A whopping 81% of hacking attacks were executed by taking advantage of weak or stolen passwords, according to Verizon's annual Data Breach Investigation Report. 81% is an enormous number – it means that it's an anomaly when a breach happens and identity does not provide the attack vector.

And outside of passwords, we've seen adversaries seek to steal massive data-sets of Americans, in large part, so that they have an easier time compromising the questions used in "identity verification" tools like Knowledge-Based Authentication or Verification solutions (KBA/KBV). This was illustrated quite vividly by the hack of the IRS's "Get my Transcript" application in 2015 – where more than 700,000 Americans had sensitive tax data compromised.

A key takeaway for this Committee to understand today is that attackers have caught up with many of the "first-generation tools" we have used to protect and verify and authenticate identity. Recent breaches may have driven this point home, but the reality is that these tools have been vulnerable for quite some time. There are many reasons for this – and certainly blame to allocate – but the most important question is: "What should government and industry do about it now?"

That's a key point – government and industry. If there is one message this Committee should take away from today's hearing, it's that industry has said they cannot solve this alone. We are at a juncture where the government will need to step up and play a bigger role to help address critical vulnerabilities in our "digital identity fabric."

Why Identity is so important to Financial Services

While identity is important to every sector of the economy, it's especially critical to the financial services industry – where it is essential to delivering four key outcomes:

1. The first is security. When the legendary bank robber Willie Sutton was asked "Why do you rob banks?" he answered "Because that's where the money is." These days, modern day Willie Suttons don't bother to show up at banks with guns – it's much easier for a robber to steal money by exploiting weaknesses in a bank or business that has mediocre identity and access controls. Financial services firms must embrace robust identity solutions that can block these attacks.

2. The second is the integrity of the financial system – particularly in blocking those who wish to make use of the financial system for money laundering, terrorist financing, and other nefarious acts.

3. The third is enabling great customer experiences. Many high-value transactions are still stuck in the paper world, thanks in part to the challenges with figuring out who is who online. If we're going to bring them online – and streamline the experience consumers and businesses go through in transactions – we need to sort out the identity layer.

4. And the fourth – emerging in importance in recent years – is enabling open banking: where consumers 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. Open banking is creating a need for more sophisticated identity solutions, as banks and fintech firms alike seek to enable consumers to authorize access to certain data

or permissions in their accounts on a granular level, and enable consumers to revoke access at any time. And getting identity right is key to making sure that the U.S. leads the way in the next generation of banking solutions.

Against this backdrop, there are three major challenges that every company in financial services must deal with:

1. The first is figuring out whether someone is who they claim to be at account opening. Not surprisingly, this is one of the areas where we have the most work to do. Losses from "New Account Fraud" increased 13% over the last year to $3.4 billion[2].

2. The second – closely tied to the first – is synthetic identity fraud. This is when fraudsters combine a fake name with a real SSN and "trick" the financial system into thinking that an applicant's identity is real when in fact it's a "Digital Frankenstein" made up of a mix of legitimate and fake identity components.

   According to a recent report from the Federal Reserve, synthetic identity fraud accounts for $6 billion in fraud each year, and some estimates suggest that number is as high as $8 billion.[3]

   The playbook for fraudsters has been a simple one: find a child's SSN – which our credit scoring systems – which double as our ID verification systems – have never seen, since

[2] See Javelin Research's Report "2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt" at https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt

[3] See https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

minors don't have credit – and pair it with a fake name to trick these systems into thinking that it's a legitimate identity. Over time, the fraudster then opens more and more accounts with this synthetic identity, racking up unpaid bills. Beyond the dollars lost, when a child turns 18 and tries to get her own credit established, she finds that her SSN is tied to a credit history that's a complete disaster – and now has to deal with the consequences.

3. And third is authentication. Once an account has been created – how you create systems that can securely log customers in to that account, in a world where passwords just don't cut it anymore?

Of these three challenges - within financial services, all of the challenges are not the same. If there is one takeaway I can offer about the state of the identity market in 2019, it is this: Authentication is getting easier, but Identity Proofing is getting harder.

Authentication is getting easier, but Identity Proofing is getting harder

Let me unpack that first part: Authentication is getting easier. By that, I mean that while passwords are broken, the ability of consumers and businesses to access tools that they can use in addition to – or in lieu of – passwords is greater than it's ever been. And with multi-stakeholder industry initiatives like the FIDO Alliance creating next-generation authentication standards that are getting baked into most devices, browsers and operating systems, it is becoming easier than ever to deliver on the vision of better security, privacy and convenience. This year, both Google and Microsoft announced that their Android and Windows platforms are FIDO certified, making it easier than ever for firms in financial services and other sectors to deliver passwordless

experiences. The development and adoption of the FIDO standards is, in my view, the most significant development in the authentication marketplace in the last 20 years.

And when these tools are paired with analytics solutions that use Artificial Intelligence and Machine Learning (AI/ML) to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords.

But while Authentication is getting easier – Identity Proofing is getting harder. By that, I mean the ability of consumers during initial account creation to prove that they are who they really claim to be is harder than ever – in part because attackers have caught up to the tools we have depended on for identity proofing and verification.

This means that it is harder than ever for businesses – as more transactions move online – to verify someone's identity when someone is creating an account or applying for a new service. Better tools are needed here. But unlike with passwords – where the market has responded with tools like FIDO authentication and behavior analytics to fix the problem – the market has not yet sorted things out here. And one thing that has become clear in discussion with industry is that the private sector cannot solve this problem on its own.

At the end of the day, government is the only authoritative issuer of identity in the United States. But the identity systems government administers are largely stuck in the paper world, whereas commerce has increasingly moved online. This "identity gap" – a complete absence of credentials suited for digital transactions – is being actively exploited by adversaries to steal identities, money and sensitive data, and defraud consumers and businesses alike.

Better Identity: How to Get There

The Better Identity Coalition lays out five key recommendations for how government and the private sector can improve the identity ecosystem.

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

   As I noted earlier, adversaries have caught up with the systems America has used for remote identity proofing and verification. Many of these systems were developed to fill the "identity gap" in the U.S. caused by the lack of any formal national identity system – for example, Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking an applicant several questions that, in theory, only he or she should be able to answer. Now that adversaries, through multiple breaches, have obtained enough data to defeat many KBV systems; the answers that were once secret are now commonly known. Next generation solutions are needed that are not only more resilient, but also more convenient for consumers.

   Industry is innovating here, and AI-enabled solutions are one of the tools that can help. But they are not enough. The single best way to address the weaknesses of KBV and other first-generation identity verification tools is for the government to fill the "identity gap" that led to their creation.

   While the United States does not have a national ID – and we do not recommend that one be created – the U.S. does have a number of authoritative government identity systems.

These systems are largely stuck in the paper world; none of them can be easily used – or validated – online.

This means that consumers are hamstrung if they need to prove their identity – or certain attributes about themselves – online, in that they are unable to use the credentials sitting in their pockets and wallets. It increases risk for both consumers and the parties they seek to transact with.

To fix this, 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 – by validating the information from the credential.

The creation of "Government Attribute Validation Services" can help to transform legacy identity verification processes and help consumers and businesses alike improve trust online.

Such services could be offered by an agency itself, or through accredited, privately run "gateway service providers" that would administer these services and facilitate connections between consumers, online services providers, and governments.

The Social Security Administration (SSA) and state governments – the latter in their role as issuers of driver's licenses and identity cards – are the best positioned entities to offer these services to consumers.

Note that the SSA is in the midst of building just the sort of Attribute Validation Service that we called for, the Electronic Consent Based Social Security Number Verification (eCBSV) Service. SSA is doing so in response to Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act, which was signed into law last year thanks, in part, to this Committee's work.

The eCBSV system will allow financial institutions and their service providers to electronically get a "Yes/No" answer as to whether an individual's SSN, name, and date of birth combination matches Social Security records.

We're thrilled to see SSA move forward here.

First, because eCBSV will change the game in the fight against synthetic identity fraud, which costs the country $6-$8 billion annually. The fact that fraudsters have been targeting the SSNs of children to commit this fraud is especially galling – eCBSV will give the country a tool to fight back.

And second, because what SSA is doing here provides a template for other agencies.

To that end, we were elated to see the White House Office of Management and Budget (OMB) embrace our recommendation for government to play a bigger role in identity proofing with the issuance in May of OMB Memorandum 19-17, entitled "Enabling

Mission Delivery through Improved Identity, Credential, and Access Management."

Page 8 of the memo[4] states:

> *"Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing· events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.*
>
> *"These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs."*

In the wake of this White House policy memo, the table is set for a new wave of tools that not only help fight identity theft and fraud, but also give consumers new ways to more easily do business online.

We were also thrilled to see the Treasury Department echo our idea of leveraging the identity proofing process tied to state driver's licenses in the report they put out last summer on "Nonbank Financials, Fintech, and Innovation." Per their report[5]:

> *"Treasury encourages public and private stakeholders to explore ways to leverage the REAL ID Act driver's license regime — particularly, robust state*

[4] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[5] https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

REAL ID license identity proofing processes — to provide trustworthy digital identity products and services for the financial sector."

Note that this concept was also embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity[6], who, in response to the wave of attacks leveraging compromised identities, stated "The government should serve as a source to validate identity attributes to address online identity challenges." Per the report:

"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

[6] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

establish parameters and trust models for validating and using those industry attributes."

The Coalition is thrilled that government has begun to act on this recommendation – as evidenced by the OMB memo and the launch of the SSA initiative. But going forward, we think four more things are needed:

1) A formal government-wide initiative, led by the White House, dedicated to identifying which Federal agencies besides SSA are best suited to offering new consumer-centric identity services, as well as ensuring each agency has adequate resources to stand these services up.

2) Work at NIST to lead development of a framework of standards and operating rules to make sure these services are built in a way that sets a high bar for security and privacy.

3) The establishment of a formal "Identity Center of Excellence" in government that can develop a standardized architecture for these services which implements the framework, and assist selected agencies in getting these systems established.

4) A new grant program to provide funding to states to help them implement this architecture and framework in state DMVs – accelerating their transition to being digital identity providers.

These four initiatives could be accomplished by legislation or via an Executive Order – we don't have strong views as to which path is pursued, only that action is taken. We

would welcome the chance to work with the members of this committee on ways to drive these initiatives forward.

2. *Rethink America's use of the Social Security Number.*

Many of our woes in identity are linked to the rather bizarre way the United States has treated the Social Security Number over the last 80 years. I expect the history of the SSN is well known to this Committee, but I do think it's worth briefly pointing out some of the contradictions in policy around how it should be managed and used.

- First, the SSN is simultaneously presumed to be both secret and public. Secret because we tell individuals to guard their SSN closely. Public, because we also tell individuals to give it out to facilitate all sorts of interactions with industry and government. Secret because we tell those entities in both government and the private sector to ensure that if they store it – which the law often requires them to do – that it be protected. And public, because that's proven quite hard to do: to the point that the majority of Americans' SSNs have been compromised multiple times over the last several years amidst a wave of data breaches.

- Second the SSN is commonly used as both an identifier and an authenticator. As I will discuss today, years of breaches mean the SSN is of little value for authentication – but it is still quite valuable in the role it was first created for, as a unique identifier. Understanding this difference is key to crafting a solid strategy for the SSN's future.

- Third, the SSN system is managed by an agency not formally tasked with providing an essential element of the country's identity infrastructure. Yet the SSA finds itself in that role by default – and is increasingly being asked to do more.

These policy contradictions are not the result of anything malicious; on the contrary, they reflect years of trying to balance several important roles played by the SSN and the SSA. What's most important now is that the government 1) recognizes these contradictions, and 2) takes steps to put policies in place that are more consistent, and that put us on a path toward a system that enhances security, privacy and convenience for Americans.

That process starts by changing how we view the SSN and how we use it.

1. Up front, government should acknowledge that there is not a need to "replace" the Social Security Number (SSN) – at least not in the way that some have suggested in recent years. Rather, government should take steps to change how we use it.

   There's been a ton of discussion on this topic over the last two years as some industry and government leaders, along with security and privacy experts, have called for the country to come up with "something to replace the SSN."

   Unfortunately, the debate has been muddled by people failing to differentiate between whether the SSN is an identifier or an authenticator. Part of the confusion is that SSN has been used as both identifier and authenticator in recent years.

At its core, the SSN was created as an identifier. It is a 9-digit code, issued by the Social Security Administration at birth, that is used to help the government know "which Jeremy Grant" they should associate wage and tax data with, and to help administer the delivery of Social Security benefits. Over time, use of the SSN has expanded beyond the purposes for which it was intended, with thousands of private sector entities collecting the SSN as part of the account opening experience — and by credit reporting firms, data brokers, and other private firms, who have used the SSN as one way to aggregate and match data about a person.

These expanded uses of the SSN are all as an identifier. But where things have really changed is the practice of using the SSN as an authenticator. Every time a party asks for the last four digits of that number, for example, the premise is that the SSN is a secret — and thus possession of the SSN could be used to authenticate a person.

There was a time when SSN as authenticator made sense: someone's SSN was not widely known or publicly available, so it was safe to presume that it was a secret. But in 2019 — after several years of massive data breaches where millions of SSNs have been stolen — the notion that SSNs are a secret is a fallacy. The Equifax breach may have woken people up to this fact, but for several years now, SSNs have been widely available on the dark web for just a dollar or two.

The message is clear: data breaches have gotten bad enough that we should assume an attacker can get someone's SSN with only minimal effort. The

attackers have caught up to authentication systems that use SSN as a factor — it's time to move on to something better.

With this, we need to move beyond using the SSN as an authenticator. Beyond delivering immediate improvements to security, such a move would also lessen the value of SSNs to criminals and other adversaries.

2. Just because SSNs should no longer be used as authenticators does not mean that we need to replace them as identifiers. When architecting a system for security, identifiers don't have to be a secret – and many times it is desirable that they be known. Given that - rather than replace the SSN as an identifier, instead, let's start treating SSNs like the widely-available numbers that they are.

Doing this is the single best way to reduce the risks associated with use of the SSN as an identifier. If we shift everybody's mindset to one where everybody understands that SSNs are widely known – and design security systems that don't allow someone with just an SSN to use it to gain access to data or services – it effectively devalues the SSN as an attack point.

There have been a number of proposals suggesting that America should instead scrap the SSN and invest in creating a new, revocable identifier administered by the SSA.

I've yet to see any proposal that does not involve spending tens of billions of dollars and confusing hundreds of millions of Americans – with very little security benefit. The reality is that both government and industry would simply

map that new identifier back to the SSN and other data in their systems. Because the new and old identifiers would be connected, the security benefits would be close to nil.

Moreover, the possibility of chaos due to errors in mapping and matching these additional identifiers would be quite high, given that many government and commercial systems deliver less than 100 percent accuracy today; think about what might happen when a system fails to associate a new identifier with the right person.

Winston Churchill once said: "Democracy is the worst form of Government except for all those other forms that have been tried." So it is with the SSN – it's not a perfect identifier, but keeping it beats the alternatives.

Rather than create a new identifier, the focus ought to be on crafting better authentication solutions that are not dependent on the SSN, and are resilient against modern vectors of attack.

3. Back on the topic of identifiers: even if we assume that the SSN is publicly known, that doesn't mean that it needs to be used everywhere. Many of the members of the Better Identity Coalition would love to reduce where they use the SSN, due to the risks that collecting and retaining SSN may create relative to other identifiers. Our Blueprint documented how one of our members, Aetna, embraced a six-year, $60 million initiative to do just that – with great success. However, in some cases, they are running up against laws and regulations that

require companies to collect and retain the SSN. Our Policy Blueprint contains a 6-page appendix detailing some of these legal requirements. Among them:

- The Federal government requires employers to collect SSN each time they hire someone
- The Federal government requires financial institutions to collect the SSN as part of account opening or applying for a mortgage – and requires them to retain it for up to five years after the account is closed
- The Federal government requires college students to provide their SSN when applying for student loans
- The Federal government requires state governments to collect the SSN when Americans apply for a driver's licenses
- Health insurers are required by the government to collect the SSN of each person they insure
- Many states require blood donation services to collect and retain the SSN of blood donors
- The Coast Guard requires SSN to be collected as part of its Vessel Identification System

Much of industry's ability to reduce their reliance on the SSN will be dependent on the government changing its requirements for them to collect it.

Moreover, this list also demonstrates just how embedded the SSN is as an identifier in so many of our identity processes – and helps to frame the complexity and cost associated with any effort to replace it.

3. *Promote and Prioritize the Use of Strong Authentication*

On the authentication topic – we need to recognize that the problems with using SSNs as an authenticator extend to using any "shared secret" for authentication. It doesn't matter if the so-called "secret" is the SSN or passwords – they both are terrible.

As I mentioned earlier, 81% of 2016 breaches were enabled by compromised passwords, which is about as clear a sign as you can ask for that things need to change. There is no such thing as a "strong" password or "secret" SSN in 2019 and we should stop trying to pretend otherwise. We need to move the country to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.

There is good news in this regard: parts of government and industry have recognized the problems with old authenticators like passwords and SSNs – as well as other forms of authentication using "shared secrets" – and worked together these past few years to make strong authentication more secure and easier to use. Multi-stakeholder groups like the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C) have developed standards for unphishable, next-generation multi-factor authentication (MFA) that are now being embedded in most devices, operating systems and browsers, in a way that enhances security, privacy and user experience. Government should recognize the significance of this market development that is enabling authentication to move beyond the password, and embrace it.

What makes this possible is the fact that the devices we use each day have evolved. Just a few years ago, MFA generally required people to carry some sort of stand-alone security device with them. This added costs and often degraded the user experience. Moreover, these devices were generally not interoperable across different applications.

Today, however, most devices – be they desktops, laptops or mobile devices – are shipping from the factory with a number of elements embedded in them that can deliver strong, multi-factor authentication that is both more secure than legacy MFA technology and also much easier to use.

What are these elements?

1) Multiple biometric sensors – most every device these days comes with fingerprint sensors, cameras that can capture face and sometimes iris, and microphones for voice.

2) Special tamper-resistant chips in the device that serve as a hardware based root of trust – such as the Trusted Execution Environment (TEE) in Android devices, the Secure Enclave (SE) in Apple devices, or the Trusted Platform Module (TPM) in Windows devices. These elements are isolated from the rest of the device to protect it from malware, and can be used to 1) locally match biometrics on the device, which then 2) unlocks a private cryptographic key which can be used for authentication.

Together, these two elements enable the ability to deliver authentication that is materially more secure than older authentication technologies, and also easier to use. Because rather

than require the consumer to carry something separate to authenticate, these solutions are simply baked into their devices, requiring them to do nothing more than place a finger on a sensor or take a selfie.

The rest of the authentication (the other factors) automatically happens "behind the scenes" – meaning that the consumer doesn't have to do the work. A biometric matched on the device then unlocks a second factor – an asymmetric, private cryptographic key, that can then be used in conjunction with a public cryptographic key to securely log the consumer in, without a password or any other shared secret. The private key is stored in – and never leaves – the hardware device that the user controls.

While the actual composition of these two elements – both biometric sensors and security chips – varies across manufacturers, most of the companies involved in making these devices and elements have been working together to create the FIDO and related W3C Web Authentication standards. The power of these standards is that they enable all of these elements all to be used – interoperably – in a common digital ecosystem, regardless of device, operating system or browser. Which means that it's become really easy for banks, retailers, governments and other organizations to take advantage of these technologies to deliver better authentication to customers. Firms such as Aetna, PayPal, Google, Microsoft, Cigna, Intel, T-Mobile, Samsung, and several major banks are among those enabling consumers to lock down their login with FIDO authentication; the General Services Administration (GSA) recently enabled Americans logging into government websites with the Login.gov solution to protect their accounts with FIDO as well.

Note that FIDO also is the essential standard in Security Keys: external, portable hardware-based authenticators that can be used across multiple devices over interfaces including USB, NFC and Bluetooth. These Security Keys are widely used in devices and environments where built-in authentication is not available, as well as in environments where an external authenticator might be preferred to one that is built in.

Government can play a role in accelerating the pace of adoption of strong authentication through three key actions:

1) First, agencies should look to follow GSA's lead and make use of the FIDO and W3C Web Authentication standards in more of its own online applications. This will set an example for the private sector to follow – and ensure that citizen-facing applications are more secure and convenient to use. The SSA should be among the first here, given the importance of its MySSA online portal.

2) Second, through the regulatory process, government should ensure that regulated industries are keeping up with the latest threats to first-generation authentication – and implementing the latest standards and technologies to address these threats.

3) Third, when crafting new rules or guidance on privacy and security, it is important to make sure that language is not written so broadly that it might preclude use of promising technologies for risk-based authentication. As I noted earlier, when tools like FIDO are paired with analytics solutions that use Artificial Intelligence and Machine Learning

(AI/ML) to "score" in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords. However, the use of these promising analytics tools might be threatened if their use is inadvertently precluded by new privacy legislation or regulation.

In Europe, they seem to have gotten this balance right. While Europe's General Data Protection Regulation (GDPR) limits the collection of data in many circumstances, it also highlights that when it comes to protecting security and preventing fraud, there are cases where an entity may have a "legitimate interest" in processing personal data – including in cases where such data can be used to deliver secure authentication or verification capabilities. This "carve out" has allowed the use of data-based security and consumer protection solutions to flourish. In fact, the European Banking Authority (EBA) is specifically encouraging banks and fintechs to use these technologies to secure open banking and payments.

In contrast, California's recently passed California Consumer Privacy Act (CCPA) has more ambiguous language that some experts have interpreted as allowing consumers to opt out of having their data used to protect against malicious, deceptive, fraudulent, or illegal activity. This could inhibit the deployment of new, innovative authentication and verification technologies and place consumers at risk – and provides an example of

the potential consequences of overly prescriptive or poorly drafted policies or frameworks.

California's state legislature is considering some tweaks to CCPA that might address these concerns, but it is unclear if they will be adopted.

4. *International Coordination and Harmonization*

Consumers and businesses operate in environments beyond American borders, and other countries are also contemplating new approaches to making identity better. The United States should look for ways to coordinate with other countries and harmonize requirements, standards and frameworks where feasible and compatible with American values.

Coordination and harmonization is particularly relevant in the financial services industry, where a shift to digital banking and the emergence of "fintech" startups is disrupting traditional business practices – and challenging requirements for managing risks associated with the Customer Identification Program (CIP) requirements of the Bank Secrecy Act (BSA), as well as related Know Your Customer (KYC) and Anti-Money Laundering (AML) rules.

In the U.S., the push for "Open Banking" – where consumers 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 – is creating a need for more sophisticated identity solutions, as banks and fintech firms alike seek to enable consumers to authorize access to certain data or permissions in their accounts on a

granular level, and enable consumers to revoke access at any time. Robust identity solutions are at the heart of these applications, given the need to ensure that those authorization requests are coming from the right person, as well as comply with KYC rules for any new account opening.

Here, we think the U.S. should look to leverage ongoing work in the Financial Action Task Force (FATF) to ensure recognition of American identity solutions for digital financial services abroad, as well as explore the possibility of allowing U.S. financial institutions to leverage high-assurance digital credentials from other countries for foreigners looking to establish accounts in the U.S. The FATF is heavily focused on anti-money laundering and terrorist financing issues – particularly the role of better identity solutions in making it easier to address these critical concerns. The benefits of coordination and harmonization here could extend beyond financial services to encompass a wide array of digital commerce.

5. *Consumer and Business Education*

Finally, as part of improving the identity ecosystem, Americans must be aware of new identity solutions and how to best use them. Government should partner with industry to educate both consumers and businesses, with an eye toward promoting modern approaches and best practices. The National Cyber Security Alliance (NCSA) – which has a strong record of driving public/private partnerships to educate the public on cybersecurity – should be leveraged to promote better identity outcomes.

In closing, while the current state of digital identity poses some challenges to the financial service industry, they are not insurmountable. On the contrary, we have before us a series of ideas on the future of identity that can be used to address these challenges – and that are actionable today. I am grateful for the Committee's invitation to offer recommendations on how government can improve the identity ecosystem, and look forward to your questions.

TESTIMONY OF AMY WALRAVEN

Founder and President of Turnkey Risk Solutions

Before the

Task Force on Artificial Intelligence

United States House Committee on Financial Services

Hearing on "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"

September 12, 2019

Chairman Foster, Ranking Member Hill, and members of the task force, thank you for the opportunity to appear before you and provide testimony today to help inform discussions on the future of Identity in the Financial Services sector: threats, challenges, and opportunities.

My name is Amy Walraven. I'm the founder and president of Turnkey Risk Solutions (TRS). TRS is a risk management company specializing in the development and application of highly complex algorithms specifically targeting emerging fraud threats. Prior to starting TRS, I spent over 20 years in the financial services sector at several major financial institutions. I have been a career risk manager primarily focused in the areas of fraud, risk, and compliance. The last 10 years of my banking career were spent at J.P. Morgan Chase. I was responsible for establishing business practices specifically focused on the proactive identification, mitigation, and remediation of various fraud threats including but not limited to credit bust outs, identity manipulation, credit abuse, and synthetic identities.

As we consider how to utilize artificial intelligence and machine learning to navigate big data to identify consumers, it is important that we clarify our target by gaining a more comprehensive understanding of what synthetic identities are. I have been asked to provide the committee a brief overview of the factors that contributed significantly to their emergence in order to better frame the threats and challenges the future of identity is facing in financial services.

For the purposes of my discussion, a synthetic identity is one that is created with a combination of potentially real and/or fake information like a Social Security Number (SSN), name, address, date of birth, etc. to create a new fictitious identity. It is important to note that creating a synthetic identity is materially different than traditional identity theft. In cases of traditional identity theft, the criminal is impersonating a real person by using that person's true identity elements to potentially open accounts and commit fraud in the victim's name or take over existing accounts held by that individual. In cases of synthetic identities, the criminal may be using limited elements of a true person's identity –for example, just their social security number and then leveraging that one piece of information to create an entirely different persona that is completely separate and distinct from the real person.

Once that synthetic identity has been created it can be leveraged just like any conventional identity. For example, it can be used to open bank accounts or apply for loans and other products in the financial

services sector. However, synthetic identities are not limited to just financial services. They can establish a presence on social media, be used to purchase cell phones or insurance policies, rent apartments, obtain utilities, enroll in benefits programs, etc. These identities can be used for whatever purpose suits the creator and/or manager of the synthetic identity.

To better understand the threat of synthetic identities, I believe it's important to understand the current landscape and the factors contributing to this rapidly growing identity fraud issue. There are four major factors contributing to the emergence of synthetic identities. They are as follows:

1) Technology – advances in technology have increased convenience, speed, and provided anonymity for the criminals. In addition, the aged infrastructure makes it difficult to combat today's threats.
2) Consumer awareness – consumers are more informed on the credit infrastructure and different fraud threats. They expect immediate access and decisions and understand the power of social media. Criminals are using those same resources designed to inform consumers to reverse engineer and help formulate their attacks.
3) Regulations and new controls - Consumer protection agencies and legislation are in place to provide consumers who have been a victim of identity theft a wealth of enhanced protections and benefits. Those same regulations and controls have had unintended consequences. We have seen those same protections be exploited, leveraged, and abused by criminals. Adding chips to credit cards to reduce counterfeit activity forced the fraud into other channels like card not present and synthetic identities.
4) Data Breaches – originally were focused on compromising credit/debit card data, those types of breaches are inconvenient for the customer and can be expensive for the issuer but can typically be resolved fairly quickly once detected. Many breaches have shifted to targeting personal identifiable information or PII allowing criminals to create entire profiles on individuals and use them to commit fraud or package them up for sale.

All of these factors have played a major role in the emergence of the use of synthetic identities. This fraud threat was specifically engineered to evade existing controls while exploiting vulnerabilities in the financial system and beyond impacting other industry verticals. Many of the groups committing this type of fraud are: highly organized, extremely sophisticated, and tend to be transnational in nature. These adversaries are focused, committed, well-funded, and have access to the same technological advances as we do. As an industry, we must be proactive in our actions, unified in our defenses, and more effective in our application of evolving technologies including artificial intelligence.

As we seek to deliver unprecedented speed and convenience to increasingly mobile and technology dependent consumers and businesses, we must remain vigilant in understanding the threats to our interests. Synthetic identity fraud in the United States and around the world is widespread and inconceivably pervasive. It is being amplified by increased digitalization of products and processes when coupled with a proliferation of available data; synthetic identity fraud readily operates across all delivery channels, providing the perpetrators with potentially unfettered access to our nation's financial system and federal programs -- making it essential that we act in a unified and collaborative manner to protect the integrity of our infrastructure.

In order to do so, we must recognize the complexity of these next generation fraud types and be fully informed on their severity and scope. Advances in technology alone cannot identify and resolve these

issues. Mitigation efforts from industry and government must be fluid and nimble to ensure we have the ability to effectively address these issues with urgency they deserve. Our control framework needs to be updated to specifically address synthetic identity fraud. It needs to be universally defined, in order for institutions to detect, report, and remediate it.

FSC Washington Testimony.

"The Future of Identity in Financial Services: Threats, Challenges, and Opportunities,"

The Task Force on Artificial Intelligence
House Financial Services Committee
United States Congress

Anne L. Washington, PhD
Steinhardt School
New York University

September 12 2019

Thank you for inviting me to speak today. My name is Anne Washington. I am an Assistant Professor of Data Policy in the Department of Applied Statistics[1] at New York University. Before my career in Academia, I spent eight years in financial services with a data-driven company in San Francisco. I also spent a decade in the legislative branch working with many of the data structures and tools used to make this hearing possible. I would also like to acknowledge that I serve on the Academic Advisory Board of the Electronic Privacy Information Center, EPIC. I hold an undergraduate degree in computer science from Brown University, a graduate degree in Library and Information Science from Rutgers University, and a doctorate from The George Washington University School of Business.

My testimony, today, represents my own views as a public interest technologist. As a computer scientist and organizational scholar with expertise in open government data, I am part

[1] I am in the Steinhardt School of Culture, Education, and Human Development at NYU and the Department of Applied

of a growing movement of people[2] using STEM[3] skills in non-profits and the public sector. My academic specialty is understanding the organizational dynamics that shape the production and consumption of information, especially in organizations that have a public mission.

The courses I teach to graduate students at New York University are the "Management and Ethics of Data" and the "Ethics of Data Science". In my testimony today, I will give you a crash course on data ethics, squeezing two semester-long courses into a five-minute briefing.

Artificial intelligence is not infallible. Even the most successful artificial intelligence systems used by online financial platforms require human input. For Americans to participate equally in our financial system, we need inclusive innovation that is aware of difference. Ignoring AI exceptions in financial services risks excluding many in our society because they are outliers from expectations. Organizations must begin to think about how they will handle future disputes over AI errors.

Artificial intelligence in the financial sector is an ethical, mathematical, and policy issue. To illustrate this, I will elaborate on three main points:

1. Artificial intelligence produces errors. When operating "at scale" even low error rates can impact millions. Errors in financial services will be consequential to specific individuals.
2. Because organizations are more likely to believe their technology systems over the experiences of individuals, individuals need procedures for recourse in the event of processing error.
3. Systems built to consider a broader range of populations must be more fault tolerant of cultural difference to be robust.

[2] Such as Desmond Patton trained in computer science and social work at Columbia University. Dierdre Mulligan trained in Law and teaching in the Berkeley Information School. See Bruce Schneier's Public Interest Technology list.
[3] Science Technology Engineering and Math

Ethics

The study of ethics concerns itself with questions of appropriate behavior and actions. For centuries, the assumption behind ethics has been that we, as human beings, were driving our actions. Today, we are confronted with computer systems acting on behalf of humans. Ethical questions arise when actions violate the public trust.

Artificial intelligence is a technology that gives organizations an incredible power over individuals. M. Lynne Markus[4] (2016) reminds us that the information on millions of people is in the hands of only a few and those organizations have a "corporate *data* responsibility".[5]

Data technology, such as artificial intelligence, drives all sectors of industry including financial services. Digital material from sensors, transactions, cell phones, networks, social media, and other digital traces feed into systems that generate artificial intelligence. Digital traces like these when reused in new contexts might trigger ethical concerns if not traceable and joined appropriately.

These pipelines into the "data supply chain"[6] are mostly owned and operated by corporate bodies and not individuals. Christine Borgman (2015) argues that digital systems generate not just big data, but also small data, or even no data[7] . These natural inconsistencies can create havoc when data technologists attempt to connect data from different sources. Many of these

---

[4] Markus, M. L. (2016). Obstacles on the Road to Corporate Data Responsibility. In C. R. Sugimoto, H. R. Ekbia, & M. Mattioli (Eds.), Big data is not a monolith (p. 143). MIT Press.

[5] The term Corporate Data Responsibility is based on the well known concept in management of corporate social responsibility. Some scholars are now understanding data is a part of that responsibility within supply chains. See Amaeshi, K. M., Osuji, O. K., & Nnodim, P. (2007). Corporate Social Responsibility in Supply Chains of Global Brands: A Boundaryless Responsibility? Clarifications, Exceptions and Implications. Journal of Business Ethics, 81(1), 223–234. doi: 10.1007/s10551-007-9490-5

[6] Washington, Anne L. (2014). Data Supply Chains. Invited Workshop Leader. The Social, Cultural, & Ethical Dimensions of "Big Data" sponsored by the White House Office of Science and Technology Policy (OSTP). Afternoon Breakout Sessions. Hosted by Data & Society Research Institute and the New York University (NYU) Information Law Institute. March 17. New York, NY. http://www.whitehouse.gov/issues/technology/big-data-review

[7] Borgman, C. L. (2015). Big data, little data, no data: Scholarship in the networked world. http://lccn.loc.gov/2014017233.

technologies are perfectly legal and necessary for innovative growth, however ethical questions remain. Those in power who use this data must be reminded that data can make people vulnerable.

Artificial intelligence (AI) has grown our economy by driving economies of scale. Its efficiency provides gains in productivity and precision (Dhar, 2013; Halevey & Norvig, 2009). AI, however, can also obscure policies (Eubanks, 2018), and exacerbate bureaucracy (Peeters & Schuilenburg, 2018) amongst other concerns (Rossi, 2019; Wiggen, 2017). The tension between pragmatic efficiency and the moral tug of appropriate action plagues adoption of AI technologies by governments.

The artificial intelligence[8] I discuss here, today, is data technology that enables oversight, automates decisions, or augments observations over large streams of data. Data technology includes data science, machine learning, predictive analytics, evidence-based policy, and computational tools based on the consumption and analysis of large quantities of information. Usually, these systems work with algorithms that sort, rank, search, and calculate in order to generate consistent outcomes. On the surface, these systems appear to be neutral, mechanical, and routine-driven, but when placed within human societies they can have substantial repercussions within our daily lives. The computer scientist Meredith Broussard says that these socially agnostic systems are not robust enough and labels them as "artificial unintelligence".[9]

The power of data technology is derived from the amount of data it uses. When data technology struggles to identify individuals in a database, the solution is often to combine more

[8] Intelligence can take many forms and has changed definitions over the years. Belkin, N. J. (1996). Intelligent information retrieval: Whose intelligence? In ISI - International Symposium for Information Science: Vol. 96. Proceedings of the Fifth International Symposium for Information Science (pp. 25–31). and Gardner, H. (1983). The Idea of Multiple Intelligences. In Frames of Mind: The theory of multiple intelligences (pp. 3–11). New York: Basic Books Inc.

[9] Broussard, Meredith 2018. Artificial Unintelligence: How Computers Misunderstand the World. MIT Press, Boston, Mass.

databases into decision making. Amassing data in this way makes individuals entirely too visible (Rocher, 2019; Sweeney, 2013). Privacy and the "politics of real names,"[10] danah boyd tells us, are real concerns. At the core of these concerns are questions not only of social categorization[11] (Cherng, 2017) but also of technical abstraction (Walsh, 1992).

Ethics programs, like the one at NYU, want to help build better data systems. By baking privacy, security, and usability into the design of our AI systems, we can build a more responsible and ethical data environment like the solutions proposed by (Shilton, 2013) and (Cranor & Garfinkel, 2005)[12]. Others, such as the scholars at the Ostrom Center for Data Commons, are using the work of Nobel-prize winning economist, Elinor Ostrom, to better understand the ethics of knowledge commons (Raymond, 2018).

Data Ethics In Real Life

Every student of data ethics understands that large populations, coincidence, and cases of mistaken identity can confound the "trustworthiness" of AI systems.

Large Data Sets

Current AI-based systems, including financial systems incorporating AI, are not ready to

[10] boyd, danah. (2010, October). Why Privacy Is Not Dead. Technology Review, 113(5), 10–11.
boyd, danah. (2012). The politics of "real names." Communications of the ACM, 55(8), 29–31. doi: 10.1145/2240236.2240247

[11] The classic text on this is Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences. MIT PRESS. See also Bowker, G. C., & Star, S. L. (2000). Invisible Mediators of Action: Classification and the Ubiquity of Standards. Mind, Culture, and Activity, 7(1–2), 147–163. doi: 10.1080/10749039.2000.9677652
Suchman, L. (1993). Do categories have politics? Computer Supported Cooperative Work (CSCW), 2(3), 177–190. doi: 10.1007/BF00749015

[12] See Schlesinger, A., O'Hara, K. P., & Taylor, A. S. (2018). Let's Talk About Race: Identity, Chatbots, and AI. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 1–14. https://doi.org/10.1145/3173574.3173889 and Levy, K & Barocas, S ."DESIGNING AGAINST DISCRIMINATION" https://scholarship.law.berkeley.edu/btlj/vol32/iss3/5/ doi.org/10.15779/Z38BV79V7K

disambiguate enormous sets of people. The USA current has close to 330 million people. Some technology platforms have more users than the populations of countries. These large Internet platforms have specific authentication methods to identify a user who logs in that includes active involvement of the individual logging in. Financial service data, which travels between multiple institutions, is harder to track down and does not include the end-user actively as part of authentication and identification. This leads to loosely coupled systems that introduce noise into financial profiles. Evelyn Ruppert (2009, 2011) calls the digital traces that represent us a "data double". Our data double is similar to us but not exactly. Daniel Solove (2004) calls these data traces an "unauthorized biography" that contains some true things but lots of noise and innudedo that is not true. The scale of users and their data can introduce error into the decisions made by financial sector AI.

The Birthday Problem

Coincidences[13] are not a surprise to any student of statistics. Basic math theory tells us that what we expect is rare may be more likely than we think. The inquiry known as the Birthday Problem[14] asks: how many people are needed in a room for a good chance that two people are born on the same day of the year? Surprisingly the number is just 23. There is a 50% chance that in a room of 23 people, given true randomness, two people have the same birthday. In a room of 75 people, the chances are over 99% and a 1/3 chance that three people do. When two items resolve to the same set of information, computer scientists building a hash algorithm know this as a "hash collision".

The Birthday Problem has real world implications when we use this information to

[13] Stewart, I. (1998). What a Coincidence! - MATHEMATICAL RECREATIONS. Scientific American, 2. doi: DOI: 10.1038/scientificamerican0698-95

[14] Weisstein, E. W. (2019, September 6). Birthday Problem. Retrieved September 1, 2019, from MathWorld Wolfram website: http://mathworld.wolfram.com/BirthdayProblem.html

disambiguate identities. A classic example is the problem of watch lists that permit entry or deny services. Jeff Jonas, a pioneer in entity recognition, has explored this tension between privacy and recognition in a famous paper about the terrorist watch list. The authors conclude that actionable information is more important than aggregate lists that violate civil liberties (Harper & Jonas, 2006). The legal scholar Margaret Hu (2015) goes into extensive detail about these lists and their impact on people's lives.

These problems are not new (Solove, 2001; 2004) nor unknown to computer scientists and statisticians (Becker, 2006). What is new, however, is that these materials are moving from identification into action in ways that can aggregate a single mistake into an ongoing situation. The data supply chain moves not in one direction but in circles exacerbating mistakes.

Examples of mistaken identity

People have a difficult time fighting these lists once their names are on them.

- Jennifer Norris[15] of Boston was in danger of losing her job because of the inability to resolve a dispute about her identity. Her work required a driver's license and only after consulting her Congressman, Capuano of Massachusetts' 7th district and a local news agency was the problem resolved.

- Kathleen Casey[16], a pharmacy technician, lost her apartment in 2011 when a system confused her with someone else. It is important to note that some industries[17] such as retail pharmacy stores used informal lists to exclude any job candidate accused of theft.

[15] Kath, R. (2018, Apr 11) I-Team: Mistaken Identity Causes Bureaucratic Nightmares For Drivers. CBS News Boston . https://boston.cbslocal.com/2018/04/11/wbz-tv-i-team-drivers-bureaucratic-nightmares-mistaken-identity-federal- database/

[16] Liedtke, Michael (2011, Dec 16) How A Clerical Error Put A Woman On The Streets. Business Insider / AP . . https://www.businessinsider.com/mistaken-identity-put-this-woman-on-the-streets-2011-12

[17] Clifford, S., & Silver-Greenberg, J. (2013). Retailers Use Databases to Track Worker Thefts. The New York Times. And Knaub, Kelly (2014, Aug 4) "LexisNexis, Retail Workers Get Nod For $2.38M Settlement," Law 360. http://www.law360.com/articles/563583/lexisnexis-retail-workers-get-nod-for-2-38m-settlement.

- A teacher in Maryland[18] could not pursue her chosen livelihood because bad data continually haunted her in a job that requires continuous recertification.

The astounding case of Lisa S. Davis[19], the novelist, who wrote about her experience of encountering her data double in official documents for 18 years and finally meeting her. For years, their addresses were confused and they would get mail for each other. They had the same day of birth, the same year of birth, and not only the same middle initial, but the same middle name. Most systems have a hard time if not impossible time disambiguating them. They assume it is one person who perhaps has just moved to a new address. This data double story has more resonance in this case because the two women are different colors and live in neighborhoods with different policing behaviors. They are both in New York State so their information has a higher chance to be co-mingled in databases.

Resolving disputes

Davis (2017) relates her story of having information that would show that her experience and paper traces verified who she was. Her lived experience was no match to the certainty of a computer. She was assumed to be a liar and told to plead guilty to pay and clear the traffic violations.

Organizations tend to trust their computer systems over the customers' experience. Individuals with a wrong match, who are outliers, who clearly can identify a flaw in the system, are perceived as liars. Humans take the blame after a systems provides an answer. People with

[18] Meyer, Eugene L. (1997, Dec 15) "Md. Woman Caught in Wrong Net; Data Errors Link Her to Probes, Cost 3 Jobs," Washington Post C1. As discussed in Solove, D. (2004). The digital person: Technology and privacy in the Information Age. New York: New York University Press.

[19] Davis, Lisa Selin (2017, Apr 3) For 18 years, I thought she was stealing my identity. Until I found her . The UK Guardian https:// www.theguardian.com/us-news/2017/apr/03/identity-theft-racial-justice

lived experience that contradicts the artificial intelligence face significant challenges. It is like watching a toy robot go towards the corner and march in place endlessly.

Technologists building these systems want to learn this feedback. Businesses do not have a financial incentive to incrementally fix small errors. Any policy or best practice would give technologists inside organizations the leverage they need to spend their time fixing the errors. This feedback once incorporated could help prevent similar mistakes from being repeated later. This agile approach with feedback would help to incrementally improve the technology.

Individuals should have recourse in these situations. It is mathematically certain that collisions will occur. Without any form of redress, innovation will stall and many people will be locked out of financial systems.

It is important to note that these stories all focus on individuals but one-person Internet shops[20] that rely on technology infrastructure are even more vulnerable. Owner-operator and new entrepreneurs, and small business who are establishing their validity in markets have high risks if locked out of financial capital.

POLICY

My remarks on policy alternatives will be the most brief. Legal scholarship in this area is extensive especially in data[21] used in policing and court data[22] system. The scholarship of

[20] BBC News (2019, Aug 15) 'My Instagram got hacked and I lost my business' - BBC News . . . https://www.bbc.com/news/business-49397038

[21] See works by Julie Cohen and Paul Ohm. Especially: Cohen, Julie E. (2012). What privacy is for. Harvard Law Review, 126, 1904. ; Ohm, Paul. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA l. Rev., 57, 1701. and Ohm, Paul. (2011). The fourth amendment in a world without privacy. Miss. LJ, 81, 1309.

[22] See Wexler, R. (2017, June 13). When a Computer Program Keeps You in Jail. The New York Times, p. A27. Wexler, R.

Danielle K. Citron and Frank A. Pasquale [23] have covered many plausible solutions.

I suspect that there will be a debate over the feasibility of establishing recourse. As usual, some will suggest that new regulations should be put in place. It would be logical to extend the Fair Credit Reporting Act (FCRA) into the 21st century and acknowledge the role of data sources. Others will suggest that self-monitoring would be sufficient. It makes sense to allow innovation to develop without unnecessary constraints since the future of these technologies is hard to foresee. Associations[24] and industry cooperatives[25] could continue to establish best practices across the field.

In my opinion, neither of these traditional responses gets to the heart of the issue which is that data-driven organizations need to establish internal data policy that matches their values with the business model. Data-driven organizations might run on a variety of business models (Shapiro & Varian, 1998) so it is a management decision what policy best matches those goals. I see these concerns as extensions of early conversations about organizational memory (Ackerman, 2000; Anand, 1998) that asked what information[26] should organizations keep as technology became ubiquitous.

(2018). Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System. Stanford Law Review. Selbst, A. D. (2017). Disparate Impact in Big Data Policing. Ga. L. Rev., 52, 109.; And Hu, M. (2017). Algorithmic Jim Crow. Fordham Law Review, 86(2), 633-696. And Eaglin, J. M. (2017). Constructing Recidivism Risk. Emory Law Journal, 67(1), 59–122.

[23] See Pasquale, F. (2015a). Reforming the Law of Reputation. Loyola University Chicago Law Journal, 47, 25. Pasquale, F. (2015b). The black box society: The secret algorithms that control money and information. Pasquale, F. (2017). Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. Ohio State Law Journal, 78(5), 1243–1255. Pasquale, F. A. (2018). A Rule of Persons, Not Machines: The Limits of Legal Automation. George Washington Law Review. Pasquale, F. A., & Citron, D. K. (2014). Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society. Washington Law Review, 89, 1413–1424.
And Citron, D. K. (2008a). Cyber Civil Rights. Boston University Law Review, 89, 61–125.
Citron, D. K. (2008b). Technological Due Process. Washington University Law Review, 85(6), 1249–1313.
Citron, D. K. (n.d.). Fulfilling Government 2.0's Promise with Robust Privacy Protections. The George Washington Law Review, 78, 24.

[24] A group like the Public Policy council for the Association of Computing Machinery is an ideal place to work out many of these policy issues with experienced technologists.

[25] An industry membership group like , such the Partnership on AI, the Future of Privacy Forum, or the Data Coalition, can share invaluable and realistic advice when confronting these issues in themidsts of operations.

[26] Agar, J. (2006). What Difference Did Computers Make? Social Studies of Science, 36(6), 869–907.

One critical role for public policy is data standards. Governments could establish data standards that would relieve the burdens of anyone trying to investigate issues across firms. Standardized data structures could also a mechanism to trigger retrospective tracking for regulators, e-discovery, or internal business intelligence. The reuse and exchange of digital material is complicated by many social and organizational challenges (Borgman, 2000; Bowker, 1996; Edwards, 2011; Fedorowicz, 2010; Markus, 2006). A solid internal information policy (McClure 1989; Robinson, Yu, Zeller, & Felton, 2008) is critical for any data-driven organization. For example, in the public sector the 2014 DATA Act produced a stable data infrastructure across all agencies that made later analysis, correction, and innovation possible. Digital government scholars such as Sharon Dawes (1996, 2010), Theresa A. Pardo (2012), Marijn Janssen (2016), Lemuria Carter (2018), Paul Jaeger & John Bertot (2010) have written extensively about the importance of data structures in government transparency.

Governments often neglect that their greatest power in public policy is mandating data infrastructure. Identity standards for financial services would greatly serve to expedite the adoption of artificial intelligence that benefits wide audiences.

Summary

Artificial intelligence, often implemented to save labor costs, will still require human labor to handle anticipated exceptions. A dispute resolution process solves two problems: procedural justice and technology improvement. First, it establishes a procedure to preserve the sanctity of human experience in situations where organizations may be more likely to trust the AI over a customer. Second, it provides the necessary feedback for incremental improvement of the technology.

Artificial intelligence will have its exceptions and people need procedures to assert the authority of their lived experience over the authority of the numbers.

BIBLIOGRAPHY

Ackerman, M. S., & Halverson, C. A. (2000). Reexamining organizational memory. Communications of the ACM, 43(1), 58–64. doi: 10.1145/323830.323845

Aitkin, R. (2017). 'All data is credit data': Constituting the unbanked. Competition & Change, 21(4), 274–300. doi: 10.1177/1024529417712830

Azerrad, David (2019) Back Row America. https://www.heritage.org/poverty-and-inequality/commentary/back-row-america

Becker, J. P., & Wallace, J. (2006). Eighty Ways to Spell Refrigerator. Proceedings of the Thirty-First Annual SAS Users Group International Conference. Retrieved from http://www2.sas.com/proceedings/sugi31/074-31.pdf

Belkin, N. J. (1996). Intelligent information retrieval: Whose intelligence? In ISI - International Symposium for Information Science: Vol. 96. Proceedings of the Fifth International Symposium for Information Science (pp. 25–31). Retrieved from http://comminfo.rutgers.edu/tipster3/iirs.html

Benjamin, R. (2019). Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life. Durham, NC: Duke University Press.

Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code. Cambridge, UK: Polity.

Berlins, M. (2008, November 2). A Kafkaesque excuse for ignorance of the law. The Guardian. Retrieved from http://www.theguardian.com/uk/2008/nov/03/law-kafka-transparency-marcel-berlins/print

Borgman, C. L. (2000). From Gutenberg to the global information infrastructure: Access to information in the networked world. Cambridge, MA: MIT Press.

Borgman, C. L. (2015). Big data, little data, no data: Scholarship in the networked world. .

Bowker, G. C. (1996). The history of information infrastructures: The case of the international classification of diseases. Information Processing & Management, 32(1), 49–61. doi: 10.1016/0306-4573(95)00049-M

Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences.

Bowker, G. C., & Star, S. L. (2000). Invisible Mediators of Action: Classification and the Ubiquity of Standards. Mind, Culture, and Activity, 7(1–2), 147–163. doi: 10.1080/10749039.2000.9677652

boyd, danah. (2010, October). Why Privacy Is Not Dead. Technology Review, 113(5), 10–11.

boyd, danah. (2012). The politics of "real names." Communications of the ACM, 55(8), 29–31. doi: 10.1145/2240236.2240247

Broussard, Meredith 2018. Artificial Unintelligence: How Computers Misunderstand the World. MIT Press, Boston, Mass.

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. Artificial Intelligence and Law, 25(3), 273–291. doi: 10.1007/s10506-017-9214-9

Cadwalladr, C. (2018, December 23). Our Cambridge Analytica scoop shocked the world. But the whole truth remains elusive. The Guardian.

Chamorro-Premuzic, T. (2015, September 24). How different are your online and offline personalities? The Guardian. Retrieved from https://www.theguardian.com/media-network/2015/sep/24/online-offline-personality-digital-identity

Cherng, H.-Y. S. (2017). The Color of LGB: Racial and Ethnic Variations in Conceptualizations of Sexual Minority Status. Population Review, 56(1). doi: 10.1353/prv.2017.0002

Chouldechova, A., & G'Sell, M. (2017, June 30). Fairer and more accurate, but for whom? Presented at the 2017 Workshop on Fairness, Accountability, and Transparency in Machine Learning (FAT/ML 2017), Halifax, Canada.

Chupapados Data https://chupadados.codingrights.org/en/they-are-stalking-you-to-calculate-your-score/

Citron, D. K. (2008a). Cyber Civil Rights. Boston University Law Review, 89, 61–125.

Citron, D. K. (2008b). Technological Due Process. Washington University Law Review, 85(6), 1249–1313.

Clifford, S., & Silver-Greenberg, J. (2013). Retailers Use Databases to Track Worker Thefts. The New York Times.

Cohen, Julie E. (2012). What privacy is for. Harvard Law Review, 126, 1904.

Cramer, Katherine J. (2017, Jun 19). The Great American Fallout: How Small Towns Came to Resent Cities. The Guardian.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10(1), 104–115. doi: 10.1287/orsc.10.1.104

Culnan, M. J., & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. MIS Quarterly, 33(4), 673–687.

Davis, Lisa Selin (2017, Apr 3) For 18 years, I thought she was stealing my identity. Until I found her . The UK Guardian https:// www.theguardian.com/us-news/2017/apr/03/identity-theft-racial-justice

Dawes, S. S. (1996). Interagency Information Sharing: Expected Benefits, Manageable Risks. Journal of Policy Analysis and Management, 15(3), 377–394.

Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. Government Information Quarterly, 27(4), 377–383. doi: 10.1016/j.giq.2010.07.001

Desmond, Ruth. (2010). Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act. University of San Francisco Law Review, 44(4), 6.

Dhar, V. (2013). Data Science and Prediction. Communications of the ACM, 56(12), 64–73. doi: 10.1145/2500499

Eaglin, J. M. (2017). Constructing Recidivism Risk. Emory Law Journal, 67(1), 59–122.

Edwards, P. N., Mayernik, M. S., Batcheller, A. L., Bowker, G. C., & Borgman, C. L. (2011). Science friction: Data, metadata, and collaboration. Social Studies of Science, 41(5), 667–690. doi: 10.1177/0306312711413314

Egan, P. (2017, July 31). Data glitch was apparent factor in false fraud charges against jobless claimants. Retrieved September 7, 2019, from Detroit Free Press website: https://www.freep.com/story/news/local/michigan/2017/07/30/fraud-charges-unemployment-jobless-claimants/516332001/

Eubanks, V. (2018, January 15). A Child Abuse Prediction Model Fails Poor Families. Wired. Retrieved from https://www.wired.com/story/excerpt-from-automating-inequality/

Fedorowicz, J., Gogan, J. L., & Culnan, M. J. (2010). Barriers to Interorganizational Information Sharing in e-Government: A Stakeholder Analysis. The Information Society, 26(5), 315–329. doi: 10.1080/01972243.2010.511556

Fergus, D. and Boyd, T. (2014) Banking without borders. Kalfou, 1(2), 7-28. doi: 10.15367/kf.v1i2.30

Fitts, P. M. (1954). The information capacity of the human motor system in controlling the amplitude of movement. Journal of Experimental Psychology, 47(6), 381.

Floridi, L. (2009). Network Ethics: Information and Business Ethics in a Networked Society. Journal of Business Ethics, 90(Supplement 4), 649–659. doi: doi:10.1007/s10551-010-0598-7

Freelon, D., McIlwain, C., & Clark, M. (2018). Quantifying the power and consequences of social media protest. New Media & Society, 20(3), 990–1011. doi: 10.1177/1461444816676646

Gardner, H. (1983). The Idea of Multiple Intelligences. In Frames of Mind: The theory of multiple intelligences (pp. 3–11). New York: Basic Books Inc.

Garfield, E. (1955). Citation Indexes for Science: A New Dimension in Documentation through Association of Ideas. Science, 122(3159), 108–111. doi: 10.1126/science.122.3159.108

Garriga, E., & Melé, D. (2012). Corporate Social Responsibility Theories: Mapping the Territory. In Citation Classics from the Journal of Business Ethics (pp. 69–96). Dordrecht, NETHERLANDS: Springer.

Gelman, A., & Loken, E. (2014). Ethics and Statistics: The AAA Tranche of Subprime Science. CHANCE, 27(1), 51–56.

Gelman, A., & Palko, M. (2013). Ethics and Statistics: The War on Data. CHANCE, 26(1), 57–60.

Gioia, D. A. (1992). Pinto Fires and Personal Ethics: A Script Analysis of Missed Opportunities. Journal of Business Ethics, 11(5/6), 379–389.

Giunchiglia, F., Villafiorita, A., & Walsh, T. (1997). Theories of Abstraction. Artificial Intelligence, 57.

Gladwell, M. (2008). Outliers: The Story of Success.

Gladwell, M. (2011). The Order of Things. New Yorker, 87(1), 68–75. Retrieved from a9h.

Gorman, M. E., Winkler, P. W., & American Library Association. (1998). Anglo-American cataloguing rules (Vol. 2nd). Ottawa. Chicago: Canadian Library Association ; American Library Association.

Gray, J., & Davies, T. G. (2015, May 27). Fighting Phantom Firms in the UK: From Opening Up Datasets to Reshaping Data Infrastructures? Presented at the Open Data Research Symposium at the 3rd International Open Government Data Conference, Ottawa. Retrieved from http://papers.ssrn.com/abstract=2610937

Griffith, J. C. (2001). Congress' legislative information systems: THOMAS and the LIS. Government Information Quarterly, 18(1), 43–60. doi: 10.1016/S0740-624X(00)00066-6

Hacking, I. (2007). Kinds of People: Moving Targets. In P. J. Marshall (Ed.), Proceedings of the British Academy, Volume 151, 2006 Lectures (pp. 285–318). Oxford University Press / British Academy.

Halevy, A., Norvig, P., & Pereira, F. (2009). The Unreasonable Effectiveness of Data. IEEE Intelligent Systems, 24(2), 8–12. doi: 10.1109/MIS.2009.36

Hedenus, A., & Backman, C. (2017). Explaining the Data Double: Confessions and Self-Examinations in Job Recruitments. Surveillance & Society, 15(5), 640–654. doi: 10.24908/ss.v15i5.6380

Herkenhoff, K., Phillips, G., & Cohen-Cole, E. (2016). The impact of consumer credit access on employment, earnings and entrepreneurship (No. w22846). National Bureau of Economic Research.

Hess, C., & Ostrom, E. (2011). Understanding knowledge as a commons: From theory to practice. Retrieved from http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=12504

Ho, K. (2009) Leveraging Dominance and Crises through the Global. In Liquidated: An Ethnography on Wall St. doi: 10.1215/9780822391371-008

Ho, K. (2018) Markets, myths, and misrecognitions: Economic populism in the age of financialization and hyperinequality. Economic Anthropology 5(1), 148-150

Hoofnagle, C. J. (2009). Internalizing Identity Theft. UCLA Journal of Law and Technology, 13(2), 38.

Hu, M. (2017). Algorithmic Jim Crow. Fordham Law Review, 86(2), 633-696.

Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. Government Information Quarterly, 27(4), 371–376

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. Government Information Quarterly, 33(3), 371–377. doi: 10.1016/j.giq.2016.08.011

Jonas, J., and J. Harper. 2006. Effective counterterrorism and the limited role of predictive data mining. Policy Analysis. Washington D.C.: Cato Institute, December 11.

Kath, R. (2018, Apr 11) I-Team: Mistaken Identity Causes Bureaucratic Nightmares For Drivers. CBS News Boston https:// boston.cbslocal.com/2018/04/11/wbz-tv-i-team-drivers-bureaucratic-nightmares-mistaken-identity-federal- database/

Katz, D. M., & Bommarito, M. J. (2014). Measuring the Complexity of the Law: The United States Code. Artificial Intelligence and Law, 22(4), 337–374. doi: 10.1007/s10506-014-9160-8

Knaub, Kelly (2014, Aug 4) "LexisNexis, Retail Workers Get Nod For $2.38M Settlement," Law 360. http://www.law360.com/articles/563583/lexisnexis-retail-workers-get-nod-for-2-38m-settlement.

Krajewski, M. (2011). Paper machines: About cards & catalogs, 1548-1929.

Krogstad, J. M. (2014, March 24). Census Bureau explores new Middle East/North Africa ethnic category. http://www.pewresearch.org/fact-tank/2014/03/24/census-bureau-explores-new-middle-eastnorth-africa-ethnic-category/

Lampland, M., & Star, S. L. (2009). Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life. Retrieved from

Levy, K & Barocas, S ."DESIGNING AGAINST DISCRIMINATION" https:// scholarship.law.berkeley.edu/btlj/vol32/iss3/5/ doi.org/10.15779/Z38BV79V7K

Liedtke, Michael (2011, Dec 16) How A Clerical Error Put A Woman On The Streets. Business Insider / AP . . https:// www.businessinsider.com/mistaken-identity-put-this-woman-on-the-streets-2011-12

Majchrzak, A., & Markus, M. L. (2013). Methods for policy research: Taking socially responsible action.

Margetts, H., 6, P., & Hood, C. (2010). Paradoxes of modernization: Unintended consequences of public policy reform.

Markham, A. N. (2018). Afterword: Ethics as Impact—Moving From Error-Avoidance and Concept-Driven Models to a Future-Oriented Approach. Social Media + Society, 4(3), 2056305118784504. doi: 10.1177/2056305118784504

Markus, M. L. (2016). Obstacles on the Road to Corporate Data Responsibility. In C. R. Sugimoto, H. R. Ekbia, & M. Mattioli (Eds.), Big data is not a monolith (p. 143). MIT Press.

Markus, M. L., & Bui, Q. "Neo." (2012). Going Concerns: The Governance of Interorganizational Coordination Hubs. Journal of Management Information Systems, 28(4), 163–198.

Markus, M. L., Steinfield, C. W., & Wigand, R. T. (2006). Industry-Wide Information Systems Standardization as Collective Action: The Case of the U.S. Residential Mortgage Industry. MIS Quarterly, 30, 439–465.

Martin, A. (2010). As a hiring filter, credit checks draw questions. New York Times, April 10. https://www.nytimes.com/2010/04/10/business/10credit.html

Martin, P. W. (1991). How New Information Technologies Will Change the Way Law Professors Do and Distribute Scholarship. Law. Libr. J., 83, 633.

Marwick, A. E., & boyd, danah. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114–133.

McArthur, T. (1986). Worlds of reference: Lexicography, learning, and language from the clay tablet to the computer. Retrieved from http://www.loc.gov/catdir/description/cam031/85007860.html

McClure, C. R., Hernon, P., & Relyea, H. C. (1989). United States government information policies: Views and perspectives. Norwood, N.J.: Ablex.

McKenzie, Patrick (2010) "Falsehoods Programmers Believe About Names"

Meyer, Eugene L. (1997, Dec 15) "Md. Woman Caught in Wrong Net; Data Errors Link Her to Probes, Cost 3 Jobs," Washington Post C1.

Neff, G. (2012). Venture labor: Work and the burden of risk in innovative industries. Cambridge Mass.: MIT Press.

Neff, G., Tanweer, A., Fiore-Gartland, B., & Osburn, L. (2017). Critique and Contribute: A Practice-Based Framework for Improving Critical Data Studies and Data Science. Big Data, 5(2), 85–97. doi: 10.1089/big.2016.0050

Ostrom, E. (1986). An agenda for the study of institutions. Public Choice, 48(1), 3–25.

Pager, D., & Shepherd, H. (2008). The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets. Annual Review of Sociology, 34(1), 181–209. doi: 10.1146/annurev.soc.33.040406.131740

Pasquale, F. A., & Citron, D. K. (2014). Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society. Washington Law Review, 89, 1413–1424.

Peeters, R., & Schuilenburg, M. (2018). Machine justice: Governing security through the bureaucracy of algorithms. Information Polity: The International Journal of Government & Democracy in the Information Age, 23(3), 267–280. doi: 10.3233/IP-180074

Pewen, W. F. (2012, August 2). Protecting Our Civil Rights in the Era of Digital Health. The Atlantic. Retrieved from http://www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343/

Picchi, Aimee (2019) Consumer Reports: How to Stop Harassment for Debts You Don't Owe. New Economy Project Blog. neweconomynyc.org

Porter, Eduardo. (2018). The hard truths of trying to "save" the rural economy. New York Times.

Powles, J. (2017, December 21). New York City's Bold, Flawed Attempt to Make Algorithms Accountable. The New Yorker.

Raymond, A. H., Young, E. A. S., & Shackelford, S. J. (2018). Building a Better HAL 9000: Algorithms, the Market, and the Need to Prevent the Engraining of Bias. 42.

Robinson, D. G., Yu, H., Zeller, W., & Felten, E. W. (2008). Government Data and the Invisible Hand. Yale Journal of Law and Technology, 11(Spring). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1138083#PaperDownload

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, 10(1), 3069. doi: 10.1038/s41467-019-10933-3

Rossi, F. (2019). Building Trust in Artificial Intelligence. Journal of International Affairs, 72(1), 127–134.

Ruppert, E. (2009). Becoming Peoples. Journal of Cultural Economy, 2(1–2), 11–31. doi: 10.1080/17530350903063909

Ruppert, E. (2011). Population Objects: Interpassive Subjects. Sociology, 45(2), 218–233. doi: 10.1177/0038038510394027

Schillo, R. S., & Robinson, R. M. (2017). Inclusive Innovation in Developed Countries: The Who, What, Why, and How. Technology Innovation Management Review, 7(7), 34-46.

Schlesinger, A., O'Hara, K. P., & Taylor, A. S. (2018). Let's Talk About Race: Identity, Chatbots, and AI. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 1–14. https://doi.org/10.1145/3173574.3173889

Singer, N. (2018, September 22). Just Don't Call It Privacy. The New York Times. Retrieved from https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html

Smith, H. J., & Hasnas, J. (1999). Ethics and Information Systems: The Corporate Domain. MIS Quarterly, 23(1), 109–127. doi: 10.2307/249412

Solove, D. (2004). The digital person: Technology and privacy in the Information Age. New York: New York University Press.

Solove, D. J. (2001). Access and Aggregation: Public Records, Privacy and the Constitution. Minnesota Law

Review, 86(6), 1137.

Spence, M. (2002). Signaling in Retrospect and the Informational Structure of Markets. The American Economic Review, 92(3), 434–459.

Star, S. L., & Bowker, G. C. (2007). Enacting silence: Residual categories as a challenge for ethics, information systems, and communication. Ethics and Information Technology, 9(4), 273–280. doi: 10.1007/s10676-007-9141-7

Starr, P. (1992). Social Categories and Claims in the Liberal State. Social Research, 59(2), 263–295.

Stendahl, M., Peter, Walter, B., Carter, & OECD,. (2005). Oslo Manual—Guidelines for Collecting and Interpreting Innovation Data (3rd edition). Organisation for Economic Cooperation and Development, OECD.

Stiglitz, J. E. (1999). On liberty, the right to know, and public discourse: The role of transparency in public life. Oxford Amnesty Lecture. Retrieved from http://www.internationalbudget.org/wp-content/uploads/On-Liberty-the-Right-to-Know-and-Public-Discourse-The-Role-of-Transparency-in-Public-Life.pdf

Taylor, A. G., & Joudrey, D. N. (2009). The organization of information (3rd ed.).

Tempini, N. (2017). Till data do us part: Understanding data-based value creation in data-intensive infrastructures. Information and Organization, 27(4), 191–210. doi: 10.1016/j.infoandorg.2017.08.001

Ticona, Julia, Alexandra Mateescu, and Alex Rosenblat. 2018. Beyond Disruption:How Tech Shapes Labor Across Domestic Work & Ridehailing. New York: Data & Society. https://datasociety.net /output/beyond-disruption/

Tress, W. (2009). Lost Laws: What We Can't Find in the United States Code. Golden Gate University Law Review, 40(2), 129–164.

Ungbha Korn Jenny (2018). Equitable Cities Instead of Smart Cities: Race and Racism Within The Race For Smart Cities. Journal of Civic Media, 1(1), 34-45.

Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. The New York Times. Retrieved from https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Walsh, T. (1992). A theory of abstraction. Artificial Intelligence, 57(2–3), 323–389. doi: 10.1016/0004-3702(92)90021-O

Washington, A. (2019). Who Do You Think We Are? The Data Publics in Digital Government Policy. Proceedings of the 52nd Hawaii International Conference on System Sciences. Presented at the Hawaii International Conference on System Sciences, Maui, Hawaii.

Washington, A. L., & Griffith, J. C. (2007). Legislative Information Websites: Designing Beyond Transparency. In A. R. Lodder & L. Mommers (Eds.), Legal Knowledge and Information Systems JURIX 2007 The Twentieth Annual Conference (p. 192).

Washington, A. L., & Morar, D. (2017). Open Government Data and File Formats: Constraints on Collaboration. Proceedings of the 18th Annual International Conference on Digital Government Research, 155–159. doi: 10.1145/3085228.3085232

Washington, A. L., Willis, D., & Tauberer, J. (2012). Do-it-yourself Transparency: Emerging Methods of Congressional Information Dissemination. Proceedings of the 13th Annual International Conference on Digital Government Research, 260–261. doi: 10.1145/2307729.2307774

Weisstein, E. W. (2019, September 6). Birthday Problem. Retrieved September 1, 2019, from MathWorld Wolfram website: http://mathworld.wolfram.com/BirthdayProblem.html

Whittlestone, J., Nyrup, R., Alexandrova, A., & Cave, S. (2019). The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions. Proceedings of the 2nd AAAI/ACM Conference on AI, Ethics, and Society, 7.

Winter, S. J., Chudoba, K. M., & Gutek, B. A. (1997). Misplaced resources? Factors associated with computer literacy among end-users. Information & Management, 32(1), 29–42. doi: 10.1016/S0378-7206(96)01086-5

Yampolskiy, R. V. (2016). Taxonomy of Pathways to Dangerous AI. 2016 AI, Ethics, and Society Workshop at the Thirtieth AAAI Conference on Artificial Intelligence, Pages 143-148. Phoenix, Arizona, USA: AAAI Press, Palo Alto, CA.

Acknowledgements

Congressional testimony has one voice but many hands.

This would not have happened without the extraordinary voluntary support from my former doctoral research assistants: David C. Morar and Rachel S. Kuo. Someone should hire them soon because they are both outstanding talent. Molly Nystrom and Kiran Samuels identified the cases used in the testimony. It was delightful to reconnect to old friends from WFNIA / BGI / BlackRock through Janice Deringer. I am grateful for my current colleagues in the Applied Statistics program and the A3SR 'Data for Social Impact' students especially the Spring 2019 Ethics of Data Science class. I appreciated the support from my fellow fellows at D&S, as well as the #unsettle event, The Hellenic Express, Team Rosario, and S.C.A.N. The Critical Race + Digital Scholars cooperative helped me identify additional citations for the bibliography.

All mistakes are my own, but I would like to acknowledge the expertise of the following people who contributed to this effort: David Morar, Rachel Kuo, Kiran Samuels, The Qlab, Jessica Spencer, Molly Nystrom, Chloe Marten, Shannon Kay, Alexandra Mateescu, David G. Robinson, Rashida Richardson, Meredith Broussard, Danielle Citron, Janice Deringer, Jenn Holmes, James R. Brandon, KO.T.N. , Mr. & Mrs. Merlin, Thing1 and Thing2.

anne.washington@nyu.edu
FSCTestimony Washington SUBMIT2.docx

House Committee on Financial Services

The Future of Identity in Financial Services: Threats, Challenges, and Opportunities

September 23, 2019
Questions for the Record from U.S. Representative Ted Budd (R-NC.)

Witness: Ms. **Valerie Abend**, Managing Director, Accenture and Mr. **Jeremy Grant**, Coordinator, Better Identity Coalition

RESPONSE FROM: Valerie Abend, Managing Director, Accenture

-Ms. Abend, it sounds like the use of AI will be a critical part of ensuring security in digital identity- should we be concerned that this kind of advanced technology could be unaffordable or otherwise unavailable to smaller/community financial institutions?

As we look to the future it is important that AI-enabled security solutions, including those that support digital identity services are available and affordable to all institutions in a manner that support their specific business models. To do this, community institutions will likely need to work through consortiums, such as trade associations or other groups to learn about and avail themselves of security innovations that leverage AI.

-Nearly 60 million Americans have been affected by identity theft, according to an online survey by The Harris Poll. In 2018, that was 14.4 million Americans alone, as found by Javelin Strategy & Research. It's estimated they had over $16.8 billion stolen from them. Those are staggering figures to say the least. We're talking about millions of Americans who are having their lives turned upside down, financially, professionally, and personally, due to someone using their identity illegally. As more commercial and government entities suffer data breaches, there's never been a stronger need for consumers to look at identity protection. Mr. Grant and Ms. Abend, can you detail the identity protection services that are available to consumers now? Explain dark web monitoring and stolen fund reimbursement and some of these other things that are on the market. Additionally, is this kind of coverage a good investment for the consumer, considering the level of data breaches we see nowadays? Furthermore, are there opportunities for businesses to adopt these technologies at a larger scale?

As your question indicates, the number and breadth of data breaches to date is staggering. Most adult Americans have likely had some of their personal information compromised and made

available to malicious actors on the dark web. Signing up for identity protection services is just one of many steps consumers take when their data is breached. In addition, we believe advances in digital identity, some of which we discussed at the hearing, present the most promise for addressing consumers' and businesses' concerns. Financial institutions are implementing an array of products and services - such as biometrics, behavioral analytics, and multi-factor authentication, supported by threat intelligence and fraud monitoring - to help enterprises make real-time, risk-based decisions about whether to authenticate a customer, approve a transaction, and what limits to set around a transaction.

The threat intelligence that support some of these products and services incorporate monitoring of dark web forums where cyber adversaries share their tactics and techniques, look for additional capabilities to compliment their attacks, and/or sell their capabilities. Often these forums are where stolen identities are bought, sold and traded.
While the financial services and the telecommunications industries are leaders in this space and innovations are happening every day, much can be done to help more businesses adopt these technologies, and to scale them across the economy. A step in the right direction would be for believes Congress to pass a national privacy law that provides consumers with rights for transparency, control, access, correction and deletion with respect to their data. A robust and secure digital identity ecosystem depends on consumer trust—which can only be established with a shared national approach to consumer privacy. Other recommendations that would help enable the scaling of the digital identity ecosystem can be found in the Business Roundtable report, *Building Trusted and Resilient Digital Identity*.[1] Those recommendations include:

- Reducing our dependency on passwords in favor of more intuitive and secure authentication;
- Increasing customer awareness, digital literacy, and confidence;
- Improving multiple sector participation in a digital identity ecosystem that enables trust in each other's attestations of identity—so users can continue to transact business even when an individual organization's digital identity system has been breached; and
- Ensuring transparency and choice to customers, empowering them with customer rights. A national privacy law would go a long way to achieving this goal.

[1] Business Roundtable, *Building Trusted and Resilient Digital Identity* July 2019
https://s3.amazonaws.com/brt.org/BRT-DigitalIDReportJuly2019.pdf

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

JEROME H. POWELL
CHAIRMAN

July 9, 2019

The Honorable French Hill
House of Representatives
Washington, D.C. 20515

Dear Congressman:

Thank you for your letter dated June 18, 2019, regarding the prevalence of wire fraud in the United States. The Federal Reserve Board (Board) has been actively engaged in efforts to respond to the increasing threat of large-value payments fraud. As you noted in your letter, fraud in wire payments can include large-value payments in connection with real estate transactions.

To combat this issue you suggested requiring "payee matching" for wire transfers, where the beneficiary's bank would check to see that the name on the payment order matches the name on the account to be credited. However, this approach presents legal and operational challenges. U.S. large-value funds transfer systems are generally governed by a uniform state law[1] that governs funds transfers, which the Board incorporated into its regulation[2] that governs the Fedwire Funds service. For example, when a beneficiary's bank receives a payment order that identifies a customer by both a name and an account number, the bank is permitted to rely on the number as the proper identification. To require otherwise would create significant operational obstacles to processing the hundreds of thousands of wire payments that occur each day. The vast majority of wires are processed by automated means using machines capable of reading standard payment order formats that identify the beneficiary's account.

Requiring banks to obtain appropriate identification from customers before opening an account is one way to combat this type of fraud. The federal banking agencies' Customer Identification Program (CIP) joint rule requires banks to obtain sufficient information from their customers in order to form a reasonable belief regarding the identity of each customer.[3] The CIP rule requires verification procedures designed to ensure that financial institutions know their customers and to assist in identifying potential bad actors.

---

[1] See Uniform Commercial Code, Article 4A.
[2] See Regulation J, 12 C.F.R. Part 210, https://www.federalreserve.gov/supervisionreg/regjcg.htm.
[3] See 31 C.F.R. § 1020.220.

Additionally, the Federal Reserve has been engaged in efforts to reduce fraud more broadly in wire payments. We have worked collaboratively with other central banks as part of the efforts by the Bank for International Settlement's Committee on Payments and Market Infrastructures (CPMI) to reduce the risk of wholesale payments fraud related to endpoint security with the broader objective of supporting financial stability.[4] As a result, the Federal Reserve and CPMI member central banks have developed a strategy to encourage and focus industry efforts to reduce the risk of fraud related to endpoint security.[5] The strategy includes key elements that payment system and messaging operators should consider as part of their efforts to mitigate payments fraud and it encourages a holistic approach to address all areas relevant to preventing, detecting, responding to and communicating about fraud.

We appreciate your concerns and the information you provided on this important issue.

Sincerely,

Jerome H. Powell

[4] See https://www.federalreserve.gov/newsevents/pressreleases/other20180508a.htm.
[5] See https://www.bis.org/cpmi/publ/d178.pdf.

Congress of the United States
Washington, DC 20515

June 7, 2019

The Honorable Jerome Powell
Chairman
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Dear Chairman Powell:

It has come to our attention that wire fraud through business e-mail compromise (BEC) and e-mail account compromise (EAC) is a rapidly growing problem in the United States. This fraud poses tremendous risks to our constituents, especially homebuyers, and their confidence in our payment system's ability to safely transfer large amounts of money as part of the homebuying process.

On October 16, 2018 the Federal Reserve published a report, "Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study," which does not appear to mention the issue of wire fraud. To our knowledge, the most substantive effort by the Federal Reserve to address this issue has been the announcement last year, by its Secure Payments Task Force to create and publish "recommended fraud definitions." Despite this initiative, we are concerned that Federal Reserve policies on wire fraud may not convey the urgency of the problem.

The United Kingdom has taken a more proactive role in preventing wire fraud, especially involving real estate transactions. In July of this year, Pay.UK, the United Kingdom's national payments system service provider, will oversee the nationwide implementation of a new "confirmation of payee" mechanism to address the growing issue of wire fraud in their jurisdiction.

On July 12, 2018 the Federal Bureau of Investigation (FBI) released a public service announcement titled, "Business E-mail Compromise the 12 Billion Dollar Scam." In this announcement, the FBI reported that between 2015 and 2017 there was an 1100% increase in the number of real estate related e-mail compromise scams taking place. Of those scams, there was a nearly 2200% increase in the amount of money lost.[1] The FBI has also reported that in fiscal year 2017 alone $969 million was "diverted or attempted to be diverted" from real estate purchases

[1] "Business E-mail Compromise the 12 Billion Dollar Scam," Federal Bureau of Investigation, Public Service Announcement, July 12, 2018. https://www.ic3.gov/media/2018/180712.aspx

and sent to "criminally controlled" accounts.[2] This was a significant increase from $19 million in 2016. The Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) have also taken steps to raise awareness of this issue. In early 2016 and again in 2017, the FTC issued warnings to consumers on the dangers of wire fraud, urging them to "Protect Your Mortgage Closing from Scammers."[3] On July 7, 2017 the CFPB issued its own warning, instructing homebuyers to "Watch out for Mortgage Closing Scams."[4]

Given the scope of this issue, and the progress being made in the United Kingdom to address it, we are interested in determining whether the United States can implement similar protocols to limit fraud – effectively verifying the payee's name on a wire payment. As you are aware, verifying that a wire payment is made to the intended recipient is not required under current regulations or used by all financial institutions.

We would appreciate your response to the following questions:

1. How is the Federal Reserve addressing criminal exploitation of weaknesses in the U.S. wire system to trick unsuspecting consumers to send their money to the wrong financial account?

2. Which federal agencies has the Federal Reserve coordinated with on addressing the issue of wire fraud?

3. Has the Federal Reserve investigated putting in place payee matching requirements when a wire transfer is initiated?

4. Do you believe the Federal Reserve has sufficient authority to institute these protections for the U.S. wire system, or at least for wire transfers that run through the Federal Reserve's Fed Wire system? If not, what authorities would the Federal Reserve need to institute these protections?

5. Has the Federal Reserve determined if the current wire transfer system's technology will allow for payee verification? If not, why was payee verification not included in the Federal Reserve's evaluation of the future of the payments system?

Respectfully,

---

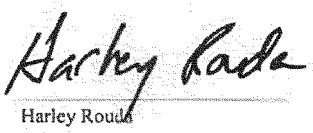
[2] "FBI: Hackers scam homebuyers out of millions — and it's getting worse," the Chicago Tribune, October 31, 2017. https://www.chicagotribune.com/g00/classified/realestate/ct-re-1105-kenneth-harney-20171030-story.html?i10c.ua=1&i10c.encReferrer=&i10c.dv=22

[3] "Protect your mortgage closing from scammers," Federal Trade Commission, Consumer Information, June 27, 2017. https://www.consumer.ftc.gov/blog/2017/06/protect-your-mortgage-closing-scammers

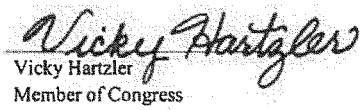
[4] "Buying a home? Watch out for mortgage closing scams," Consumer Financial Protection Bureau, June 7, 2017. https://www.consumerfinance.gov/about-us/blog/buying-home-watch-out-mortgage-closing-scams/

Brad Sherman
Member of Congress

David Kustoff
Member of Congress



Harley Rouda
Member of Congress

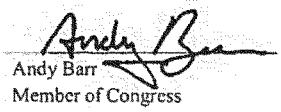


Vicky Hartzler
Member of Congress

Bill Foster
Member of Congress

Sean Duffy
Member of Congress

Stephen Lynch
Member of Congress

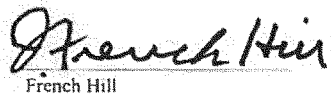


Andy Barr
Member of Congress

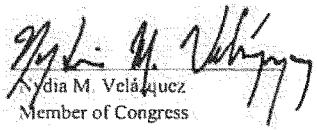
Vicente Gonzalez
Member of Congress

Ted Budd
Member of Congress

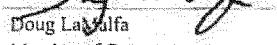
Carolyn Maloney
Member of Congress



French Hill
Member of Congress



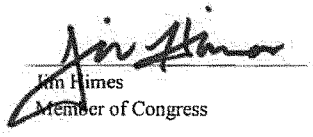
Nydia M. Velázquez
Member of Congress



Doug LaMalfa
Member of Congress

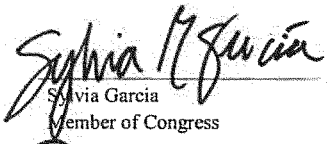
Katie Porter
Member of Congress

Scott Perry
Member of Congress



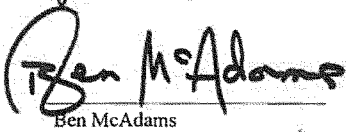
Kim Himes
Member of Congress

John Rose
Member of Congress

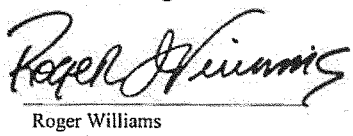


Sylvia Garcia
Member of Congress

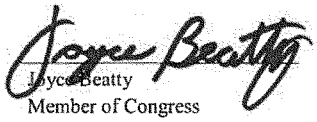
Scott Tipton
Member of Congress



Ben McAdams
Member of Congress

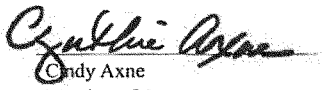


Roger Williams
Member of Congress

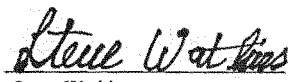


Joyce Beatty
Member of Congress

Lance Gooden
Member of Congress

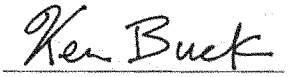


Cindy Axne
Member of Congress

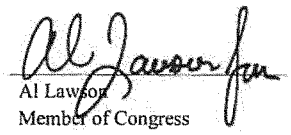


Steve Watkins
Member of Congress

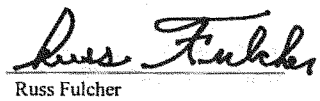
Tulsi Gabbard
Member of Congress



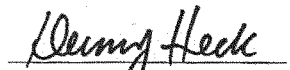
Ken Buck
Member of Congress



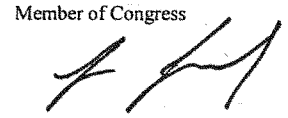
Al Lawson
Member of Congress



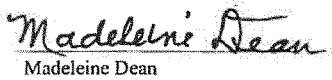
Russ Fulcher
Member of Congress



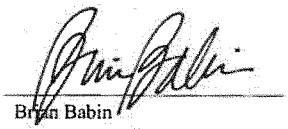
Denny Heck
Member of Congress



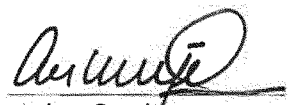
Lee Zeldin
Member of Congress



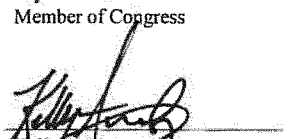
Madeleine Dean
Member of Congress



Brian Babin
Member of Congress



Anthony Gonzalez
Member of Congress



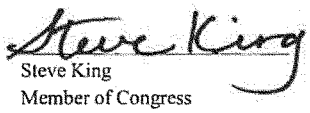
Kelly Armstrong
Member of Congress

Chris Collins
Member of Congress

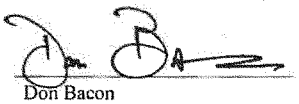
Ross Spano
Member of Congress

Guy Reschenthaler
Member of Congress

Bradley Byrne
Member of Congress

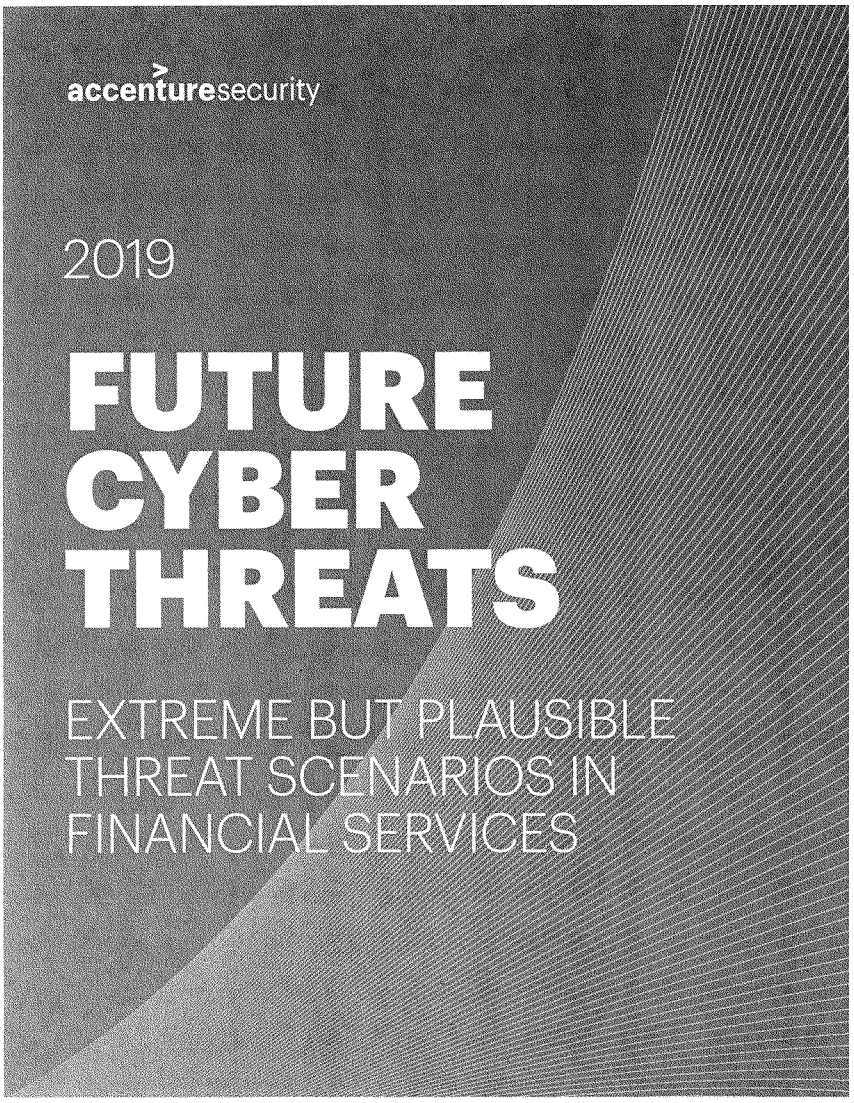


Steve King
Member of Congress



Don Bacon
Member of Congress

Christopher H. Smith
Member of Congress


accenturesecurity
2019
FUTURE CYBER THREATS
EXTREME BUT PLAUSIBLE THREAT SCENARIOS IN FINANCIAL SERVICES

CONTENTS

FOREWORD

While financial services organizations have always been a target for sophisticated criminals, cyber adversaries' capabilities are breaking new ground as they advance rapidly.

Accenture cyber threat intelligence research points to several key threats that, when combined, lay the groundwork for multistage, multiparty attacks that could result in a new wave of extreme cyberattack scenarios for financial services.

Our report describes each of these threats in their earlier and current forms and examines how they could evolve in the future. We explore:

- Credential and identity theft
- Data theft and manipulation
- Disruptive and destructive malware
- Emerging technologies: Blockchain, cryptocurrency and artificial intelligence
- Disinformation

By understanding the past and anticipating the future nature of threats, we aim to help financial services organizations to be better prepared. With a long history of collaboration, we are certain that now, more than ever, financial services organizations need to come together to address security and resilience challenges. As they maintain this spirit of collaboration and gain momentum—both within the sector and with governments around the world—they can secure the trust that is essential to the success and sustainability of the whole financial system.

Valerie Abend
Managing Director, Accenture Security

Howard Marshall
Principal Director, Accenture Security

EXECUTIVE SUMMARY

Trust is the fuel that drives the digital economy—it strengthens an organization's standing and leads to new revenue-generating opportunities.[1] It also underpins the stability of the global financial sector. As cyber threats facing financial institutions evolve over time, adversaries erode trust through well-orchestrated, multistaged cyberattacks. Financial services organizations must continually reassess the wide spectrum of cyber threats targeting the financial sector to sustain cyber resilience.

This report discusses five cyber threats affecting the financial sector today. We assess how these threats are evolving and how they could create major lasting impacts for both organizations and the global sector at large. The threats featured are:

Credential and identity theft: Breaches of enterprise credentials and consumer financial data continue to grow in frequency and scale. As the landscape changes, adversaries may use these large data sets in innovative ways, including simultaneous multiparty access and network abuse.

Data theft and manipulation: Financially, politically, and ideologically motivated adversaries have routinely stolen data from financial institutions. Well-resourced adversaries may evolve to incorporate data manipulation for financial gain, destabilizing financial systems and markets.

Destructive and disruptive malware: Adversaries are using ransomware attacks against the financial sector at exponential rates. Increased deployment has coincided with threat adversaries employing destructive malwares, pseudo-ransomwares and defense

1 Redefine your company based on the company you keep: Intelligent Enterprise Unleashed, Accenture Technology Vision. (2018). Accenture. https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

evasion techniques. Looking ahead, adversaries may deploy wiper malware to conceal their true intentions and stifle the incident response process during financially or politically motivated attacks.

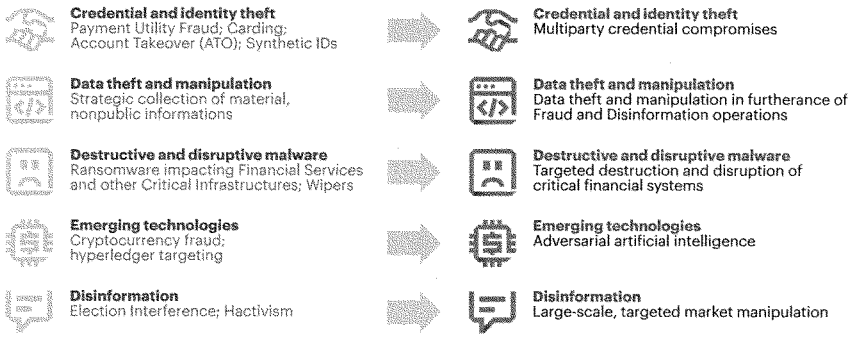
Emerging technologies: Financial services organizations continually explore applications of emerging technologies to deliver faster, more secure and customer-centric services. Increasingly, as financial services organizations leverage blockchain and artificial intelligence, threat adversaries may seek to exploit these emerging technologies as part of a new wave of malicious campaigns.

Disinformation: Disinformation has played a role in campaigns targeting financial institutions and markets since the birth of financial transactions. Combined with the other threats, disinformation may factor more prominently during highly targeted, multistage attacks.

As time goes on, these five threats are likely to overlap and intersect. In doing so, they can create the right conditions for new classes of cyberattacks—ones that simultaneously affect numerous organizations essential to financial services' most critical processes. A proactive cyber defense plan that incorporates multiparty attack simulations to test against these key threats could help financial institutions to be better prepared—not only to recognize cyber threats today, but also to defend them tomorrow.

EXECUTIVE SUMMARY

Financial Services
Current and future state of the threat



Source: Accenture iDefense Threat Intelligence

KEY THREATS

Based on our research of current and evolving cyber threats, the Accenture Security iDefense Threat Intelligence Services Team highlights the following five threats as key for organizations within the financial services sector:

- Credential and identity theft
- Data theft and manipulation
- Destructive and disruptive malware
- Emerging technologies: Blockchain, cryptocurrency and artificial intelligence
- Disinformation

CREDENTIAL AND IDENTITY THEFT

Credential and identity theft
Payment Utility Fraud; Carding; Account Takeover (ATO); Synthetic IDs

Credential and identity theft
Multiparty credential compromises

Social engineering remains the number one threat in breaching security defenses, regardless of the maturity and frequency of security awareness campaigns.[2] Increasingly, most organizations experience frequent and sophisticated phishing and other types of social engineering attacks[3] and, unfortunately, people continue to be the weak link in cybersecurity defense.[4]

The primary and most immediate impact of social engineering attacks is usually theft of customer, employee and other third-party credentials. These attacks often occur through account takeover (ATO) and synthetic identity fraud. In 2018, more than 43,000 breaches across all industries involved the use of customer credentials stolen from botnet-infected clients.[5] Such activity is a concern for financial institutions whose customers routinely repurpose usernames and passwords or where employee or third-party credentials are delegated for enterprise access.

Financially motivated adversaries take advantage of real-time payment networks by using ATO, wire fraud, check fraud, card fraud and a variety of other fraud types to steal funds.[6] The increase in consumer data available to fraudsters is driving fraud losses higher every year,[7]

---

2 Phishing as a Service: The Phishing Landscape. Accenture Security. (2018). https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-71/Accenture-Phishing-As-Service.pdf

3 Microsoft Security Intelligence Report Volume 24. (2019). https://clouddamcdnprodep.azureedge.net/gdc/gdcVAOQd7/original

4 Ninth Annual Cost of Cybercrime. (2019). https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

5 2018 Data Breach Investigations Report. Verizon. (2019). https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

6 Faster Payments, Faster Fraudsters. (2019, March 19). PYMNTS. https://www.pymnts.com/news/security-and-risk/2019/real-time-payments-faster-fraudsters-security/

7 Witt, P. (2019, February 28). The top frauds of 2018. Federal Trade Commission. https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018

propelling the shift from counterfeit cards to identity theft and synthetic identity fraud.[8] Cybercriminals use compromised credentials to quickly and widely establish user profiles. These credentials are easy to obtain firsthand or through criminal marketplaces, where they are sold in large volume at affordable rates. Synthetic identities have become a particular concern for financial institutions. This form of account theft is attractive to fraudsters because it enables them to obtain control of the account, cultivate high credit limits and bypass account alerts—all to facilitate high-dollar transactions with low risk of detection.[9] Fraudsters using synthetic identities are likely to continue to increase alongside traditional fraud.

Credential theft is a rapidly expanding threat for enterprise networks, incorporating e-mail addresses and login credentials; system credentials, such as certificates; and other forms of identification that third parties and employees use to authenticate themselves.[10] Unfortunately, the number of compromised credentials being used continues to rise.[11] In the United States, the Federal Financial Institutions Examination Council (FFIEC) published a statement warning financial institutions of the growing trend of credential theft.[12] It is a reminder that firms need to keep up-to-date with changing tactics, techniques and procedures (TTPs) used by the threat groups who compromise credentials.

Frequently, corporate credential theft is a targeted effort. Adversaries often conduct extensive reconnaissance of individuals at a target

8 Chasing ever-shifting payments fraud. (2018, September 6). Accenture. https://bankingblog.accenture.com/chasing-ever-shifting-payments-fraud?lang=en_US

9 Ibid

10 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

11 Goodin, D. Hard-to-detect credential-theft malware has infected 1,200 and is still going. (2019, February 20). Ars Technica. https://arstechnica.com/information-technology/2019/02/hard-to-detect-credential-theft-malware-has-infected-1200-and-is-still-going/

12 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

organization using social media and news channels. Once cybercriminals identify specific users with credentials to access critical data, the adversaries conduct phishing campaigns and create fake websites to gather an individual's credentials.

E-mail lures and fake sites used in corporate credential theft are often far more sophisticated than those used for consumer credential theft.[13] Following a successful compromise, adversaries use a variety of evasive measures so that they can keep using the credentials. Adversaries have been observed modifying permissions, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. Such actions include account activity designed to undermine security policies, such as performing iterative password updates to disrupt password duration policies and preserve the life of compromised credentials.[14]

In recent years, malicious adversaries have taken careful steps to obtain large sets of customer and corporate credentials for the purpose of credential abuse. In particular, privileged credential abuse—where adversaries gain access to critical processes and data within a financial institution or set of financial services organizations—is one of the most popular breach strategies used by organized crime and state-sponsored organizations.[15] In some cases, adversaries may not need to use malware to achieve their objectives when corporate credentials are effective enough on their own.

---

13 Shopen, K. is a Credential-Based Attack? (2017, February 16). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack

14 Account Manipulation. MITRE. https://attack.mitre.org/techniques/T1098/

15 Columbus, L. (2019, April 15). CIO's Guide To Stopping Privileged Access Abuse - Part I. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2019/04/15/cios-guide-to-stopping-privileged-access-abuse-part-i/

In an increasingly complex threat landscape, credential abuse across many enterprises at the same time is likely to be the cornerstone of sophisticated cyberattacks that impact financial services.

Compromised employee and third-party credentials may provide initial access to trusted internal systems, enabling adversaries to gain and use system administrator-level access to obtain confidential business information, modify and disrupt information systems, and destroy or corrupt data.

Stolen system credentials can also be used to gain access to internal systems and data to further distribute malware or impersonate the financial institution to facilitate fraud, such as accessing payment processing systems for automated clearing house transactions.[16] Repeating this process across a set of organizations can ensure adversaries maintain end-to-end visibility for their campaigns; it also affords threat adversaries operational resilience. In recent months, advanced adversaries have showcased their capacity to execute multiparty compromises effectively. In April 2018, five banks in Mexico were hacked, forcing them to connect to the domestic payment network, SPEI, via back-up methods.[17]

The applications for multiparty compromises are somewhat limitless when threat adversaries use credential abuse. Paired with ransomware, destructive malware, disinformation, high-dollar fraud or even defacement, multiparty compromises can compound the impact of an attack. The advent of advanced adversaries leveraging their access through compromised credentials to multiple, critical entities concurrently is likely to impact the financial sector's ability to collaborate—in turn, challenging its resilience.

16 Cyber Attacks Compromising Credentials. (2015). Federal Financial Institutions Examination Council. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

17 Davis, M. (2018, May 29). Mexico Foiled a $110 Million Bank Heist, Then Kept It a Secret. *Bloomberg*. https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

DATA THEFT AND MANIPULATION

Data theft and manipulation
Strategic collection of material, nonpublic informations

Data theft and manipulation
Data theft and manipulation in furtherance of Fraud and Disinformation operations

Data is the most critical asset for financial institutions. Maintaining the availability and integrity of data is vital to financial markets globally. Playing such a pivotal role, data is an ideal target for malicious adversaries, with information theft being the most expensive and fastest-rising consequence of cybercrime.[18]

Data breaches are an ever-present threat, with the number of United States data breach incidents hitting a record high in recent years. These breaches have involved the financial sector, including entities such as banks, credit unions, credit card companies, mortgage and loan brokers, investment firms and trust companies, payday lenders and pension funds and even financial authorities.[19] Data loss or data destruction are top-rated concerns for organizations.[20]

The ability to monetize material, nonpublic information through sales on criminal marketplaces or insider trading has attracted financially motivated adversaries to target financial institutions, technology service providers, central banks and relevant government agencies over the years. For example, adversaries stole documents related to a card processing system used by around 200 banks in the United States and Latin America, which could be potentially used for future attacks.[21]

18 Ninth Annual Cost of Cybercrime Study. (2019). Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

19 The Impact of Cybersecurity Incidents on Financial Institutions. (2018, February). Identity Theft Resource Center. https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

20 The State of Cybersecurity and Digital Trust 2016. (2016, June 27). Accenture. https://www.accenture.com/t20170510T000709__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Executive-Summary-June.pdf

21 Cuthbertson, A. (2017, December 12). Bank Robber Hackers Steal Millions of Dollars in Silent Heists Across U.S. and Russia. *Newsweek*. https://www.newsweek.com/bank-robber-hackers-steal-millions-dollars-silent-heists-745087

In 2016, adversaries extracted files from the United States Securities & Exchange Commission's EDGAR system to trade on nonpublic earnings results.[22] In 2017, adversaries targeted Poland's financial regulator, KNF, to exfiltrate data from several Polish banks. In what was labelled the most serious attack in Polish history at the time, the incident speaks to the diversity of ways threat adversaries can attempt data theft from critical financial entities.[23] This kind of activity is likely to continue as some institutions support their clients with initial public offerings (IPOs) and large mergers. Financial institutions are direct targets because of the sensitivity of the data they hold.[24] Both financially and politically motivated threat adversaries searching for competitive intelligence may continue to target firms as central repositories of valuable insider information.

As cyber threats progress, adversaries are likely to change as they shift their focus from data theft to strategic data manipulation. Unlike most data theft (where data is stolen because it is valuable) or extortive attacks (when data is imprisoned or destroyed until someone pays to release it), manipulation hacks are hard to detect: they occur when adversaries (or bots) change vital information, often below the threshold of attention.[25] Business is more data driven than ever, but inaccurate and manipulated information threatens to compromise the insights that companies rely on to plan, operate, and grow. Moreover, increasingly, financial services organizations are making use of autonomous, data-driven decision making. Left unchecked, adversaries could cause significant harm through the

---

22 SEC Brings Charges in EDGAR Hacking Case. (2019, January 15). Securities and Exchange Commission. https://www.sec.gov/news/press-release/2019-1

23 O'Neill, P. (2017, February 2). Hackers break into Polish banks through government regulator charged with bank security standards. CyberScoop. https://www.cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/

24 Cyber attacks on financial services sector rise fivefold in 2018. (2019, February 24). *Financial Times*. https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5

25 Cooper, B. (2017, November 20). The dangerous data hack that you won't even notice. University of California, Berkeley. https://news.berkeley.edu/berkeley_blog/the-dangerous-data-hack-that-you-wont-even-notice/

manipulation of these autonomous processes or via the large volumes of data that fuel this type of decision making.[26]

Both politically and financially motivated threat groups can benefit from manipulating data, a sentiment echoed by the United States Intelligence Community in recent years. In the future, firms are likely to see cyber operations that involve changing or manipulating electronic information, instead of simply deleting it or disrupting access to it. Should highly-resourced threat groups manipulate and disrupt access to key data sets, they could undermine the trust in the organization's systems and the organization itself. Decision making by senior government officials, corporate executives, investors, or others could be impaired if they cannot trust the information they are receiving.[27] Manipulating credit scores, bank account numbers, and also market data (including pricing and transaction volumes) is a natural evolution from yesterday's big data breaches, where the personal information on millions of consumers, healthcare patients and government workers could already be in use for such manipulation schemes.[28]

From an enterprise perspective, successful cyber threat operations, targeting the integrity of information, can overcome institutionalized checks and balances that are designed to prevent the manipulation of data; for example, market monitoring and clearing functions in the financial sector.[29] Evidenced by the large-scale data theft and financial crime over

---

26 Redefine your company based on the company you keep: Intelligent Enterprise Unleashed, Accenture Technology Vision 2018. (2018). Accenture. https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

27 Clapper, J. (2015, September 10). Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

28 Overfelt, M. (2016, March 9). The next big threat in hacking — data sabotage. CNBC. https://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html

29 Clapper, J. (2015, September 10). Statement for the Record, Worldwide Cyber Threats, House Permanent Select Committee on Intelligence. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

the past decade, both financially and politically motivated groups have positioned themselves as adversaries capable of penetrating the defenses of institutions of all sizes and may set their sights on data manipulation.

Critical pieces of intellectual property for financial organizations, such as algorithmic trading code, may play a central role in advancing the threat landscape for data. The globalization of asset trading, the emergence of ultrafast information technology and interconnected communications has made it impossible for humans to efficiently participate in a routine, low-level decision-making process.

Today, most trading decisions in equities and electronic futures contracts are made by algorithms: they define where to trade, at what price, and what quantity.[30] Malicious insiders at financial institutions have a storied history of stealing this trading algorithm code, including the use of credential stealers and malware designed to capture encryption keys for trading models.[31] This tendency is likely to evolve to include the alteration of these algorithms. Influencing trading algorithms to behave abnormally or ineffectively in small increments may be difficult for organizations to identify. Eventually, these changes could begin to accumulate, causing algorithms to become unstable, leading to extremely diverse outcomes including catastrophic failures.[32]

Financial services organizations should work to combat the manipulation of data by employing countermeasures aimed at early detection of alteration—provenance, threat modeling and alerting. By verifying the

30 Bacoyannis, V., et al. (2018, November 30). Idiosyncrasies and challenges of data driven learning in electronic trading. https://arxiv.org/pdf/1811.09549.pdf

31 Computer Engineer Arrested For Theft Of Proprietary Trading Code From His Employer. (2017, April 7). U.S. Attorney's Office Southern District of New York. https://www.justice.gov/usao-sdny/pr/computer-engineer-arrested-theft-proprietary-trading-code-his-employer

32 Know your Threat: AI is the New Attack Surface. (2019). Accenture. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

history of data from its origin throughout its life cycle, firms can certify and recertify the authenticity of their data. Assessing a firm's enterprise data landscape for inaccurate data and subsequently quantifying the trust within that data could enable security teams to forecast targeting through plausible, but extreme, threat models for cyberattacks.

In the future, firms are likely to see cyber operations that involve changing or manipulating electronic information instead of simply deleting it or disrupting access to it.

DESTRUCTIVE AND DISRUPTIVE MALWARE

Destructive and disruptive malware
Ransomware impacting Financial Services and other Critical Infrastructures; Wipers

Destructive and disruptive malware
Targeted destruction and disruption of critical financial systems

The cost of business disruption—including diminished employee productivity and business process failures that happen after a cyberattack—continues to rise at a steady rate. The financial consequences of ransomware alone have increased 21 percent in the last year.[33] Ransomware is overtaking banking trojans in financially motivated malware attacks, a trend that is predicted to continue in the near future.[34] The risk of large-scale disruption in financial services may rise as threat adversaries develop variants of extortive malware.

In recent years, financial services organizations have been among the most targeted organizations from adversaries conducting ransomware campaigns.[35] One insurance company that provides protection against ransomware attacks has observed that, of all the attacks they noted, 20 percent targeted financial institutions. That said, successful infections have been significantly lower and have primarily affected smaller banks and credit unions—some more than once.[36] Organized cybercriminal groups continue to target firms they deem likely to pay the ransom. In some ways, this explains the lack of successful infections reported by large financial institutions, often perceived by adversaries to have more mature cybersecurity postures.

---

33 Ninth Annual Cost of Cybercrime Study. (2019). Accenture. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

34 2018 Internet Organised Crime Threat Assessment (IOCTA). (2019). Europol. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

35 Crosman, P. (2016, November 3). Ransomware: Should Banks Prepare to Pay or Be Ready to Refuse? *American Banker*. https://www.americanbanker.com/news/ransomware-should-banks-prepare-to-pay-or-be-ready-to-refuse

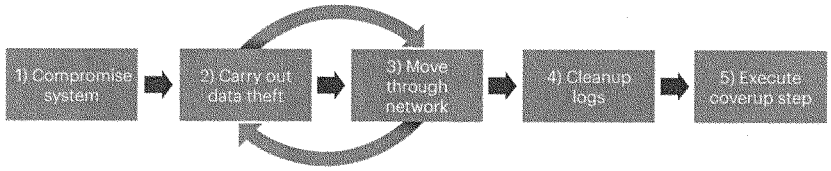
36 Yurcan, B. (2018, June 15). Ransomware is taking a toll on banks. Here's how they're fighting back. *American Banker*. https://www.americanbanker.com/news/ransomware-is-taking-a-toll-on-banks-heres-how-theyre-fighting-back

DESTRUCTIVE AND DISRUPTIVE MALWARE

The same threat groups operating ransomware also operate banking trojans that hit banks' consumer and commercial clients with wire fraud and automated clearing house fraud.[37] To help reduce the effectiveness of these attacks, banks should consider threats holistically, rather than looking at each specific attack. By doing so, organizations can better anticipate specific vulnerabilities and gaps as future TTPs evolve.

A critical advancement in adversaries' TTPs has been their ability to evade detection through deploying destructive malware, often referred to as wiper ware, that erases data including logs used to monitor for suspicious activity. Usually, an adversary's malware, tools, or other activity leaves traces behind indicating what was done within a network and how. Adversaries are incentivized to remove these files over the course of an intrusion to minimize their footprint or remove it as part of the post-intrusion cleanup process.[38]

Anatomy of the coverup



Source: Accenture iDefense Threat Intelligence

Several threat adversary groups have incorporated these TTPs into their attacks that specifically target financial institutions.[39] As this type of activity continues to become more targeted, threat adversaries may take

37 Crosman, P. (2016, November 3). Ransomware: Should Banks Prepare to Pay or Be Ready to Refuse? *American Banker*. https://www.americanbanker.com/news/ransomware-should-banks-prepare-to-pay-or-be-ready-to-refuse

38 File Deletion. MITRE. https://attack.mitre.org/techniques/T1107/

39 Ibid

advantage of system encryption and file destruction for greater impact to critical systems supporting the delivery of core financial services.

With this evolution, cyber defense operators supporting financial institutions could face challenges around deciphering the differences between the attack and the coverup. Data manipulation and theft, followed by ransomware or a wiper malware, impedes incident responders' ability to perform forensics, stop the attack, and remove the adversaries from their systems.

Institutions also face attackers fighting back after they are detected, trying to circumvent defenses and the investigation into the attack. Adversaries are leaving behind destructive malware and using Distributed Denial-of-service (DDoS) to create smokescreens during events.[40] In 2018, adversaries reportedly deployed wiper malware that affected 9,000 workstations and 500 servers inside Chile's largest financial institution to shield their theft of US$10 million.[41]

Cyber-espionage campaigns, aimed at targeting the financial sector, use destructive malwares and pseudo-ransomware. More than 40,000 systems were rendered inoperable during an attack on South Korea's banking and communications sectors in 2013. Affecting four large banks, as well as several subsidiaries, there were widespread outages that had an impact on Automated Teller Machines (ATMs), payment terminals, and mobile banking services.[42] More generally, the use of destructive malware is increasing in

---

40 Higgins, K. (2018, May 22). Cybercriminals Battle Against Banks' Incident Response. DarkReading. https://www.darkreading.com/endpoint/cybercriminals-battle-against-banks-incident-response/d/d-id/1331869

41 Seals, T. (2018, June 13). Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist. Threatpost. https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/

42 Martin, D. (2015, November 20). Tracing the Lineage of DarkSeoul. SANS Institute. https://www.sans.org/reading-room/whitepapers/warfare/tracing-lineage-darkseoul-36787

frequency and scale, as shown by the Petya[43] and Shamoon[44] campaigns of 2017 and 2018 respectively.

Considering this growing threat, financial organizations should incorporate destructive attacks into their incident response playbooks and adversary simulations. Mindful of the dissolving siloes between financial, political, and ideologically motivated operations, financial institutions should prepare for likely increases in destructive computer network attacks aimed at disrupting and degrading their infrastructure.

43 Global Ransomware Outbreak Cripples Major Companies Worldwide. (2017, June 27). iDefense IntelGraph.

44 Assessing the 2018 Shamoon Campaign. (2018, December 21). iDefense IntelGraph.

EMERGING TECHNOLOGIES: BLOCKCHAIN, CRYPTOCURRENCY AND ARTIFICIAL INTELLIGENCE (AI)

Emerging technologies
Cryptocurrency fraud; hyperledger targeting

Emerging technologies
Adversarial artificial intelligence

Financial organizations are often early adopters of new technologies in their business processes. A recent example is financial organizations' exploration of blockchain technologies to enable real-time multiparty transactions with increased transparency and instant audit trails.

New technologies often provide opportunities for malicious cyber adversaries to expose gaps in security or in business processes. As crypto-assets and distributed ledger technology evolves, institutions and policy makers are working to understand how to best use these technologies while managing potential risk.[45]

One of the most discussed technologies in the financial services industry today is blockchain banking, enabling banks to process payments more quickly and more accurately while reducing transaction processing costs. Adversaries are likely to be targeting blockchain transactions already. Researchers in the security community have simulated attacks against hyper-ledger-derived frameworks being developed by major financial institutions.[46] As firms continue to explore the applications of blockchain within the sector and partner with third-party service providers to bring offerings to market, adversaries may continue to exploit opportunities.

But, targeting hyper-ledgers and derivative payment solutions was far from the first foray of cybercriminals into the cryptocurrency and blockchain space. For several years, financially motivated hackers have made use of cryptocurrency as a key mechanism for laundering ill-gotten funds and demanding ransom during extortive campaigns.

---

45 Wigglesworth, R. (2019, April 12). IMF and World Bank explore crypto merits with blockchain project. *Financial Times*. https://www.ft.com/content/1cfb6d46-5d5a-11e9-939a-341f5ada9d40

46 Haro, J. (2018). Targeted Attacks on the Blockchain (Hyperledger). CODE BLUE 2018.

EMERGING TECHNOLOGIES: BLOCKCHAIN, CRYPTO CURRENCY AND ARTIFICIAL INTELLIGENCE (AI)

It is widely accepted that technology, and cybercrime with it, develops so fast that law enforcement cannot keep up.[47] Senior law enforcement officials estimated last year that criminals crypto-laundered US$4.2 billion to US$5.6 billion in Europe alone.[48] Accenture Security has observed adversaries across English—and Russian—speaking marketplaces offering cryptocurrency "mixing" services that enable users to hide their identities while exchanging bitcoins and alternative cryptocurrencies, such as Monero and Ethereum.[49] These laundering services have seemingly succeeded in moving stolen and tainted digital currency at scale while protecting the anonymity of criminal groups.

In addition to using cryptocurrency to launder money, cybercriminals have also developed lucrative schemes to steal the coins and to conduct illicit coin mining. Numerous cryptocurrency exchanges have reported thefts of digital currency at alarming rates. More than US$1 billion worth of cryptocurrency was stolen in the first half of 2018.[50] The trend has carried into 2019 with exchanges in New Zealand, Israel and Singapore reporting breaches and reinforcing the global nature of this threat.

Another threat to blockchain and cryptocurrency is blockchain reorganization, which was undertaken by malicious adversaries in early 2019. In what is dubbed a "51 percent attack," adversaries stole nearly US$1.1 million in Ethereum Classic coins by hijacking more than 50 percent of the blockchain. The adversaries were able to "sell" Ethereum Classic coins for cash while rewriting the blockchain to steal both the

---

47 2015 Internet Organised Crime Threat Assessment (IOCTA). (2016). Europol. https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf

48 Crypto money-laundering. (2018, April 26). *The Economist*. https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

49 The Money Laundering Networks Facilitating The Cyber-criminal Underground. (2018, July 13). iDefense IntelGraph.

50 Rooney, K. (2018, June 7). $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. CNBC. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

cash and the coins. In a conventional payment system, it is up to banks and other central enforcers to stop this from happening. There is no such enforcement for cryptocurrency.[51]

With the price of cryptocurrency declining throughout 2018, hackers set their sights on cryptojacking. Malicious programs designed to mine cryptocurrency on infected machines plagued many organizations. Total CoinMiner malware grew as much as 4,000 percent in 2018.[52] Coupled with information stealers, mining malware became a feature of other campaigns as well. The Xbash malware, for example, combined botnet, coin mining, data-destructive ransomware and self-propagation into one package.[53] Financial services firms should continue to track the evolving nature of cryptojacking targeting corporate networks, especially as a possible indicator of a more severe malware infection.

Recently, some banks have started to endorse cryptocurrency exchanges and explore launching their own exchanges to capitalize on the potential business opportunity.[54, 55] Additionally, legislation in France opened the door for some insurance companies to offer life insurance contracts exposed to cryptocurrencies through specialized funds.[56] However, if a

---

51 Brandom, R. (2019, January 9). Why the Ethereum Classic hack is a bad omen for the blockchain. Verge. https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto

52 McAfee® Labs Threats Report, December 2018. (2018, December 19). McAfee Labs. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

53 Claud, et al. (2018, September 17). Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

54 Alexandre, A. (2019, February 26). Bahrain Central Bank Releases First Crypto Exchange to Graduate Its Regulatory Sandbox. CoinTelegraph. https://cointelegraph.com/news/bahrain-central-bank-releases-first-crypto-exchange-to-graduate-its-regulatory-sandbox

55 BelTA. (2019, January 28). Belarusbank might set up cryptocurrency exchange. Belarusian Telegraph Agency. https://eng.belta.by/economics/view/belarusbank-might-set-up-cryptocurrency-exchange-118236-2019/

56 Bloch, R. (2019, April 11). EXCLUSIF : Le bitcoin a désormais sa place dans les contrats d'assurance-vie. *Les Echos*. https://www.lesechos.fr/finance-marches/banque-assurances/exclusif-le-bitcoin-a-desormais-sa-place-dans-les-contrats-dassurance-vie-1008678

cybercriminal successfully targeted these funds, it could prove devastating for the insurers.

Along with blockchain, artificial intelligence (AI) is another technology that presents great opportunities for the financial services sector. Many institutions are incorporating AI into their business processes to find efficiencies, improve their decision making, and offer better customer experiences. Even though AI attack surfaces are just emerging, future security strategies should take account of adversarial AI, with the emphasis on engineering resilient modeling structures and strengthening against attempts to introduce adversarial manipulation.[57]

As adversarial AI has emerged over the past five years, Accenture has seen an increasing number of adversarial attacks exploiting machine learning models.[58] Such exploitation could multiply with the magnitude of threats facing financial services companies. As adversaries benefit from efficiencies gained through AI and machine learning, the return on investment for their malicious activities may increase. The ability to use autonomous target reconnaissance and vulnerability exploitation could decrease the turnaround time for campaigns for both well-resourced and less-skilled cyber adversaries. The ability to authenticate data and validate its integrity may be challenged by the adversarial application of AI, fracturing the basis of trust across many institutions through data theft, manipulation and forgery.

New attacks may also arise using AI systems to complete tasks that would be otherwise impractical for humans. Malicious adversaries may exploit the vulnerabilities of AI systems deployed by defenders—an important point

57 Know your Threat: AI is the New Attack Surface. (2019). Accenture. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

58 Ibid

to remember as information security teams construct their organization's threat models.[59]

When considered on its own or coupled with other threats that are increasing in frequency and potency, the malicious application of AI could be a linchpin for both financially and politically motivated adversaries throughout the many phases of their campaigns.

Accenture has seen an increasing number of adversarial attacks exploiting machine learning models.

59 Brundage, et al. (2018, February). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

DISINFORMATION

Disinformation
Election Interference; Hactivism

Disinformation
Large-scale, targeted market manipulation

Troll farms, Twitter bots and fake news—disinformation has taken center stage in the public sphere. Despite its recent prominence, disinformation has always been a tool deployed by financial, ideological, and politically motivated adversaries throughout history—the information age has simply increased the scale and speed of its impact.

The Accenture Security iDefense Threat Intelligence team has reported on the increasing significance of disinformation since the mid-2000s. In April 2007, protests over a controversial statue in Estonia were suspected of being exacerbated by false news reports of Soviet war grave defacements. Riots broke out in Tallinn—hundreds were detained, dozens injured, and one person died.[60] Beginning in 2014, Ukraine faced an onslaught of disinformation through television, online news, and other websites to split families along ethnic, political and regional lines—ultimately to damage the morale of Ukrainian soldiers.[61]

More recently, hacktivists adopted disinformation in campaigns targeting the financial sector. In January 2019, a firm was targeted by an elaborate hoax involving a spoofed letter purporting to be written by the fund group's chief executive officer.[62] The letter claimed the firm was divesting in coal companies in its actively-managed funds and changing voting patterns to take a stronger stance on climate change.[63] The adversaries

60 Van Puyvelde, D. (2015). Hybrid war – does it even exist? Nato. https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

61 Vasilyeva, N. (2018, November 26). Russia's conflict with Ukraine: An explainer. Military Times. https://www.militarytimes.com/news/your-military/2018/11/26/russias-conflict-with-ukraine-an-explainer/

62 Smith, P. (2019, January 9). BlackRock targeted by fake letter on climate change. *Financial Times*. https://www.ft.com/content/bd2113e4-198e-11e9-b93e-f4351a53f1c3

63 Morris, M. (2019, January 19). Someone wrote a fake letter pretending to be BlackRock CEO Larry Fink and some reporters got duped. *Business Insider*. https://www.businessinsider.com/larry-fink-fake-letter-on-climate-change-2019-1

also created a website that looked like the large investment management corporation's genuine webpage. Several thousand people received the fake letter and large news outlets initially picked up the letter as a legitimate communication. It was eventually revealed that the letter and website were the work of an activist seeking to raise awareness for social issues, such as the environment. The incident emphasized the low barrier to entry for an effective disinformation campaign.

These incidents remain dangerous indicators for the future of cyber threats to financial institutions and financial market infrastructures. A well-orchestrated disinformation campaign may have serious consequences on brand reputation, specific markets, and even market stability. The tools required to implement a successful campaign are well within the capability for ideologically, financially, and politically motivated threat adversaries already targeting the financial sector.[64]

Central Banks have voiced concerns regarding information operations, warning of their ability to undermine the trust in a country's banking sector. Recently, the governor of the Romanian National Bank stressed that: "as impatience has filtered into many domains, an erosion of confidence in independent, accountable public institutions like central banks has emerged."[65] To cope with this, central banks worldwide have boosted their defensive efforts related to fake news and negative campaigns.

As malicious adversaries use disinformation to maximize the effectiveness of multi-dimensional cyberattacks, trust in financial services could continue to be tested.

---

64 Trends: The Increasing Significance of Disinformation Efforts. (2008, October 5). iDefense IntelGraph.

65 Isărescu, M. (2019, March 25). Central bank communication as a policy tool – an ongoing challenge. https://www.bis.org/review/r190327d.pdf

PROACTIVE DEFENSE

THE FUTURE OF ADVERSARY SIMULATION

Cyber defense teams continuously prepare their organizations for extreme scenarios to advance cyber resilience to the next level of maturity and effectiveness.[66] Cyber threat intelligence drives these operations, enabling organizations to establish an intelligence-led cyber defense strategy. As part of this process, simulation exercises need to reflect the evolving threat landscape for the financial sector.

The attack landscape has shifted over the years. Now, the door is opening for adversaries to gain access to a wider array of capabilities ranging from targeted credential theft to destructive malware and autonomous tools. When mixed with disinformation, organized cybercriminals and politically motivated adversaries are equipped with a harmful cocktail of TTPs at their disposal.

For financial services, such attacks could upend the stability and trust that sustains the entire system. The combination of the multifaceted and multistaged campaigns of disinformation, paired with cyberattacks, can be expected to continue in coming years.

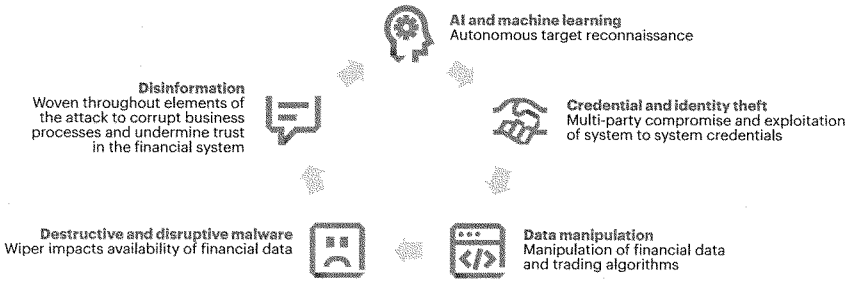
Here are five actions financial services organizations may wish to consider in the face of new threats and adversaries:

- **Collaborate** with peers and third parties on multistage exercises.
- **Invest** in people, processes and tools that identify potential disinformation concerning their firms.
- **Strengthen** insider threat programs to detect and prevent malicious adversaries from gaining access to key systems and data.

66 Duffy, S. (2019, February 21). Accenture Adversary Simulation Service: Fueled by iDefense Threat Intelligence. Accenture. https://www.accenture.com/us-en/blogs/blogs-accenture-adversary-simulation

- **Improve** online accountability through threat informed approaches to authentication and authorization.
- **Simulate** adversarial threats using disinformation, emerging technologies and compromised corporate credentials.

Simulating multiparty attacks – extreme, but plausible scenarios



Source: Accenture iDefense Threat Intelligence

GLOSSARY

Name	Type	Description	Mentioned on page:
Blockchain reorganization	Attack	Also referred to as a 51 percent attack, blockchain reorganization refers to an attack on a blockchain by a group of miners controlling more than 50 percent of the network's mining hashrate, or computing power. The attackers are able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.[67]	**22**
Petya	Malware	Petya is a ransomware that appeared in March 2016. It was first delivered to victims via an e-mail from an applicant seeking a job. Petya overwrites the Master Boot Table (MBT) to deny victims access to their computer and files. On June 27, 2017 government and business entities were paralyzed by a global campaign delivering the malware.	**20**
Shamoon	Malware	Shamoon, also known as DistTrack, is a destructive implant highly likely created by the BLACKSTURGEON threat group. Shamoon was identified in August 2012 and was publicly identified in November 2016 as part of a campaign targeting organizations in the government and resources verticals. The latest wave of Shamoon was identified in December 2018.	**20**
Xbash	Malware	Xbash is a malware that has ransomware and coin mining capabilities. It also has self-propagating capabilities and spreads by attacking weak passwords and unpatched vulnerabilities. Xbash is data-destructive; destroying Linux-based databases as part of its ransomware capabilities. The malware has been tied to the Iron Group, also known as Rocke, a Chinese-speaking hacking group that has grown in notoriety for its use of cryptojacking malware that leverages a backdoor from HackingTeam's leaked code.[68, 69]	**23**

67 Frankenfield, J. (2019, February 7). 51% Attack. Investopedia. https://www.investopedia.com/terms/1/51-attack.asp

68 Claud, et al. (2018, September 17). Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows. Palo Alto Networks. https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

69 O'Neill, P. (2018, September 18). Chinese-speaking cybercrime group launches destructive malware family. CyberScoop. https://www.cyberscoop.com/iron-group-cybercrime-destructive-malware-palo-alto-networks/

CONTACT US

Valerie Abend
Managing Director, Accenture Security
valerie.abend@accenture.com

Rikki George
Associate Principal, Accenture Security
rikki.george@accenture.com

Howard Marshall
Principal Director, Accenture Security
howard.marshall@accenture.com

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

LEGAL NOTICE & DISCLAIMER

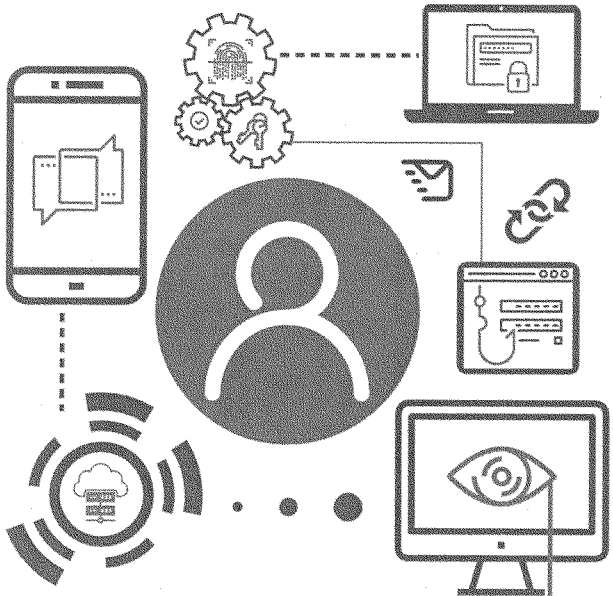
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

BR Business Roundtable



Building Trusted & Resilient

DIGITAL IDENTITY

JULY 2019

Business Roundtable CEO members lead companies with more than 15 million employees and $7.5 trillion in revenues. The combined market capitalization of Business Roundtable member companies is the equivalent of over 27 percent of total U.S. stock market capitalization, and Business Roundtable members invest nearly $147 billion in research and development — equal to over 40 percent of total U.S. private R&D spending. Our companies pay $296 billion in dividends to shareholders and generate $488 billion in revenues for small and medium-sized businesses. Business Roundtable companies also make more than $8 billion in charitable contributions. Learn more at BusinessRoundtable.org.

Building Trusted & Resilient DIGITAL IDENTITY

JULY 2019

CONTENTS

Introduction

The ability of individuals to recognize and trust each other plays a fundamental role in economic and social interactions.

Before the digital age, identification systems relied upon physical documents and face-to-face interactions. The internet and the proliferation of internet-enabled devices have dramatically changed the interplay between individuals and institutions — from the way we bank and shop to the way we communicate with each other. At the same time, the internet has made disguising, hiding or misrepresenting their identities substantially easier for malicious actors, forcing us to find new ways to confidently interact with one another online.

Personal information is a lucrative target for theft. Misusing it to create illegitimate digital identities is one of the simplest methods for committing online fraud. Indeed, identity fraud costs the U.S. economy billions of dollars annually — in 2018, $14.7 billion was stolen from U.S. consumers online.[1] Malicious actors also exploit fraudulent identity information to illegally collect government benefits, such as food stamps; unemployment assistance; and Medicare, Medicaid and Social Security payments. The surface area available for attack will significantly expand as we increasingly interact with internet-connected devices across all aspects of life.

While service providers and cybersecurity firms work to keep up with evolving threats, criminals use creative and sophisticated tools to stay a step ahead. As a result, illegitimate identity may well be the likeliest path for fraud and other cybersecurity intrusions.

Yet having a digital identity is more than a data protection and security mechanism — it enables individual users and institutions to establish an appropriate level of trust to transact and interact in the digital world, including activities ranging from banking to health care to social media. And in a world in which boundaries among sectors are increasingly blurred, the relationship of a user and a company is no longer always directly owned or governed by the company. With digital identity being a key enabler for participation in digital interactions, it must not only be secure but also convenient so it can be used across sectors and in daily interactions.

To continue to reap the benefits of the online world, it is imperative that the U.S. government and the private sector work together to strengthen digital identity without sacrificing the speed or convenience that today's society demands. Meeting this goal would strengthen the entire online ecosystem — from e-commerce to health care, employment, supply chains and more.

This paper presents an approach to digital identity that would reduce identity theft and fraud without creating undue costs or burdens for users or service providers. It describes the current state of play, offers a vision for the future, and then puts forward a realistic action plan for how the private and public sectors can bolster digital identity.

Digital Identity Today Promise & Challenges

While anonymity is a fundamental and cherished aspect of the internet, some services require at least partial knowledge of an individual's identity to function properly.

Digital identity is the online persona of a subject, and a single definition is widely debated internationally.[2] Digital identity proofing and authentication are the two primary methods of establishing verifiable identity attributes, and opportunities exist to improve both, which may represent one's physical and online personas. (For a "Primer on Digital Identity," see the Appendix.)

Identity Proofing

Identity proofing establishes that a subject is whom he or she claims to be.[3] Service providers conduct identity proofing early in a transaction, such as opening a bank account or applying for a student loan. In a brick-and-mortar establishment, the service provider can check a customer's driver's license or passport to prove the person's identity. This process is more difficult online, however.

Digital identity proofing consists of three steps: resolution, validation and verification. Resolution often involves using records available from public sources to ascertain the identity of an individual. Validation confirms the authenticity and accuracy of the identity information by checking an authoritative source, and verification relies on information that only the individual and the party doing identity proofing should know — such as transaction history — to confirm ownership of the claimed identity (see the Appendix).

The resolution and verification stages have historically involved individuals confirming personal information. In the digital world, however, knowledge-based proof is no longer sufficient for many purposes. Data breaches and the increased sharing of sensitive data via online platforms such as social media mean that this method is no longer as trustworthy as it once was. Additionally, this method of identity proofing may unintentionally favor certain portions of the population, such as those with longstanding accounts and credit histories.

New technologies have created opportunities to increase confidence in the authenticity of identity evidence. For example, a bank could remotely match identity documents and biometrics — such as a photo — from a digital driver's license with the individual presenting the evidence. These approaches can be done remotely with mobile phones and personal computers and are effective for many users.

IDENTITY PROOFING VS. AUTHENTICATION

IDENTITY PROOFING: The process by which an organization collects, validates and verifies information about a person, often occurring at the time of enrollment.

AUTHENTICATION: The process of determining the validity of one or more credentials presented by a party as a prerequisite for granting access to a system or information.

These new technologies are a step toward the future; thanks to the digitization of government-issued identification, users with a driver's license and a passport have a high likelihood of being able to prove their identity online. However, an individual without these forms of identification — or without a smartphone — will struggle with (or be unable to use) these solutions. The individual will often have to fall back to inconvenient alternatives, such as visiting a brick-and-mortar location, which increases the effort to the user and costs the service provider time and money. While progress has been made, much work remains to be done to improve identity proofing.

Authentication

Authentication factors include things users **know** (namely passwords), **have** (namely credentials) or **are** (namely biometric identifiers). Knowledge-based authentication, commonly used today, has inherent weaknesses. Strong authentication relies on the robustness of identity information available at the time of the presentation of the identity claim. Often, improving the robustness of this information involves multifactor authentication (MFA), in which at least one factor is not knowledge based. Companies and governments are increasingly offering, and in some instances requiring, MFA. MFA can include asking a user to present his or her biometrics (verifying who the user *is*) or sending a code to a smartphone (verifying what the user *has*).

MFA solutions may have some residual user friction. For example, if MFA options are specific to each service provider, second-factor authenticator fatigue could set in on top of existing password fatigue. If adopted broadly and implemented well, smartphone-based authentication, biometrics and other promising technologies could mitigate this risk.

The application of data analytics, artificial intelligence, machine learning and multimodal biometrics to authentication is also increasing the availability of trusted authentication solutions.

Identity Federation and Decentralized Identity

When two or more traditional identity systems (e.g., a government entity and a bank) establish mutual trust — either by distributing components of proofing and trust or by mutually recognizing each other's proofing and trust standards — a federated identity system results.[4] These systems are prevalent in some day-to-day activities. For example, consumers know they can get cash at virtually any ATM (while paying a fee to do so), rent a car using a driver's license from another state, and log in to a third-party service through their social media or email accounts.

At the enterprise level, identity federation has seen widespread adoption. For example, many companies federate an individual's corporate identity to allow easy access to benefits information, such as health care claims and retirement planning. Federation has also found success in the defense, aerospace and automobile industries, with the government and/or industry partners taking a shared approach to employee vetting, such as security clearances. The benefits of federation have long been clear to participants in those industries, where trust is established among multiple

DECENTRALIZED IDENTITY SYSTEM PILOTS

MALTA: The government of Malta is piloting a program in which educational institutions use blockchain technology to issue credentials (such as diplomas and 15 professional certifications) to individuals, who can access and manage them through a mobile application.

ANTWERP: The city of Antwerp has piloted a system for individuals to create and manage a through-life identity on a mobile application employing blockchain technology, starting with identity attestations at birth from doctors, hospitals and the government birth registry.

organizations or where a single organization has individual trust relationships with other organizations such as a trusted intermediary. Federation may create efficiencies by accepting the identity proofing and authentication conducted by a different trusted institution. However, a federated model is based on individual agreements between institutions to trust and accept the digital identity of another. While the user may be required to remember one fewer set of login credentials per federation agreement, the digital identity often is not accepted more broadly and depends on established governance between institutions.

For broader consumer adoption, decentralized identity systems, which are mostly in pilot phases, offer some intriguing alternatives to central and federated identity schemes. Instead of partners relying on a data owner, a set of owners or a trusted intermediary to establish and manage identities, consumers could use their digital devices to hold attestations from several trust anchors, such as governments, banks and employers. The individual could choose which attestation or data attribute to share and with whom to share it.[5] Therefore, in a decentralized identity system, a user often would have greater control over his or her own identity and identity data. Decentralized identities, however, would still require large or complex governance and liability models and are currently being explored as this landscape continues to evolve.

A Vision for the Future

Objectives for Improving Digital Identity

To take full advantage of advances in technology, an appropriate mix of policy and process needs to be in place.

Businesses, governments and individuals should be able to securely, intuitively and easily execute digital transactions that respect privacy, are free from fraud, have relatively low costs, and present choices that have very little friction for both individuals and organizations. To meet this goal, the U.S. government and the private sector must work together to establish digital identity systems based on:

1. Strong identity proofing that reduces identity fraud by discouraging reliance solely on knowledge-based techniques.
2. Strong authentication, with effective options for MFA that are free to consumers, and strong fraud detection capabilities to protect against unauthorized release or access to personal and account information.
3. Use of identity federation and decentralized identity to reduce unnecessary repetition of identity proofing and authentication, while providing more transparency and control of identity data to users.

These systems should achieve the following goals:

Strengthen and Sustain the Security and Privacy of Digital Services

Policies should promote user confidence in online services — from financial transactions and accessing health care benefits to requesting government services. To reduce the risk and impact of identity theft, digital identity solutions must embed robust security and privacy that consumers can trust and must be able to introduce new security techniques as the threat landscape evolves.

Insure Digital Identity with a Safety Net

For a digital identity to be resilient, organizations must not only provide security to prevent a breach from occurring but also be prepared for *when* a breach occurs. Users will put more trust in a digital identity if a "safety net" insures the users against the harm done when identity data are stolen and enables continuity of service. When liability is clearly assigned and an ecosystem of trusted participants helps hold

the safety net, users can continue to transact business even when an individual organization's digital identity system — and trust in it — has been breached. These factors create a truly resilient digital identity.

Enable Convenient Access to Digital Services

Individuals should be able to conduct online transactions quickly and easily. Future solutions must reduce or replace the number of usernames and passwords required and prevent a confusing proliferation of second-factor options required of users.

Provide Transparency and Choice

Greater transparency and choice will require organizations to design privacy risk management into their products and empower users to take an active role in the management of their personal information. Users should have informed consent regarding the information they share, the ability to revoke that consent and control access to information, and the ability to access their information throughout their relationship with the service.

Enable Wide Availability of Authoritative Attribute Sources

Industry and federal, state and local governments are among the stewards of information that can assist in authentication and in identity proofing an individual. Organizations that maintain verified and accurate information should provide services to support attribute verification. This information must be accessible only by service providers meeting defined security and privacy protection standards, which are critical to outline in the terms of use agreed to by ecosystem participants. If done properly, this approach can reduce the number of times identity proofing is necessary by sharing specific pieces of verified information with user consent.

Increase Digital Literacy and Awareness

Users should be well educated in how their information is collected, used and shared — and the potential implications of those actions. Consumer awareness programs should help individuals understand how to create, use and maintain their digital identity, in addition to their other options and responsibilities as a digital citizen. Helping all stakeholders understand the value of stronger identity solutions and how they function will increase security while encouraging widespread adoption.

An Action Plan
to Establish Trust & Resiliency in Digital Identity

The action plan that follows will promote strong and resilient digital identity systems and help reach the aforementioned goals.

Industry will lead the development, delivery and adoption of digital identity solutions that are meaningful, convenient, secure and privacy enhancing. Government will play a supportive role to remove barriers, while also adopting industry-proven solutions for its own services.

ACTION 1
Reduce Dependency on Passwords to Provide More Intuitive and Secure Authentication

Industry and government should not create a greater authentication problem than the one that currently exists. To avoid exacerbating password fatigue by requiring additional authenticators (also known as tokens), industry and government should:[6]

- Transition from issuing authenticators to accepting authenticators a user already has and likes through decentralized identity. For example, allow users to register to their account a verified and secure authenticator, such as a mobile app or the biometric sensors available on a mobile device.
- Adopt open standards, such as Fast Identity Online, to strengthen authentication solutions that provide a path to password-less options.
- Maintain risk-appropriate levels of friction for the user — make authentication as intuitive and user friendly as possible, and as secure as necessary, for a given transaction.
- Adopt and enhance strong fraud detection capabilities where possible; robust authentication and fraud detection should go hand in hand.
- Develop and adopt authentication technologies that correspond to the current maturity of attack techniques, adapting as the threat landscape evolves.
- Offer the option to enable MFA everywhere and require MFA for services that maintain information or for services of significant value to users.
- Develop and offer national metrics, testing and reporting programs for better identity and MFA solutions, including comparability, efficacy and compliance with standards.

ACTION 2
Eliminate Identity Proofing Solutions That Are Solely Knowledge Based

Industry and government must work to adopt and encourage the development of identity proofing solutions that are both more secure and less onerous. Multiple solutions must be available that work for all segments of the population and that are able to prove comparability to other solutions. Industry and government should ensure that everyone has a chance to successfully prove their identity online.

To that end, government should encourage industry to:

- Eliminate identity proofing based solely on knowledge of information (e.g., Social Security number [SSN], password and answers to personal questions).
- Develop and adopt approaches to support identity proofing across demographic and economic boundaries, including individuals with little to no financial history.
- Partner with government at all levels, including internationally, to develop responsible information sharing agreements to expand the types of evidence that can be used to identity proof an individual.
- Collaborate across sectors to reduce repetitive identity proofing and provide services to validate the authenticity of information.
- Collaborate to deploy solutions that can facilitate more accurate detection of potential fraudulent behaviors.
- Develop and offer cross-industry metrics, testing and reporting programs for identity proofing solutions, including comparability, efficacy and compliance with standards.
- Adopt standards to share validated and verified attributes without requiring a complete identity proofing instance when minimal personal information is needed to deliver the service.

ACTION 3
Change the Use of SSNs

The SSN is an identifier, not an authenticator. Knowing a given SSN does not prove that it is the individual's SSN. As an identifier, the SSN is highly effective. It helps to delineate among, for instance, multiple people with the same name and birthdate. The SSN is a helpful tool to find key information about an individual, but the individual must prove his or her identity through other means.

As the authoritative source for SSNs, the Social Security Administration (SSA) is uniquely positioned to correct one of the greatest weaknesses in digital identity. Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 establishes a means for organizations to validate the SSN against authoritative SSA data.[7] This process is a great step forward to thwart identity fraud.

Congress and the Administration should:

- Fully implement Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018, which empowers the SSA commissioner to expand the definition of permitted entities to include other organizations that have a need to validate an SSN.
- Discourage the use of SSNs as an authenticator within both government and industry but continue to allow the use of SSNs as an identifier.
  - In providing identity verification services to permitted entities, SSA should specify that the information is used only for verification and identity proofing purposes and not for authentication purposes.
  - The Administration should prohibit the use of SSNs for any authentication services offered by agencies.
- Provide options for individuals to configure how service providers can leverage their SSN and to receive alerts if their SSN has been verified by the SSA for a third party.

All entities, including government, the private sector and academia, must find new ways to authenticate individuals and adopt innovation as it becomes available to further deter SSN-related identity theft.

ACTION 4
Improve Government Support for Validating Identity Attributes and Verifying Identity Claims

Comprehensive identity proofing solutions will need to validate an individual's attributes from multiple data sources, including those managed by federal, state and local governments. Whether the source is a driver's license, passport, military ID or financial account, strong digital identity relies on access to authoritative data sources to determine that the information exists, is correct and is authentic.

To support enhanced identity proofing solutions, Congress, the Administration, and state and local governments should:

- Update laws, regulations and policies that currently prohibit government agencies from sharing data regarding identity attributes of individuals with the private sector and other public agencies. Specific attention should be paid to agencies such as SSA, the Internal Revenue Service, the Department of State, the Department of Defense and the Department of Veterans Affairs.
  - Government attribute validation services should be limited to validating claims rather than revealing personal information. In other words, the government should, with proper privacy protections in place, offer "yes" or "no" responses to organizations' inquiries.
- Increase federation of identity across the federal government. For example, the Transportation Security Administration and Customs and Border Protection issue Pre-Check and Global Entry credentials based on rigorous identity proofing. That background check could be incorporated into federal job applications and other federal benefits and services.
- If an individual has successfully completed the Pre-Check process, he or she should not need to repeat similar portions of the process for volunteering in a child care setting or working in a health care environment.
- Develop solutions and services to validate identity claims that bind documents to document holders — for instance, use biometrics to verify that a document belongs to the person providing the document.

ACTION 5
Reduce Barriers to the Adoption of New Technologies

New categories of information (e.g., device intelligence, biometrics, behavioral analytics) can be used to assist in proofing and authenticating individuals. However, current legal and regulatory regimes may impede some companies from adopting these innovative technologies.

In consultation with private-sector and consumer groups, Congress, the Administration and state governments should:

- Provide clarifying guidance to reduce legal uncertainty around the use of new categories of information or technologies and to avoid conflicts across jurisdictions. For example, as biometrics have become near-ubiquitous, some states and countries have specified appropriate use and storage of biometric data.
- Create a communication network and repository for federal and state governments to learn about and adopt each other's technology and implementations.
- Expand guidelines, such as the National Institute of Standards and Technology (NIST)

Special Publication 800-63, that outline acceptable use and standards of care for identity proofing via digital means. These guidelines, if enacted through law or regulation, should offer states options and should not stifle innovation.

- When updating regulatory regimes, ensure that regulators work with industry to incorporate best practices in digital identity while allowing flexibility in specific implementation. This action will promote alignment of regulatory regimes, resulting in a safer, more efficient regulatory environment while allowing room for innovation.

ACTION 6
Establish a Public-Private Partnership to Focus on Implementation of Digital Identity Solutions at Scale

Digital identity affects all users of the internet and will continue to do so for the foreseeable future. To develop requirements, test and pilot solutions, and transition them into the market, the Administration should:

- Direct the Department of Commerce's NIST to advance international standardization of Special Publication 800-63 to an international standards development organization.
- Direct the National Cybersecurity Center of Excellence and IT Modernization Centers of Excellence in the General Services Administration (GSA), in collaboration with other federal agencies, to develop a "proving ground" for identity proofing solutions. NIST and GSA should leverage their existing capabilities to engage the private sector, assess the effectiveness of market innovations and rapidly transition successes throughout government agencies.
- Direct the National Science Foundation, the Networking and Information Technology Research and Development program, the Department of Homeland Security, and other research agencies to promote long-term evolution in digital identity through R&D activities in authentication and identity proofing.

ACTION 7
Enhance Privacy Through Digital Identity

Advances in digital identity must preserve and, wherever possible, enhance the current state of individual privacy. Business Roundtable supports a national consumer privacy law that champions privacy and accountability, fosters innovation and competitiveness, harmonizes regulations, and facilitates interoperability.[8]

To champion privacy in digital identity solutions, industry should:

- Build solutions that empower users with choices related to how their personal data are collected, used, processed, transferred and shared and that clearly define obligations and accountability.
- Build solutions that maximize global interoperability and enable compliance with privacy regimes.
- Take a technology-neutral, principles-based approach to allow different types of organizations to adopt appropriate risk-based privacy protections.

Policymakers should:

- Support state and municipal pilots that test decentralized identity systems to enable greater user trust and control of data. Decentralized systems can support a more appealing digital consumer experience since individuals increasingly expect and can manage greater personalization and transparency. These systems can also facilitate interoperability between existing, isolated systems through verifiable claims.[9]

ACTION 8
Bolster Digital Identity Education and Awareness

All stakeholders, including individuals, business leaders and government officials, should understand the basics of how digital identity works and what happens when users make the decision to share their information online. It is critical that users understand their rights and what companies and third-party entities intend to do with their data. Increased understanding of digital identity and its role in the digital world will encourage more widespread adoption of stronger, privacy-enhancing solutions.

The Administration and state governments should:

- Create a digital identity education and awareness initiative for individuals. The program should improve digital literacy and increase understanding of how the digital identity ecosystem works, the role of various stakeholders and how improved solutions can benefit all Americans. Many stakeholders have not yet embraced next-generation solutions because they do not understand how they function. Increased adoption of next-generation digital identity solutions will require greater understanding of the risks associated with continued usage of legacy identity proofing and authentication solutions as well as the benefits of transitioning to new approaches.

Congress should:

- Fund and direct law enforcement agencies, agency offices of the inspectors general, the Department of Homeland Security and NIST to develop outreach programs in collaboration with the National Cyber Security Alliance to educate the public and raise understanding of digital identity and digital citizenship.

Education and awareness programs are needed to promote shared understanding of digital identity challenges and solutions and enable dialogue among all stakeholders in the ecosystem.

Conclusion

Improving the state of digital identity is a national imperative.

The United States needs solutions for digital identity that are proactive and that support the enterprising and entrepreneurial spirit of the American digital economy. Governments and industry must collaborate to build a better path forward for the digital ecosystem.

This action plan builds on the lessons learned from the past and augments meaningful progress in the market. Execution of these near-term and attainable actions will bring together the necessary efforts of many entities that have a shared vision of strengthening digital identity. All organizations, large and small, public and private, can reap the benefits if these actions are taken.

Real progress requires decisive action and meaningful collaboration. Doing nothing is the biggest risk of all. By embracing this plan as a collective mission, the U.S. government and private sector can reduce fraud, protect individuals, and improve security and privacy for all.

APPENDIX

Primer on Digital Identity

This section explains the primary components of digital identity: identity proofing, authentication and federation.

Digital Identity

Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service means that, for instance, every username is a unique digital identity, but the real-life identity behind the username may not be known.[10]

For the purposes of this document, there are two critical takeaways from this definition:

1. Digital identity as an online persona means that an individual can have any number of digital identities to interact online; and
2. A digital identity is always unique in the context of the service being accessed.

Digital identity also offers similar benefits to the offline world. When paying with a credit card, the store needs to know a verified attribute — that the credit card is valid. It does not need to know the user's name, address or birthdate.

Over time, most online services have trended in the opposite direction. Individuals tend to share a lot of personal information to transact — yet this broad sharing of personal information does not have to happen. With a good digital identity, an individual can assert identity (sometimes via an online third party, a credit card number, an address or a birthdate, all validated) to obtain a benefit or service without giving away more information than necessary.

In fact, digital identity can reveal even fewer attributes than transactions in the physical world, if done right. Simple technical approaches exist that allow age validation without giving away all of the information on a driver's license. A common trusted source can simply assert, for instance, that the user is older than 25 without sharing the entire date of birth — let alone name, address, height and weight.

These methods, however, have experienced slow adoption. The technological capability exists, but legal, policy and institutional barriers remain.

Identity Proofing

Some online transactions require a subject to prove identity. This requirement is no different than in physical transactions, such as walking into a bank to open an account. The process has three parts: resolution, validation and verification.

In person, a representative of the bank will typically take the applicant's driver's license and enter it into a system that looks for other accounts with that information. This process is called *resolution*.

More commonly, stores are scanning driver's licenses to *validate* them — a digital process. The difficulty comes mostly in *verification* — proving that the person presenting the evidence is actually the owner of the evidence. In the physical world, this is usually accomplished by looking at a picture on a form of identification and comparing it to the person in front of the verifier. Digital service providers have a particularly difficult time determining exactly who is on the other side of the screens, Wi-Fi and fiber optic cables.

The generic identity proofing process is depicted in Figure 1. These days, even in a physical setting, resolution and validation are typically done through digital means by the company or service provider, though the process includes physical checks such as making sure the driver's license looks and feels right.

Two forms of fraud involve identity proofing: traditional identity fraud, which involves impersonating a real-life individual (usually called identity theft), and synthetic identity fraud, which involves combining different individuals' personal information (e.g., address, birthdate and Social Security number) into a new, fictitious person. Collecting and validating personal information, or identity evidence, goes a long way toward combating synthetic identity fraud. But it does not solve traditional identity fraud. One must prove that he or she is the rightful owner of the information to stop the traditional form of fraud.

Authentication

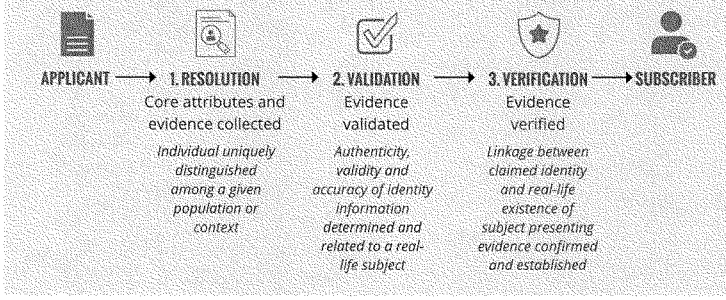
Authentication provides a means for a returning user — and only that returning user — to get back to his or her previous work. When an individual registers for an online service, he or she is usually given one or more authenticators to use from that point on. Authenticators are tools for the user to provide reasonable assurance that the same user is coming back.

Historically, the authenticator of choice has been a password. Now, organizations are moving toward multifactor authentication (MFA). MFA is familiar to Americans, though they may not know it by name. The use of an ATM with a debit card (something a user has) and a PIN (something a user knows) is a form of MFA individuals have been using for decades.

While strong authentication practices have grown at steady rate, they have not become ubiquitous. For example, widespread adoption of MFA comes with a set of challenges:

- Asking a user to download a free login application before checkout, such as an app that generates a time-based one-time code. This process adds significant user friction.
- Asking a user to purchase authentication hardware or the organization issuing that same hardware to the user. With issuance comes delay in service accessibility because the hardware, such as secure USB keys, must be shipped to the user.

FIGURE 1
GENERIC IDENTITY PROOFING PROCESS



- Creating an overload of authenticators by requiring users to have a different password and hardware or software authenticator for each site with which they interact.

Digital Identity Federation

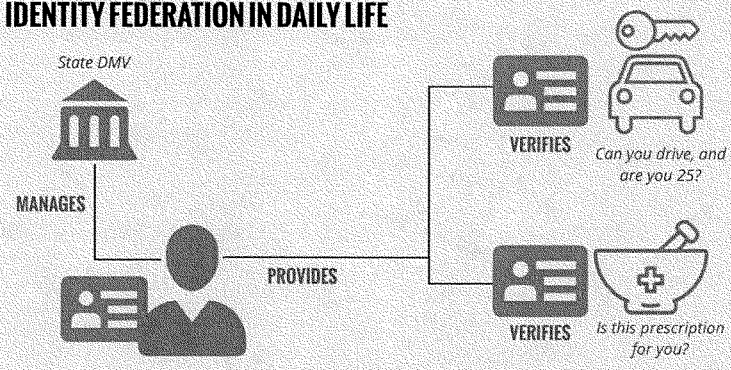
Digital identity federation allows identity information and authentication mechanisms to be shared and trusted by organizations that did not originally proof the identity or issue the authenticators. At a higher level of assurance, proofing organizations and those that establish and maintain authenticators with the user (credential service providers [CSPs] or identity providers [IdPs]) provide information on how they operate. Relying parties (RPs) or service providers (SPs), organizations that receive information from CSPs and IdPs, trust the proofing and authentication mechanisms used by the IdPs and establish rules and agreements for sharing information.

Federation is a mechanism that can reduce the number of credentials a user must remember and offers the promise of enhancing privacy by allowing a user to share verified information, but only the information deemed necessary to use a service — versus, for instance, a user needing to share a multitude of attributes with many organizations so that each organization may perform identity proofing and authentication processes. The techniques have existed for decades, but modern technologies, near-ubiquitous internet connectivity and widespread adoption of powerful consumer devices create an opportunity to bring these approaches into the mainstream.

Americans federate their identities every day. The driver's license is a great example of an individual being issued something (the license) by a third party (the Department of Motor Vehicles [DMV]) and it being accepted in many places. As depicted in the diagram below, a license asserts, "I can drive" and "I am of the required age to rent a car." The license also asserts, "I am me" and "I can buy a prescription written for me." The number of use cases for the driver's license beyond driving is vast.

The same approach is recommended for digital identity. An IdP establishes a digital identity for individuals who complete the identity proofing process. The IdP issues an authenticator to the individual or lets the individual link his or her own authenticator to the account. From that point on the individual can use that authenticator at any site that will accept it.

FIGURE 2
IDENTITY FEDERATION IN DAILY LIFE



A major consideration of federated identity approaches is managing privacy risk. Without proper protections, an IdP will know each time the user logs in to any given service. This approach could create a single entity that effectively knows everywhere a user goes on the internet. Technology measures exist that can mitigate this situation, but they must be built in from the start (often known as "privacy by design" or "by default"). Users must also be educated to understand how their personal information is being used. This situation, too, replicates the physical world, as the DMV does not know every movie theater and liquor store at which an individual shows a driver's license.

When implementing federation, it is also important to consider the potentially high governance overhead involved in setting up agreements between many parties. While some methods of federation allow dynamic registration of IdPs or SPs, each party involved — whether an IdP or an SP — must decide which organizations it trusts to either provide or receive information. The parties must also decide on the rules by which information is shared; the protocols and technical infrastructure to be used and implemented; and requirements for audits, testing and certifications.

In the consumer space, federation of digital identity for higher-risk services has seen low adoption. The solution provides clear consumer advantages — fewer logins and more personalized experiences — but businesses need to evaluate the value proposition based on their own circumstances. Traditionally, businesses claim that owning the account creation process is crucial to establish and maintain the relationship with the customer. However, that process does create a barrier for consumer acquisition. Alternatively, companies could outsource this function by adopting federated identity solutions in which they rely on credentials established through a third party. Federated identity is consumer friendly because it reduces login requirements, removes a barrier to customer acquisition, and enables customer-centric communications and marketing. It can also be business friendly by reducing the costs and effort associated with establishing and maintaining independent identity proofing and authentication. Instead, federated companies could amortize the costs across participating companies and remove the need to independently maintain specialized personnel and solutions for identity proofing and authentication. Organizations must also consider how liability is to be assigned among the parties and, critically, must develop mechanisms for redress.

Decentralized Digital Identity

Decentralized identity is an emerging archetype; unlike centralized or federated systems, decentralized systems do not rely on system owners to manage and control digital identity data. Rather, users, usually through a mobile app, are provided *attestations* of identity by various trusted organizations (trust anchors). In this way, the individual is able to control and manage his or her trusted identity data — including with whom to share the data. Decentralized identity systems are often built on distributed ledger technology and supported by a wide consortium of players.

Decentralized identity's strengths lie in giving the user more transparency and control over his or her own identity data, as opposed to traditional models in which the identity system owners generally manage not only identity management but also the relationship with the end user. Therefore, organizations must consider how a decentralized identity system changes the model for consumer engagement. Additionally, with the introduction of new technology, governance and legal models for digital identity will need to evolve.

This type of identity system is still being explored, though several pilots are ongoing across the globe.

ENDNOTES

1 Javelin Strategy & Research. (2019). Consumers increasingly shoulder burden of sophisticated fraud schemes, according to 2019 Javelin Strategy & Research study. Retrieved from https://www.javelinstrategy.com/press-release/consumers-increasingly-shoulder-burden-sophisticated-fraud-schemes-according-2019

2 Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity guidelines* (NIST Special Publication 800-63-3). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

3 *Ibid.*

4 World Economic Forum. (2018, September). *Identity in a digital world: A new chapter in the social contract.* Retrieved from http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

5 *Ibid.*

6 Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., & Richer, J. P. (2017, June). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

7 Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub. L. No. 115-174, § 215. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/2155/text#toc-id300CF8635ABE45D48B8E289E6B95C4FA

8 Business Roundtable. *Framework for consumer privacy legislation.* Retrieved from https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf

9 World Economic Forum. (2018, September). *Identity in a digital world: A new chapter in the social contract.* Retrieved from http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

10 Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017, June). *Digital identity guidelines* (NIST Special Publication 800-63-3). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf