

IDENTITY VERIFICATION IN A POST-BREACH WORLD

HEARING BEFORE THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 30, 2017

Serial No. 115–83



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

28–714 PDF

WASHINGTON : 2018

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon

Chairman

JOE BARTON, Texas

Vice Chairman

FRED UPTON, Michigan

JOHN SHIMKUS, Illinois

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. MCKINLEY, West Virginia

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

TIM WALBERG, Michigan

MIMI WALTERS, California

RYAN A. COSTELLO, Pennsylvania

EARL L. "BUDDY" CARTER, Georgia

JEFF DUNCAN, South Carolina

FRANK PALLONE, JR., New Jersey

Ranking Member

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

RAUL RUIZ, California

SCOTT H. PETERS, California

DEBBIE DINGELL, Michigan

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

VACANCY

Chairman

H. MORGAN GRIFFITH, Virginia

Vice Chairman

JOE BARTON, Texas

MICHAEL C. BURGESS, Texas

SUSAN W. BROOKS, Indiana

CHRIS COLLINS, New York

TIM WALBERG, Michigan

MIMI WALTERS, California

RYAN A. COSTELLO, Pennsylvania

EARL L. "BUDDY" CARTER, Georgia

GREG WALDEN, Oregon (*ex officio*)

DIANA DeGETTE, Colorado

Ranking Member

JANICE D. SCHAKOWSKY, Illinois

KATHY CASTOR, Florida

PAUL TONKO, New York

YVETTE D. CLARKE, New York

RAUL RUIZ, California

SCOTT H. PETERS, California

FRANK PALLONE, JR., New Jersey (*ex officio*)

C O N T E N T S

	Page
Hon. H. Morgan Griffith, a Representative in Congress from the Commonwealth of Virginia, opening statement	2
Prepared statement	3
Hon. Kathy Castor, a Representative in Congress from the State of Florida, opening statement	4
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	5
Prepared statement	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	8
Prepared statement	9
WITNESSES	
Troy Hunt, Information Security Author and Instructor, Pluralsight	11
Prepared statement	13
Answers to submitted questions	99
Jeremy Grant, Managing Director, Technology Business Strategy, Venable, LLP	25
Prepared statement	28
Answers to submitted questions	102
Edmund Mierzwinski, Consumer Program Director, U.S. PIRG	47
Prepared statement	49
SUBMITTED MATERIAL	
Subcommittee memorandum	95

IDENTITY VERIFICATION IN A POST-BREACH WORLD

THURSDAY, NOVEMBER 30, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in room 2322, Rayburn House Office Building, Hon. H. Morgan Griffith (vice chairman of the subcommittee) presiding.

Members present: Representatives Griffith, Brooks, Collins, Walberg, Costello, Carter, Walden (ex officio), Schakowsky, Castor, Tonko, Clarke, Ruiz, and Pallone (ex officio).

Staff present: Jennifer Barblan, Chief Counsel, Oversight and Investigations; Samantha Bopp, Staff Assistant; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight and Investigations, Digital Commerce and Consumer Protection; Elena Hernandez, Press Secretary; Paul Jackson, Professional Staff Member, Digital Commerce and Consumer Protection; Bijan Koochmaraie, Counsel, Digital Commerce and Consumer Protection; Alex Miller, Video Production Aide and Press Assistant; John Ohly, Professional Staff Member, Oversight and Investigations; Hamlin Wade, Special Advisor for External Affairs; Jessica Wilkerson, Professional Staff Member, Oversight and Investigations; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Julie Babayan, Minority Counsel; Jeff Carroll, Minority Staff Director; Chris Knauer, Minority Oversight Staff Director; Miles Lichtman, Minority Policy Analyst; Dino Papanastasiou, Minority GAO Detailee; and C.J. Young, Minority Press Secretary.

Mr. GRIFFITH. We will go ahead and get started.

Welcome to this meeting of the O&I Subcommittee of Energy and Commerce. So that everybody knows, there are a lot of folks who are at another hearing downstairs and will be drifting in and out.

Also, I would like to take a point of personal privilege and recognize Allie Gilmer and Olivia Smoot, who are here visiting today from my district at Auburn High School in Riner, Virginia.

They are too young to remember this but I started representing the Riner area in 1994 in the State legislature. So it's good to have you.

Ms. CASTOR. Do you want to stand up?

Mr. GRIFFITH. Yes, stand up. Be recognized. Thank you.

Thank you again. Welcome. Glad you're here with us today.

That being said, let's get started with our business here today, and other folks will join us as we go forward on this very important issue.

OPENING STATEMENT OF HON. H. MORGAN GRIFFITH, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

We are here today to talk about a very important topic: identity verification in a post-breach world. This hearing is especially timely, given several events that have taken place since the hearing itself was announced last week, including three newly discovered data breaches that comprised an additional 58.7 million records as well as two major shopping days—Black Friday and Cyber Monday.

With consumers rushing to take advantage of holiday sales both in stores and online, the questions and challenges around modern identity verification become even more pressing.

Data breaches have been increasingly—have been an increasing problem over the last several years. In fact, it is likely that everyone in this room has had their information included in a recent breach.

Between the 57 million accounts comprised in Uber's recent disclosed 2016 breach, the 145 million accounts compromised in Equifax's breach, or the 22 million accounts compromised in the OPM breach, as well as many others, I would argue that it would be difficult to find an American whose information has not been compromised.

While these breaches themselves are troubling enough, they also raise a subtle more complicated series of questions and issues around the ways in which organizations including government agencies, banks, health care organizations, and retail companies perform identity verification of their citizens and their customers.

It is a well understood concept that, to quote the famous cartoon on the internet, nobody knows you're a dog when you're in the internet.

This anonymity has many advantages and it is important to many aspects of the modern internet.

However, as the global economy has become more and more digital and an increasing amount of commerce takes place online, it also creates significant challenges for organizations attempting to ensure that they provide information and services only to authorized individuals.

Because these interactions usually take place on opposite ends of an internet connection with participants rarely if ever meeting face to face, the ability of organizations to remotely verify individuals has been a constant struggle.

As a result, for years many organizations have relied on a type of identity verification known as knowledge-based authentication, or KBA. We are all familiar with this process even if we don't quite know it.

For example, some online accounts ask consumers to provide answers to security questions such as their mother's maiden name, the make and model of their first car, or the street on which they grew up on.

Similarly, when consumers attempt to open new credit lines, they are often asked a series of multiple-choice questions that may ask who provided a consumer loan and in what year.

These are all examples of KBA. The effectiveness of KBA depends on a very important assumption—that information such as birthdays, mothers’ maiden names, addresses, work histories and other KBA attributes remain relatively secret.

In today’s post-breach world, this is a tenuous assumption. Add the wealth of personal information consumers voluntarily share about their lives through social media and this assumption appears almost laughable.

So what do we do? If modern commerce and many other services including government services rely on KBA for identity verification and that verification is no longer as secure or reliable as it was in the past, we need new strategies and new technologies to ensure that consumers are protected and economic growth continues and we need them quickly.

With the exponential growth of connected devices and services, it is likely that we will see more data breaches more often, not less.

Luckily, we are not starting from scratch. In the public sector, the National Institute for Standards in Technology—NIST—spent the past several years developing strategies and frameworks for identity verification under their Trusted Identities Group—TIG.

As a part of this work, NIST’s TIG has provided funding to pilot programs looking to develop, implement, and leverage innovative new technologies that move organizations beyond KBA.

Similarly, in the private sector, many companies and organizations from a wide variety of sectors have come together to create the Fast Identities Online, or FIDO, Alliance.

The FIDO Alliance provides a forum for collaboration and co-operation around the development of standards-based interoperable technologies. These standards are freely available and already deployed in the products of companies like Google and PayPal.

Our witnesses today will not only help us understand the cumulative impact of the dozens of data breaches that have occurred in recent years go also assess how current practices can and should be improved to protect consumers and their information and how it’s been breached.

Today’s hearing is the start of what I expect will be a much longer conversation. But it’s a necessary conversation to have as our world becomes ever more connected. Identity verification is a challenge that will only continue to grow.

[The prepared statement of Mr. Griffith follows:]

PREPARED STATEMENT OF HON. H. MORGAN GRIFFITH

We are here today to talk about a very important topic: identity verification in a post-breach world. This hearing is especially timely given several events that have taken place since the hearing itself was announced last week, including three newly disclosed data breaches that compromised an additional 58.7 million records, as well as two major shopping days, Black Friday and Cyber Monday. With consumers rushing to take advantage of holiday sales, both in stores and online, the questions and challenges around modern identity verification become even more pressing.

Data breaches have been an increasing problem over the last several years. In fact, it is likely that everyone in this room has had their information included in a recent breach. Between the 57 million accounts compromised in Uber’s recently disclosed 2016 breach, the 145 million accounts compromised in Equifax’s breach,

or the 22 million accounts compromised in the OPM breach, as well as many others, I would argue that it would be difficult to find an American whose information has not been compromised.

While these breaches themselves are troubling enough, they also raise a subtle, more complicated series of questions and issues around the ways in which organizations, including government agencies, banks, healthcare organizations, and retail companies perform identity verification of their citizens and customers.

It's a well understood concept that, to quote the famous cartoon, on the Internet nobody knows you're a dog. This anonymity has many advantages, and is important to many aspects of the modern Internet. However, as the global economy has become more and more digital, and an increasing amount of commerce takes place online, it also creates significant challenges for organizations attempting to ensure that they provide information and services only to authorized individuals. Because these interactions usually take place on opposite ends of an Internet connection, with participants rarely meeting face to face, the ability of organizations to remotely verify individuals has been a constant struggle.

As a result, for years, many organizations have relied on a type of identity verification known as "Knowledge-Based Authentication" or "KBA." We are all familiar with this process, even if we don't quite know it. For example, some online accounts ask consumers to provide answers to "security questions" such as their mother's maiden name, the make and model of their first car, or the street on which they grew up. Similarly, when consumers attempt to open new credit lines, they are often asked a series of multiple-choice questions that may ask who provided a consumer a loan, and in what year. These are all examples of KBA.

The effectiveness of KBA depends on a very important assumption—that information such as birthdays, mother's maiden names, addresses, work histories, and other KBA attributes remain relatively secret. In today's post-breach world, this is a tenuous assumption. Add the wealth of personal information consumers' voluntarily share about their lives through social media and this assumption appears almost laughable.

So what do we do? If modern commerce and many other services, including government services, rely on KBA for identity verification, and that verification is no longer as secure or reliable as it was in the past, we need new strategies and new technologies to ensure that consumers are protected, and economic growth continues. And we need them quickly; with the exponential growth of connected devices and services, it is likely that we will see more data breaches more often, not less.

Luckily, we are not starting from scratch. In the public sector, the National Institute for Standards and Technology (NIST) spent the past several years developing strategies and frameworks for identity verification under their Trusted Identities Group (TIG). As part of this work, NIST's TIG has provided funding to pilot programs looking to develop, implement, and leverage innovative new technologies that move organizations beyond KBA.

Similarly, in the private sector, many companies and organizations from a wide variety of sectors have come together to create the Fast Identities Online, or FIDO, Alliance. The FIDO Alliance provides a forum for collaboration and cooperation around the development of standards-based, interoperable technologies. These standards are freely available and already deployed in the products of companies like Google and PayPal.

Our witnesses today will not only help us understand the cumulative impact of the dozens of data breaches that have occurred in recent years, but also assess how current practices can and should be improved to protect consumers after their information has been breached.

Today's hearing is the start of what I expect will be a much longer conversation. But it's a necessary conversation to have. As our world becomes ever more connected, identity verification is a challenge that will only continue to grow.

Thank you, and I yield back and now recognize Ms. Castor of Florida for an opening statement.

OPENING STATEMENT OF HON. KATHY CASTOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Ms. CASTOR. Well, thank you, Mr. Chairman, and thank you for calling this hearing.

Mr. Chairman, data breaches are compromising the personal information of millions of Americans. The Equifax breach earlier this

year, for example, exposed the personal information including names, Social Security numbers, birth dates, addresses, and other sensitive data of as many as 145 million Americans.

And there have been many more—Yahoo, JPMorgan Chase, eBay, Uber. We simply cannot accept this as standard operating procedure. When companies like Equifax, Yahoo, and Uber fail to protect the vast information they collect about consumers, it poses very serious risks.

It's not limited to private corporations. Governmental entities have also failed to adequately protect personal private data.

But with each data breach after each data breach, compromising more and more of consumers' personal information, we have got to ask how do we ensure an online identity can be verified only by the person in question.

I also think it's important that we not forget that companies should be held accountable when they fail to protect our data.

The Equifax breach exposed the personal information of nearly half of the American population and it could have been prevented by applying basic security standards.

So what is the recourse? What is the appropriate recourse? I know that experts are working to develop methods to better protect online identities and I would like to hear what your recommended solutions are.

Under President Obama, the White House released the National Strategy for Trusted Identities in Cyberspace. It's a framework for public and private collaboration on protecting digital identities and improving online transactions.

So building on that effort, companies have begun experimenting with ways to improve identity verification and authentication.

I would like to hear about some of these solutions as well as what we can do to protect consumers' privacy. As more and more of our lives are online, it is equally important that we ensure that these systems are secure and that the ways in which we access these systems are protected.

I would like to thank our witnesses—Mr. Jeremy Grant, Mr. Troy Hunt, Mr. Ed Mierzwinski—for coming today to discuss the principles and various challenges in verifying online identities.

Each of you brings a wealth of knowledge and experience to this hearing and it's a pleasure to have you here today. Thank you, and I yield back.

Mr. GRIFFITH. I thank the gentlelady.

I now recognize the chairman of the full committee, Mr. Walden of Oregon.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. I thank the chairman, and we appreciate your leadership on this and so many other issues, and we want to thank the witnesses for being here today.

We have another hearing going on downstairs on the anniversary of the 21st Century Cures legislation so I am bouncing back and forth today.

Today's hearing is about the future of digital commerce, as we all know, and it's about the future of how we ensure the person on

the other end of an online transaction is in fact the person they claim to be. What a concept.

For years, we have relied on user names, passwords, and knowledge-based questions to confirm a user's identity. It's not a particularly sophisticated process. Your mother's maiden name or the make and model of your first car aren't exactly reliable forms of verification.

Regardless, this process was suitable for a period of time in the evolution of our connected world but that time has long since passed, as we all know.

As noted by one of our witnesses today, it was almost a decade ago that the 2008 Commission on Cybersecurity for the 44th presidency highlighted identity as a frequent attack vector for cyberattacks.

This prompted the previous administration to launch the National Strategy for Trusted Identities in Cyberspace, or NSTIC.

As we will hear today, this high-level Federal attention encouraged the progress but we still have a long ways to go.

How far? Well, according to Verizon's annual data breach investigation report, about 80 percent of breaches last year used identity as a point of compromise—80 percent.

What has changed to make existing identity management practices so ineffectual and vulnerable to attack? There are a number of factors at play but the underlying answer is fairly simple.

Today, the information necessary to compromise identity is readily available to those who wish to find it. We live in a post-breach world. Just look at the massive breaches that have occurred over the last several from Target and Home Depot to Yahoo, Anthem, OPM, Equifax and, most recently, Uber, to name a few.

I would be surprised if anyone in this room has not had at least some portion of their personal details stolen in the last 2 years, let alone their digital lifetime.

I remember a former colleague from Michigan who chaired the Intelligence Committee, Mike Rogers, used to say there are two types of companies in America—those that know they've been breached and those that don't.

It is not, however, just stolen data that undermines current identity verification practices. The explosion of social media is also a factor.

Every day, consumers voluntarily post, tweet, and share details about their lives, adding to the rich data set of information available to malicious actors.

One of our witnesses, Mr. Hunt, is a global expert on these issues and that's why your testimony is so very valuable to our work, especially on how bad actors can compromise identity through the collection of personal information and data that already exists in the digital universe.

He endured a 27-hour journey to be here, I am told, and I suspect his testimony will be illuminating for all of us. I thought I had a long trip back and forth to the West coast every week.

We can no longer ignore the current reality. Whether through theft or voluntary disclosure, our information is out there and this is not likely to change.

Social media will continue to grow. Social, cultural, and economic benefits are just too great for it not to. Likewise, digital commerce and online transactions are integral to our economic prosperity both now and in the future.

As our lives become increasingly entwined in the digital—with the digital space, this must come with an acceptance that our information will always be at risk.

Such is the nature of the cyber threat we face and there is no perfect security in the connected world. But that makes it even more important that we find ways to reduce vulnerabilities in our digital ecosystem.

Clearly, identity is one of those weaknesses. So therefore, I look forward to the work this committee is doing and the testimony you all have submitted to us and the policies that will develop, moving forward.

With that, Mr. Chairman, I yield back the balance of my time and, again, thank our witnesses for being here and, as I said, I've got a couple of these I have to bounce between. But we appreciate the work you're doing.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Today's hearing is about the future of digital commerce. It is about the future of how we ensure the person on the other end of an online transaction is, in fact, the person they claim to be. For years, we have relied on user names, passwords and knowledge-based questions to confirm a user's identity. It's not a particularly sophisticated process—your mother's maiden name, or the make and model of your first car aren't exactly reliable forms of verification.

Regardless, this process was suitable for a period of time in the evolution of our connected world—but that time has long-since passed. As noted by one of our witnesses, it was almost a decade ago that the 2008 Commission on Cybersecurity for the 44th Presidency highlighted identity as frequent attack vector for cyberattacks.

This prompted the previous administration to launch the National Strategy for Trusted Identities in Cyberspace [N-STIC]. As we will hear today, this high-level Federal attention encouraged some progress but we have a long way to go. How far? Well, according to Verizon's annual Data Breach Investigation Report, more than 80 percent of breaches last year used identity as a point of compromise.

What has changed to make existing identity management practices so ineffectual and vulnerable to attack? There are a number of factors at play but the underlying answer is fairly simple—today, the information necessary to compromise identity is readily available to those who wish to find it.

We live in a post-breach world. Just look at the massive breaches that have occurred over the last several years from Target and Home Depot to Yahoo, Anthem, OPM, Equifax and most recently Uber—to name a few. I would be surprised if anyone in this room has not had at least some portion of their personal details stolen in the last 2 years, let alone through their digital lifetime.

It is not, however, just stolen data that undermines current identity verification practices. The explosion of social media is also a factor. Every day consumers voluntarily post, tweet, and share details about their lives—adding to the rich data set of information available to malicious actors.

One of our witnesses, Mr. Hunt, is a global expert on these issues—especially how bad actors can compromise identity through the collection of personal information and data that already exists in the digital universe. He endured a 27-hour journey to be here today and I suspect his testimony will be illuminating for all of us.

We can no longer ignore the current reality. Whether through theft, or voluntary disclosure, our information is out there. And this is not likely to change. Social media will continue to grow—the social, cultural and economic benefits are too great. Likewise, digital commerce and online transactions are integral to our economic prosperity—both now and in the future. As our lives become increasingly entwined with the digital space, this must come with an acceptance that our information will always be at risk.

Such is the nature of the cyber threat. There is no perfect security in the connected world, but that makes it even more important that we find ways to reduce vulnerabilities in our digital ecosystem. Clearly, identity is one of those weaknesses and I look forward hearing from all our witnesses about what options exist to address this challenge.

Mr. GRIFFITH. Thank you, Mr. Chairman. I appreciate that.

I will tell you that Mr. Hunt not only sacrificed with the 27-hour flight to get here but also put on a suit and tie for us where he normally wears jeans and a black T-shirt, according, at least, to his comments on the internet.

[Laughter.]

Mr. GRIFFITH. But anyway—

Mr. WALDEN. I was starting to wonder if it's actually him or a stolen identity before that. But I don't know. Thank you.

Mr. GRIFFITH. Anyway, thank you, Mr. Chairman.

At this point, I would ask—oh, I would recognize Mr. Pallone of New Jersey for an opening statement. Glad you made it. Thank you.

Mr. PALLONE. Thank you, Mr. Chairman.

I want to—I have actually got the wrong statement here from the other committee.

Mr. GRIFFITH. We will give you a minute. We have explained to everybody that we have two hearings going on at the same time and that folks are having to bounce back and forth so—

Mr. PALLONE. All right.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

So let me, again, thank you, Mr. Chairman.

So much of our lives today is linked to what we do online and companies in virtually every sector of the economy collect vast amounts of personal data about consumers, and these companies know they are targets for malicious attacks and all too often they fail to protect the valuable consumer information they collect and store.

For example, recently the ride service company Uber revealed that it had been hacked more than a year ago, and this breach reportedly exposed the personal information of 57 million riders and drivers.

This security breach is yet another example of a company that failed to protect the data of its customers and then failed to come clean about their security breach, in this case for more than a year.

Then there was the Equifax data breach which compromised the personal data of more than 145 million Americans, and what's worse, the Equifax breach compromised personal data like Social Security numbers and birth dates that are difficult or impossible to change.

And consumers affected by the Equifax breach are vulnerable, particularly because these identity verifiers can give someone access to other sensitive information.

The committee is still waiting for answers to questions we asked Equifax both before and after our hearing on the breach and, obviously, that's unacceptable so, hopefully, we will get answers.

It's also unacceptable to the American people because when companies fail to protect consumer data consumers pay the price, sometimes years after a breach.

So as data breaches continue to compromise our personal information, it's important that we explore how consumers and the holders of consumer information can verify that individuals are who they say they are online.

For example, how many times has each of us been asked to provide the last four digits of our Social Security number to get access to other information?

But how do we protect consumers' digital identities, especially after the Equifax data breach exposed the Social Security numbers of nearly half the U.S. population.

And as companies suggest that they may move to behavioral and biometric verifiers, are we comfortable with how much more personal information will be collected and used?

Are we comfortable with trusting that companies will keep this data secure? And these are important questions now facing the world of digital commerce.

According to the Identity Theft Resource Center, as many as 1,190 data breaches have occurred so far this year. Any data breach exacerbates the issues the public is facing in verifying their identities and authenticating access online.

Hackers and other malicious actors erode the trust we have online by using the data they've been able to glean about each and every one of us, and that's not good for business and it's certainly not good for consumers.

So, again, I just want to thank our witnesses for being here today to discuss the latest in identity verification and the challenges of protecting people's data and I believe that unless we act and pass meaningful legislation we will continue to see more data breaches and the unfortunate ripple effects that result from them.

I don't know if—you don't want to add anything? All right. I yield back, Mr. Chairman.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

Thank you, Mr. Chairman. So much of our lives today are online. Companies in virtually every sector of the economy collect vast amounts of personal data about consumers. These companies know they are targets for malicious attacks, and all too often, they fail to protect the valuable consumer information they collect and store.

Just this past week for example, the ride service company, Uber, revealed that it had been hacked—more than a year ago. This breach reportedly exposed the personal information of 57 million riders and drivers. This security breach is yet another example of a company that failed to protect the data of its customers, and then failed to come clean about their security breach—in this case for more than a year.

Then there was the Equifax data breach, which compromised the personal data of more than 145 million Americans. What's worse, the Equifax breach compromised personal data like Social Security numbers and birth dates that are difficult or impossible to change.

Consumers affected by the Equifax breach are vulnerable—particularly because these identity verifiers can give someone access to other sensitive information. This committee is still waiting for answers to questions we asked Equifax both before and after our hearing on the breach. This is unacceptable.

This is also unacceptable to the American people because when companies fail to protect consumer data, consumers pay the price—sometimes years after a breach.

As data breaches continue to compromise our personal information, it is important that we explore how consumers and the holders of consumer information can verify that individuals are who they say they are online.

For example, how many times has each of us been asked to provide the last four digits of our Social Security number to get access to other information? But how do we protect consumers' digital identities, especially after the Equifax data breach exposed the Social Security numbers of nearly half the U.S. population?

And as companies suggest that they may move to behavioral and biometric verifiers, are we comfortable with how much more personal information will be collected and used? Are we comfortable with trusting that companies will keep this data secure? These are important questions now facing the world of digital commerce. According to the Identity Theft Resource Center, as many as 1,190 data breaches have occurred so far this year.

Any data breach exacerbates the issues the public is facing in verifying their identities and authenticating access online. Hackers and other malicious actors erode the trust we have online by using the data they have been able to glean about each and every one of us. That's not good for business, and it's certainly not good for consumers.

I want to thank our witnesses for being here today to discuss the latest in identity verification and the challenges of protecting people's data. I believe that unless we act and pass meaningful legislation, we'll continue to see more data breaches and the unfortunate ripple effects resulting from them.

Thank you, and I yield back.

Mr. GRIFFITH. Thank you very much for yielding back. I appreciate that, Ranking Member.

With that being said, I would now ask for unanimous consent that the Members' written opening statements be made a part of the record. Without objection, they will be so entered.

I would now like to introduce our panel of witnesses for today's hearing and appreciate all of you being here.

First, we have Mr. Troy Hunt, the information security author and instructor for Pluralsight. Next is Mr. Jeremy Grant, who serves as the managing director of Technology Business Strategy at Venable. And finally, we have Mr. Ed Mierzwinski, who is the consumer program director at U.S. PIRG, or PIRG.

Thank you all for being here today, and I look forward to your testimony and we appreciate you providing that testimony. We look forward to the opportunity to discuss identity verification with you all.

As you all are aware, the committee is holding an investigative hearing and when doing so it is the practice of this committee—this subcommittee of taking that testimony under oath.

Do any of you have an objection to testifying under oath?

Seeing none, the Chair then advises you that under the rules of the House and the rules of this committee, you are entitled to be accompanied by counsel.

Do any of you desire to be accompanied by counsel during your testimony today?

Seeing no request for counsel, in that case would you please rise and raise your right hand, and I will swear you in.

[Witnesses sworn.]

Seeing affirmative answers from all, you are now under oath and subject to the penalties set forth in Title 18 Section 1001 of the United States Code.

You may now give a 5-minute summary of your written statement, and we will begin with you, Mr. Hunt.

Thank you so much for being here. You have 5 minutes.

STATEMENTS OF TROY HUNT, INFORMATION SECURITY AUTHOR AND INSTRUCTOR, PLURALSIGHT; JEREMY GRANT, MANAGING DIRECTOR, TECHNOLOGY BUSINESS STRATEGY, VENABLE, LLP; AND EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PIRG

STATEMENT OF TROY HUNT

Mr. HUNT. Vice Chairman Griffith, Ms. Castor, and distinguished members of the House Energy and Commerce Committee, thank you for the opportunity to testify today.

My name is Troy Hunt. I am an independent information security author and instructor for Pluralsight. I am also the creator of data breach notification service known as Have I Been Pwned.

In my time running this service, I've analyzed hundreds of individual data breaches containing many billions of records, and I've observed firsthand both the alarming increase in incidents and, indeed, the impact they are having on people's lives.

This testimony draws on my experiences running the service and describes the challenges we are now facing in a time where data breaches have become the new normal.

When we talk about data breaches, we are really talking about a range of different types of events that can lead to the exposure of our personal information.

We typically think of malicious actors exploiting vulnerabilities and protected systems and, indeed, that's an enormous prevalent and alarming situation.

But increasingly we also see data breaches occur as a result of simple human error. For example, accidentally publishing data to an unprotected publicly facing server where it's then discovered by intended parties.

We have a perfect storm of factors that are causing both the frequency and scale of these incidents to accelerate. Cloud services have made it easier than ever to publish data publicly, and that has helped to drive the expansion of other online services, which have in turn increased the overall attack surface of the internet.

At the same time, we have the rapidly growing internet of things, collecting classes of data we simply never had digitized in the past and, increasingly, we are seeing that information appear in data breaches, too.

Organizational attitudes to our personal information lead to data maximization. That is a desire to collect as much of it as possible, often well beyond the scope of what is actually needed by the service it's being provided to.

Frequently, this is without informed consent, particular by the likes of data aggregators and, indeed, we have seen them suffer data breaches, too, both here in the U.S. and overseas.

Now, data is viewed as an asset yet organizations fail to recognize that it is also a liability. Exacerbating exposure of data is a rampant trading scene. Data is not only sold for profit but regularly exchanged by individuals building personal collections.

I liken it to kids exchanging baseball cards, except that unlike trading a physical commodity, the exchange of data breaches is more like making a photocopy, as the original version still exists.

Once it enters circulation, it is impossible to contain it. The data breach genie is out of the bottle. We are also learning how much we don't know as significant data breaches that occurred years ago come to light.

We have no idea how many more unknown incidents are out there, and not only do we not know which organizations have lost their data and are unaware of it themselves, we don't know which ones are deliberately concealing data breaches.

There is a lack of accountability when a breach does occur. We know this because very little changes in the industry afterwards.

We constantly see large data breaches and people ask, will this be the watershed moment where we start taking these breaches more seriously.

Yet, nothing changes and we merely repeat the same discussion after the next incident. We are also disclosing large amounts of personal data of our own free will, such as our date of birth, by social media.

We think nothing of it because a growing proportion of the population has never known a time where we didn't do this. They are the internet natives that have grown up in an environment of personal information sharing.

Consider the impact on knowledge-based authentication, the very premise that there is information that you know that is sufficient to prove your identity. That same information is increasingly public.

My dad recently had some help setting up a new broadband connection, and after calling up the provider the first thing they asked him was his date of birth. That's the same personal attribute I had exposed after I donated blood and that subsequently appeared in a data breach.

And that is really the challenge we have today, the premise of authenticating one's self with information that only they should know, yet is increasingly in the public domain.

That worked years ago when information was contained in a small number of silos, but that's not the world we live in today. And consequently, our assumption about who knows what has to change accordingly in the age of the data breach.

Thank you very much.

[The prepared statement of Mr. Hunt follows:]

Statement of Troy Hunt

For the House Committee on Energy and Commerce

“Identity Verification in a Post-Breach World”

30 November 2017

Summary

1. Data breaches occur via a variety of different “vectors” including malicious activity by attackers exploiting vulnerabilities, misconfiguration and behalf of system owners and software products intentionally exposing data by design.
2. There is frequently a long lead-time (sometimes many years) between a data breach and the service owner (and those in the breach) learning of the incident. We have no idea of how many incidents have already occurred but are yet to come to light.
3. The industry has created a “perfect storm” for data exposure. The rapid emergence of cheap, easily accessible cloud services has accelerated the growth of other online services collecting data. Further to that, the rapidly emerging “Internet of Things” is enabling us to digitise all new classes of information thus exposing them to the risk of a data breach.
4. An attitude of “data maximisation” is causing services to request extensive personal information well beyond the scope of what is needed to provide that service. That data is usually then retained for perpetuity thus adding to an individual’s overall risk.
5. Lack of accountability means that even in the wake of serious breaches, very little changes in the industry and we continually see other organisations repeat the same mistakes as their peers.
6. Data breaches are redistributed *extensively*. There’s an active trading scene exchanging data both for monetary gain and simply as a hobby; people collect (and thus replicate) breaches.
7. Many of the personal data attributes exposed in breaches cannot be changed once in the public domain, nor can these breaches be “scrubbed” from the internet once circulating.
8. Even without data breaches, we’re willingly exposing a huge amount of personal information publicly via platforms such as social media.
9. The prevalence with which our personal data is exposed has a fundamental impact on the viability of knowledge based authentication. Knowledge which was once personal and could be relied upon to verify an individual’s identity, is now frequently public knowledge.

Opening

Vice Chairman Griffith, Ranking Member DeGette, and distinguished Members of the House Energy and Commerce Committee, thank you for the opportunity to testify.

My name is Troy Hunt. I'm an independent Australian Information Security Author and Instructor for Pluralsight, an online learning platform for technology and cybersecurity professionals. I'm commissioned on a course-by-course basis to create training material that has been viewed by hundreds of thousands of students over the last 5 years. I'm also a Microsoft Regional Director (RD) and Most Valuable Professional (MVP), both titles of recognition rather than permanent roles. I've been building software for the web since 1995 and specialising in online security since 2010.

Of particular relevance to this testimony is my experience running the data breach notification service known as Have I Been Pwned (HIBP). As a security researcher, in my analysis of data breaches I found that few people were aware of their total exposure via these incidents. More specifically, I found that many people were unaware of their exposure across *multiple* incidents (one person appearing in more than 1 data breach) and indeed many people were unaware of *any* exposure whatsoever. In December of 2013, I launched HIBP as a freely accessible service to help people understand their exposure. Over the last 4 years, the volume of data in the service has grown to cover more than 250 separate incidents and over 4.8 billion records. What follows are insights drawn largely from running this service including the interactions I've had with companies that have been breached, those who have had their personal data exposed (myself included) and law enforcement in various jurisdictions around the world.

Data Breach Vectors

Data breaches have become a fact of modern digital life. Our desire to convert every aspect of our beings into electronic records has delivered both wonderful societal advances and unprecedented privacy risks. It's an unfortunate yet unavoidable reality that the two are inextricably linked and what follows describes the risks we are now facing as a result.

The term “data breach” is used broadly to refer to many different discrete vectors by which data is exposed to unauthorised parties. Some are as a result of malicious intent, some occur due to unintentional errors and yet others are inadvertent by-products of software design; they’re “features”, if you will.

Malicious incidents are the events we immediately associate with the term “data breach”. In this case, a “threat actor” has deliberately set out to gain unauthorised access to a protected system, often with the intention of causing harm to the organisation and their subscribers. We frequently see successful attacks mounted through exploitation of very well-known vulnerabilities with equally well-known defences. They exploit flaws in our software design, our security measures and indeed our human processes. They may be as sophisticated as leveraging previously unknown flaws or “zero days”, yet they’re frequently as simple as exploiting basic human shortcomings such as our propensity to choose poor passwords (and then to regularly reuse them across multiple services).

Especially in recent years with the growing ubiquity of easily accessible cloud services, data breaches often take the form of unintentionally exposed data. The ease today with which a publicly facing service can be provisioned and large volumes of data published to it is unprecedented – it can take mere minutes. Equally unprecedented is the simplicity with which an otherwise secure environment can be exposed to the masses; a single firewall setting or a simple access control change performed in mere seconds is all it takes.

The very design of some online services predisposes them to revealing large volumes of data about their subscriber base. Particularly in systems intended to make people discoverable such as social media or dating sites, we’ve seen many precedents of large volumes of publicly accessible information collated in an automated fashion in order to build a rich dataset. Some may be reluctant to even call this a “data breach”, yet the end result is largely consistent with the previous two examples of malicious intent and unintentionally disclosed data.

We Often Don't Know Until Years Later

We simply have no idea of the scale of data that has been breached. We can measure what we know and conclude that there's an alarmingly large amount of personal information having been exposed, but it's the extent of the "unknown unknowns" that is particularly worrying.

Increasingly, we're realising the significance of the problem. During 2016 and 2017 in particular, we saw many incidents where large data sets belonging to well-known brands appeared after having been originally obtained years earlier. These incidents were frequently of a scale numbering in the millions, tens of millions or even hundreds of millions of customers. In some cases, the organisations involved were aware of a successful attack yet consciously elected not to disclose the incident. Many of the recent large breaches involved companies that *were* aware of unauthorised access to their systems, yet the scope of the intrusion was not known until years later when large volumes of data appeared in the public domain. In other cases, intrusions were entirely unknown until the organisation's data appeared publicly.

I've been personally involved in the disclosure of multiple incidents of this nature directly to the organisations involved. They're consistently shocked – *shocked* – that a breach had taken place and had not seen prior indicators that their data may have fallen into unauthorised hands. The passage of time frequently means that root cause analysis isn't feasible and indeed many of these systems have been fundamentally rearchitected since the original event.

It begs the questions – how much more data is out there? And what are we yet to see from events that have already occurred? We simply don't know nor is there any feasible way of measuring it. The only thing I can say with any certainty is that there is still a significant amount of data out there that we're yet to learn of.

A Perfect Storm of Data Exposure

Data breaches have been increasing in regularity and the incidents themselves have been increasing in terms of the volume of records impacted. There are a variety of factors contributing to what can only be described as a “perfect storm” of data exposure:

Firstly, as mentioned above, the rapid emergence of cloud services has enabled organisations and individuals alike to publish data publicly with unprecedented ease, speed and cost efficiency. The low barrier to entry has meant that it’s never been easier to collect and store huge volumes of information and very little technical expertise is required to do so.

Then we have the ever-increasing array of online services collecting data; social media sites, e-commerce, education, even cooking – every conceivable area of human interest has an expanding array of online services. In turn, these services request personal information in order to subscribe or comment or interact with others. As a result, the number of pools of user data on the internet grows dramatically and so too does the total attack surface of information.

The more recent emergence of the class of device we refer to as the “Internet of Things” or IoT is another factor. We’re now seeing data breaches that expose information we simply never had in digital format until recently. In recent times, we’ve seen security vulnerabilities that have exposed data in cars, household appliances and even toys (both those targeted at children and those designed for consenting adults to use in the bedroom). All internet connected and all leaking data that didn’t even exist in digital form a few years ago.

Data Maximisation as a Feature

Exacerbating both the prevalence and impact of data breaches is a prevailing attitude of “data maximisation”, that is the practice of collecting and retaining as much data as possible. We constantly see this when signing up for services with requests for information that is entirely unnecessary for the function of the service itself. For example, requests for personal attributes such

as date of birth and physical address, both data points that frequently provide no functional benefit to the service.

Further compounding the data maximisation problem is the fact that the retention period of the data usually extends well beyond the period in which the service is used by the owners of the data. (Indeed, even that term – “data ownership” – can be interpreted to mean either the service retaining it or the individuals to whom the data relates.) For example, signing up to an online forum merely to comment on a post means the subscriber’s personal data will usually prevail for the life of the service. There are many precedents of data breaches occurring on sites where those who’ve had their personal data exposed haven’t used the service for many years.

Individuals’ personal data is also frequently collected without their informed consent, that is it’s obtained without them consciously opting in to the service and the purpose for which it’s being used. Our data is aggregated, “enriched” and sold (often entirely legally) as a commodity; the people themselves have become the product and alarmingly, we’re seeing the aggregation services themselves suffering data breaches both in the US and abroad. In this environment, it’s the organisations holding personal data that control it, not the people to whom that data rightfully belongs.

I frequently hear from subscribers of HIBP that they have no recollection of using a service that’s suffered a data breach. The alert they receive after the data is exposed is often the first they’ve heard of the service in many years. In fact, so much time has often passed that they frequently reject the notion that they were members of the site until they discover the welcome email in their archives or perform a password reset and logon to the service. The site was providing zero ongoing value to them yet it still retained their data and subsequently exposed it in a breach.

Data maximisation prevails as a practice for a variety of reasons. One is that it’s increasingly cost effective to simply retain everything possible, once again due to the emergence of cloud services as well as rapidly declining storage costs. Another is that purging old data comes at a cost; this is a

feature that has to be coded and supported. It also creates other challenges around technical constraints such as referential integrity; what happens to records such as comments on a forum when the creator of that comment has their record purged? Organisations view data on their customers as an asset, yet fail to recognise that it may also become a liability.

Attempts by individuals to *reduce* their data footprint often lead to frustration. There's frequently no automated way of purging their own personal information and in some cases, organisations have even imposed a financial barrier in a "user-pays to delete" model. Even then, the purging of data from a live system is unlikely to purge that same data from backups that may stretch back years and we've seen many cases of the backups themselves being exposed in breaches.

We need to move beyond an attitude of data maximisation and instead embrace the mantra of "you cannot lose what you do not have".

There's a Lack of Accountability and a Propensity to Repeat Mistakes

Time and time again, we see serious data breaches that impact people's lives around the world and we ask "Is this the watershed moment?" "Is this the one where we start taking things more seriously?" Yet clearly, nothing fundamental has changed and we merely repeat the same discussion after the next major incident.

There's a lack of accountability across many of the organisations that suffer breaches as they're not held strictly liable for the consequences. Despite the near-daily headline news about major security incidents, there remain fundamental shortcomings in the security posture of most organisations.

They trade off the cost of implementing security controls against the likelihood of a data breach occurring and inevitably, often decide that there's not a sufficient return on investment in further infosec investments. This attitude contributes to both the frequency and severity of serious security incidents and without greater accountability on behalf of the organisations involved, it's hard to see the status quo changing. There's not enough incentive to do things *right* and not enough disincentive to do them *wrong* therefore the pattern repeats.

Data Breach Redistribution is Rampant

An important factor exacerbating the impact of data breaches is the prevalence with which the data is redistributed once exposed. Data breaches often spread well beyond the party that originally obtained it and the ease with which huge volumes of digital information can be replicated across the globe means that once it's exposed, it spreads rapidly.

There are multiple factors driving the spread of data that has been breached from a system. One is commercial incentives; data breaches are often placed for sale in marketplaces and forums where they may be sold many times over. The personal information contained within these breaches poses value to purchasers ranging from the ability to compromise other accounts of the victims' (frequently due to the prevalence of password reuse unlocking other unrelated services) to value contained within the accounts themselves (such as the ability to acquire goods at the victims' expense) through to outright identity theft (the accounts contain data attributes that help attackers impersonate the victim). In short, there is a return on investment for those who pay for data breaches therefore it has created a thriving marketplace.

More worrying though in terms of the spread of data breaches is the prevalence with which they're redistributed amongst individuals. Data breach trading is rampant and I often liken it to the sharing of baseball cards; two people have assets they'd like to exchange so they make a swap. However, unlike a physical commodity, the trading of data breaches replicates the asset as each party retains their original version, just like making a perfectly reproduced photocopy. Most of those involved in the redistribution of this data are either children or young adults, doing so as a hobby. Often, they'll explain it away as a curiosity; they wanted to see if any of their friends (or sometimes, enemies) were involved. Other times they're experimenting with "hash cracking", the exercise of determining the original passwords when a system stores them as cryptographic hashes. They rarely believe there are any adverse consequences as a result of redistributing the data.

The exchange of data breaches is enormously prevalent. Sites hosting hundreds or even thousands of separate incidents are easily discoverable on the internet; there's often terabytes of data simply sitting there available for anyone to download. Forums dedicated to the discussion of data breaches frequently post links to new breaches or old data which may have finally surfaced. These are not hidden, dark web sites, these are easily discoverable mainstream websites.

Exposed Data is (Often) Immutable and (Usually) Irrevocable

Many of the data classes exposed in breaches are immutable, that is they cannot be changed. For example, people's names, their birth dates, security questions such as their mother's maiden name or even the IP address they were using at the time (which can be used to geographically locate them and potentially tie them to other exposed accounts). Other data attributes may be mutable albeit with a high degree of friction; an email address or a physical address, for example. They may both change over time but the effort of doing so is high and it's unlikely to happen merely because that data has been exposed in a breach.

Paradoxically, the data that is most easily changed is frequently the data people are most concerned about. Credit cards, for example, are often referenced in disclosure statements as not having been impacted by a breach yet a combination of fraud protection by banks and the ability to cancel and refund fraudulent transactions whilst issuing a new card means the real-world impact on card holders is frequently limited and short lived.

Exposed passwords are also easily changed and the impact of them falling into unauthorised hands can be minimal, albeit with one major caveat: The prevalence of password reuse means that the exposure of one system can result in the compromise of accounts on totally unrelated systems. But the password itself is readily changed and unlike immutable personal attributes, doing so immediately invalidates its usefulness.

Frequently, I'm asked how someone's data can be removed from the web; they're a victim of a data breach, now how do they retrieve that data and ensure it's no longer in unauthorised hands? In

reality, that's a near impossible objective, exacerbated by the aforementioned redistribution of data breaches. Digital information replicates so quickly and is so difficult to trace once exposed, there's no putting the data breach genie back in the bottle.

The Emerging Prevalence of OSINT Data and the Power of Aggregation

Data available within the public domain is often referred to as "Open Source Intelligence" or OSINT data. OSINT data can be collated from a range of sources including social media, public forums, education facilities and even public government records to name but a few. It's data we either willingly expose ourselves or is made publicly available by design. Often, the owner of the data is not aware of its publicly available presence; they inadvertently published it publicly on a social media platform or had it put on public display without their knowledge by a workplace or school. In isolation, these data points may appear benign yet once aggregated from multiple sources they can expose a huge amount of valuable information about individuals.

Data aggregation – whether it be from OSINT sources alone or combined with data breaches – is enormously powerful as it can result in a very comprehensive personal profile being built. One system may leak an email address and a name in the user interface, another has a data breach and exposes their home address then that's combined with an OSINT source that lists their profile photo and date of birth. Suddenly, many of the ingredients required to identify and indeed impersonate the individual are now readily available.

The Impact on Knowledge-Based Authentication

Knowledge-based authentication (KBA) is predicated on the assumption that an individual holds certain knowledge that can be used to prove their identity. It's assumed that this knowledge is either private or not broadly known thus if the individual can correctly relay it then, with a high degree of confidence, they can prove their identity. KBA is typically dependent on either static or dynamic "secrets" with the former being the immutable data attributes mentioned earlier (date of birth, mother's maiden name, etc.) and the latter being mutable such as a password.

The risks associated with static KBA have changed dramatically in an era of data breaches and an extensive array of OSINT sources. Further to that is the frequency and effectiveness of phishing attacks which provide nefarious parties with yet another avenue of obtaining personal data from unsuspecting victims. In years gone by, personal data attributes used for verification processes had very limited exposure. For example, one's date of birth or mother's maiden name would normally only be known within social circles which in the past, meant people you physically interacted with. A government issued ID was typically only provided to professional services that had limited exposure.

Now, however, the availability of static KBA data has fundamentally changed yet its use for identity verification prevails. The threat landscape has progressed much more rapidly than the authentication controls yet we're still regularly using the same static KBA approaches we did before the extensive array of OSINT sources we have available today and before the age of the data breach.

Closing

Data breaches will continue to grow in both prevalence and size for the foreseeable future. The rate at which we willingly share personal data will also continue to grow, particularly with an increasing proportion of the population being "internet natives" who've not known a time where we *didn't* willingly share information online. Increasingly, the assumption has to be that everything we digitise may one day end up in unauthorised hands and the way we authenticate ourselves must adapt to be resilient to this.

Mr. GRIFFITH. Thank you, Mr. Hunt. I appreciate that, and now recognize Mr. Grant.

STATEMENT OF JEREMY GRANT

Mr. GRANT. Good morning, Vice Chairman Griffith, Ms. Castor, members of the committee. Thank you for the opportunity to discuss identity with you today.

As background, I've worked for more than 20 years in both industry and Government at the intersection of identity and cybersecurity.

In 2011, I was selected to lead the National Strategy for Trusted Identities in Cyberspace, or NSTIC, which was a White House initiative focused on improving security, privacy, choice, and innovation online for better approaches to digital identity.

In that role, I built out what is now the Trusted Identities Group at the National Institute of Standards and Technology and also served as NIST's senior executive advisory 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, though I should note today my testimony represents my views alone.

So let me say up front I'm quite 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 policy makers in the U.S., and at a high level the way that we handle identity in America impacts our security, our privacy, and our liberty.

From an economic standpoint, particularly as we start to move high-value transactions into 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 with their privacy.

When we don't get identity right we enable a great set of attack points for criminals and other adversaries looking to execute attacks in cyberspace and, unfortunately, we have not been doing very well here.

Last year, a whopping 81 percent of hacking attacks were executed by taking advantage of weak or stolen passwords. Eighty-one percent is an enormous number.

It means that it is an anomaly when a breach happens and identity does not provide the attack factors and, as my colleague, Troy, will probably discuss today with his Web site, Have I Been Pwned, there is now billions of compromised usernames and passwords that are out there in the marketplace. It is high time we find a way to kill the password.

Outside of passwords, we have seen adversaries go after massive datasets of Americans in large part so they have an easier time compromising the questions used in identity verification tools like KBA.

This was illustrated quite vividly by the 2015 hack of the IRS' Get My Transcript application 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 that we have used to protect and verify identity.

The recent Equifax breach might 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 there is certainly blame to allocate. But the most important question at this point is, What should Government and industry do about it now?

As I lay out today, I believe the Government is going to need to step up and play a bigger role to help address critical vulnerabilities in our digital identity fabric.

There are five primary areas where Government, working together with the private sector, can help address the weaknesses of first generation identity verification and authentication tools and deliver next-generation solutions that are not only more secure but also better for privacy and consumer experiences.

First, when talking about the future of the Social Security number and whether it needs to be replaced, it is essential for folks to understand the difference between SSN's role as an identifier and its use as an authenticator.

SSN should no longer be used as authenticators but that does not mean we need to replace them as identifiers. Instead, let's just try treating like the widely available numbers that they are.

That means that as a country we stop pretending that knowledge of somebody's Social Security number can actually be used to prove that they are who they claim to be.

Second, along with the SSN let's just recognize how useless passwords have become as a security tool. There is no such thing as a strong password in 2017 and we should stop trying to pretend otherwise.

Third, recognize that it's not all bad news out there. Government and industry have recognized the problem with old authenticators like passwords and SSNs and they've actually been working together the last few years to make strong authentication easier.

Multistakeholder efforts like the FIDO Alliance, which Vice Chairman Griffith mentioned earlier, 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 Government can play a role in helping to drive user adoption.

Fourth, while authentication is getting easier, identity proofing is getting harder as attackers have caught up to first-generation solutions like static KBA.

This might actually be the most impactful area where the Government can help, by allowing consumers to ask agencies that already have their personal information and have validated it, in many cases with an in-person process, to then vouch for them for—with other parties that they seek to do business with.

The Social Security Administration and State Department and Motor Vehicles have the most to offer here, and this is actually a concept that was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity.

Here, the Federal Government should work to develop a framework of standards and rules to make sure this is done in a secure, privacy-enhancing way and look at funding work to get it started.

Finally, technology can help solve the problem but better standards will be needed for companies and agencies to apply it. Further investments in Government research and standards work can go a long way toward making it easier for any party in the public or private sector to implement stronger identity solutions.

I appreciate the opportunity to testify today and look forward to answering your questions.

[The prepared statement of Mr. Grant follows:]

Jeremy Grant
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

“Identity Verification in a Post-Breach World”
November 30, 2017

Vice Chairman Griffith, Ranking Member DeGette and members of the committee, thank you for the opportunity to discuss identity with you today.

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. Note that my testimony today represents my views alone; they are not the views of my firm.

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. Last year, 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. As my colleague Troy Hunt will discuss today, there are billions of compromised usernames and passwords out in the marketplace – his site "Have I Been Pwned" is a great resource to know if your account has been compromised. We need to kill the password.

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 identity. The recent Equifax breach 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?”

I believe 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.”

What has been done to date

Before I get into what government should do, I’d like to talk for a minute about what government has done – particularly over the last few years with the National Strategy for Trusted Identities in Cyberspace (NSTIC) – because there are some notable takeaways from the program that may help to inform where government and industry should focus in 2017 and beyond.

As background, the creation of NSTIC was driven, in part, by a key recommendation from the 2008 Commission on Cybersecurity for the 44th Presidency, which flagged the high prevalence of cyberattacks where identity provided an attack vector and called on the next Administration to take steps to address these issues.

Digital identity is a tricky issue, in that many countries address it through creation of a national ID system – something that we do not have in America for a number of good reasons. However, just because we do not have a national ID does not mean that we do not need a national identity strategy – identity is too challenging an issue, particularly in cyberspace, to solve without some government involvement, and too important to our economy to ignore. The approach the Obama Administration took was to recognize these issues, and craft a uniquely American strategy to tackle digital identity.

When it launched in 2011, NSTIC called for the government to collaborate with the private sector on development of an “identity ecosystem” – essentially a marketplace where all Americans could, in a few years, choose from a variety of different types of digital credentials that they could use everywhere they go online in lieu of passwords, and that would be more secure, convenient and better for privacy.

The role of the government in NSTIC was largely focused on two areas: First, how can government take steps to catalyze the market for NSTIC-aligned identity solutions? And second, are there barriers to better identity solutions that government needs to help remove in order to ensure that a robust identity ecosystem can flourish?

To do this, we focused on four areas:

1. Funding pilots – both to seed the marketplace with new, NSTIC-aligned solutions, as well as to learn what works well and what doesn’t. Some of the most promising solutions to the identity verification challenges we are discussing in this hearing today emerged from these pilots; many of them featured participation from both government entities and the private sector.
2. Working on better standards – to help to measure the effectiveness of different identity technologies, and to make it easier for every stakeholder in the identity ecosystem to make use of these new solutions in the marketplace.
3. Getting US Government applications to embrace better identity solutions – which was helpful not only for purposes of enabling new high-value digital services, but also demonstrating to industry that the government was serious about this topic.

4. Focusing on governance – looking to bring together different stakeholders from the private sector to create a framework of standards and operating rules for the identity ecosystem. Part of that meant sorting out questions such as: What does it mean to be aligned with NSTIC? How would this be measured? And certified?

But above all these activities – the most important thing NSTIC did was having the President sign it. Because by throwing down a marker, the President got everybody's attention.

Companies that loved it came in to ask how they could get our help in making their next generation of identity products align with NSTIC and its vision of better security, privacy and convenience – that was a win for all Americans!

Companies that hated it – and to be clear, there were a few – still had to pay attention to it, and account for it in their product planning and roadmap. Because their customers would ask what they were doing to comply with it.

Six years after the strategy was published, the identity market has made significant progress. In some areas, more than others, however. If there is one takeaway I can offer about the state of the identity market post-NSTIC, 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. 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.

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 some of the tools we have depended on for identity proofing and verification. One example of the ways they have caught up are the terabytes of data that have been stolen through major breaches such as Equifax, which have captured Congress’ attention this fall – and, I assume, led to the Committee calling this hearing.

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 ways to fix the problem – the market has not yet sorted things out here.

The good news is that some of the most promising approaches to better identity proofing emerged from pilots that the government funded through the NSTIC program. The bad news: funding for those pilots has been cut in the 2018 budget, while the challenges in the marketplace are greater than ever.

The history of what has happened to date is important for context setting. But as I stated earlier, the most important question is: “What should government and industry do about it now?”

What should government and industry do about it now?

I believe there are five areas where government can and should engage, and in doing so, can contribute to material improvements in the confidentiality, reliability and integrity of America's identity ecosystem, while also improving privacy and eliminating barriers to digital commerce.

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 weeks. Rather, government should take steps to change how we use it.

There's been a ton of discussion on this topic over the last few weeks as industry and government leaders, along with security and privacy experts, have called for the country to come up with something to replace the SSN in the wake of the Equifax breach.

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 and other data brokers, who have used the SSN as one way to aggregate 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 that 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 2017 — 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, government should start to push companies to stop 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.

However — and this is key — just because SSNs should no longer be used as authenticators does not mean that we need to replace them as identifiers. Instead, let's start treating them like the widely-available numbers that they are.

While it might be tempting to create a new, revocable identifier in response to the overuse (relative to its intended purpose) of the SSN, 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.

Rather than create a new identifier, the focus ought to be on crafting better identity vetting and authentication solutions that are not dependent on the SSN, and are resilient against modern vectors of attack. That tees up my next four recommendations:

2. Along with the SSN, we also need to recognize how useless passwords have become as authenticators. 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 in 2017 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.

The reality is that very few compromises of passwords are executed by “brute force” attacks to crack the password. Instead, attackers either spear-phish someone into entering their password into a phishing site. Or they break into companies that store millions of user-name and password combinations and just steal them outright. In either case, it does

not matter whether a password has four characters or 24. Even the most complex password is still a “shared secret” that is easily compromised in 2017.

Beyond passwords: the problems with shared secrets extend well beyond passwords to also make other forms of first-generation multi-factor authentication (MFA) vulnerable. For example, “one time password” (OTP) technology – which generates a time-limited login code that is good for only 30 seconds – used to provide excellent protection against many attacks on passwords. But in 2017 the attackers have caught up – that 30 seconds is enough to phish or compromise an OTP. It is still a shared secret that both the user and the service provider know – and that creates routes for compromise.

The same issues apply to authentication codes delivered by text message, for example, using SMS. In addition to being phishable, malware can redirect text messages away from the intended device, including MFA codes. We have also seen attacks on the mobile network itself – attacking the SS7 protocol – to intercept MFA codes. And we’re increasingly seeing mobile phone account hijacking (aka “SIM swap”) attacks – taking over someone’s phone account via social engineering, with the goal of stealing these codes.

The bottom line: these days, most attackers can successfully phish MFA based on shared secrets just about as easily as they can a password. The government needs to make it a priority to move the market to modern, unphishable authentication.

3. 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 efforts like the FIDO Alliance 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 a 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, and 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 to securely log the consumer in, without a password or any other shared secret.

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 standards. The power of FIDO 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. Major firms like Aetna, PayPal, Google, Microsoft, Bank of

America, Intel, USAA and Samsung are among those enabling consumers to lock down their login with FIDO authentication; the Department of Veterans Affairs recently enabled Veterans logging into the Vets.gov website to protect their accounts with FIDO as well.

Government can play a role in accelerating the pace – first by enabling FIDO standards to be used in more of its own online applications. And second, through the regulatory process, by ensuring 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.

4. As I mentioned earlier: while authentication is getting easier, identity proofing is getting harder, as attackers have caught up to first-generation solutions like static Knowledge Based Verification (KBV). Adversaries have targeted massive data-sets of Americans, in part, so that they have an easier time compromising the questions used in “identity proofing” tools like KBV.

A notable challenge here is that KBV has been the de-facto standard for years, and while industry understands it’s time to move to something better, the market has not yet – in my view – developed the logical successor. One reason: industry cannot do this alone. They need the government’s help.

Providing this help may be the single most meaningful thing government can do to improve identity. Government can do so through a relatively simple approach: allowing consumers to ask agencies that have their personal information to vouch for them. Let me detail what I mean:

While we do not have a national ID, most Americans have at least one government-issued identity document:

- At birth, you are issued a birth certificate, from the city or county you are born in.
- Also at birth, you are issued a Social Security Number from the Federal government.
- At or around 16, state governments issue a driver's license or state ID card – which, thanks to the Real ID Act of 2005, now requires an incredibly rigorous identity proofing process.
- If you travel outside the US, you go to the US Postal Service to apply for a passport or passport card – which is then manufactured by the US Government Publishing Office and issued by the State Department.
- If you go overseas a lot – as I do – you may go to DHS to enroll in the Global Entry program – getting another ID card.

That's five government-issued credentials that I have today – but all of them are stuck in the physical world.

Meanwhile, this past February when I went to open up a new bank account – to take out a loan – I had to appear in person at the bank so that they could validate my identity. The highly sophisticated process entailed me showing them my driver's license so they could ascertain if it looked real.

Which – in 2017 – seemed a bit ridiculous. I would have much preferred to simply log into the DC DMV with my FIDO security key and asked them to let my bank know who I was – in this case by sharing several attributes about me that the DMV had already validated. But that sort of system does not exist today in the United States.

If it did, it could solve many of our problems with identity verification in a post-breach world.

In 2017, consumers ought to be able to ask agencies that have their personal information to provide validated attributes about themselves to parties they seek to do business with. The Social Security Administration at the Federal level and Departments of Motor Vehicles (DMV) at the state level have the most to offer here.

- The Social Security Administration could make a significant dent in identity fraud by setting up a simple service to electronically verify that there really is a “Jeremy Grant” with a SSN and date of birth that corresponds to my name. The lack of such a service makes it much easier today for criminals to set up fraudulent accounts with “synthetic identities” using a fake name and a real SSN – often the SSN of a child. Note that SSA offers a paper-based version of this service today – the Consent Based Social Security Number Verification (CBSV) Service – but requires that the requester provides a physical signature on paper from the applicant. In era where most everything is digital, this requirement, for all purposes, precludes this service from being used for real-time identity proofing. It’s time to change that. Note that the CBSV is not tied to SSN’s use as an authenticator, only as an identifier – it is used only to verify that a person actually

exists. Making the system digital could lower the cost of digital transactions and close off a loophole that is commonly exploited by criminals to steal identities and fund illicit activities.

- And in the states, the DMVs could help to pave the way for easier account openings that are more convenient and more secure. State DMVs already put people through a rigorous, in-person identity proofing process today – consumers should be able to leverage the fact that they went through this costly, time-consuming process to avoid having to go through similar hassles for other transactions.

Note that this concept was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity, 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 last December’s report¹:

“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

¹ <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>

set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes."

To date, I do not believe that the Trump Administration has acted on this recommendation. But I believe they should, with a particular focus on having the Federal government 1) lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-enhancing way and 2) fund work to get it started.

Note that some work was done in the previous Administration on this – the NSTIC program funded DMV-focused pilots in states including Virginia, North Carolina, Georgia, Colorado, Idaho, Maryland and Washington DC. The learnings from these pilots² should be leveraged to jumpstart the Commission's recommendation, with a particular focus on making sure such a system places the consumer and his or her rights and needs at the center of any new service. Since these services involve consumers' personal information – let's architect systems that are designed to put the consumer in control!

Toward that end, NSTIC also worked with industry to set up a privately-led Identity Ecosystem Steering Group (IDESG)³ tasked with creating a framework of standards, requirements and best practices for modern, user-centric identity systems. This framework has been used in the state NSTIC pilots, and can serve as a guidepost for any future government offering here.

² See <https://www.nist.gov/itl/tig/pilots>

³ More details at <https://www.idesg.org/>

5. Finally, government needs to support continued work on identity research and standards.

When I look at the positive impacts of NSTIC, one of the top items has been the emergence of a robust Trusted Identities Group in NIST's Information Technology Lab (ITL), focused on working with government and industry to develop better standards, guidelines and best practices for next-generation identity solutions. The publication of NIST's updated "Digital Identity Guidelines" this past summer is one example of the great work that NIST has done here⁴ – it's a document that has been nearly universally praised around the world in taking a forward-thinking approach to digital identity.

Unfortunately, the FY 2018 budget proposed to cut funding for research and standards work in NIST's Trusted Identities Group, singling out NIST's work on biometrics for commercial and government applications.

From my perspective, this is an awful decision. Biometrics – if applied properly – offer one of the most promising tools to improving identity solutions. But the technologies on the market today vary widely in accuracy and reliability. Moreover, some ways in which biometrics can be deployed can enhance security and privacy, while other models present material security and privacy risks. If we're worried about "Identity Verification in a Post-Breach World," government should be increasing the government's budget for research as well as development of better standards and best practices in this area, not cut it back. The FY18 budget cut funding for what is literally the one office in government

⁴ See <https://pages.nist.gov/800-63-3/>

that is tasked with working with industry on tools that can improve the reliability, security and privacy of biometrics and other next-generation authentication technologies.

In closing, America faces challenges at the intersection of identity and cybersecurity – but we also have some actionable ideas that we can implement to address these challenges. I am grateful for the Committee’s invitation to offer my recommendations on how government can improve identity verification, and look forward to your questions.

Mr. GRIFFITH. I thank the gentleman and now recognize Mr. Mierzwinski for 5 minutes.

STATEMENT OF EDMUND MIERZWINSKI

Mr. MIERZWINSKI. Thank you, Vice Chairman, and Representative Castor, and members of the committee.

The Equifax breach was an epic fail in a lot of different ways. I know that this full committee has held hearings on it.

Mr. Walden, the chairman of the full committee, used an excellent line when he said, "I can't fix stupid," when he was talking about Equifax's many problems.

I agree with the chairman on that, but I want to point out a few other points about Equifax that may not have been pointed out in that hearing.

First of all, I think everybody sees them as a credit bureau, and that is true—they are one of the big three credit bureaus that collect information and sell it for the purpose of employment and credit and insurance decisions.

They are gatekeepers to our financial and economic opportunity. So it's very important that they do a better job. In fact, that's their only job is buying and selling data. So you can't blame Target or even OPM the same way you can blame Equifax for their many, many epic fails in that—in that debacle.

But I want to point out also—and the Federal Trade Commission has issued several reports on this—Equifax is not only a credit bureau. It is a data broker, and data brokers, unlike credit bureaus, are ubiquitous in society and they are virtually unregulated and they buy and sell information every day that's very similar to credit reports but unregulated. So we need to take a look at the data broker system and figure out a way to regulate it more closely.

Second, I think we need to go back to first principles. Mr. Hunt referred to data maximization. The code of fair information practices says data minimization should be a goal and the code of fair information practices is embedded in a number of our laws, including the U.S. Privacy Act of 1974.

So we can't just protect all information. We've got to start collecting less information and keeping it for shorter periods of time.

We have already heard from several witnesses and members of the committee about the problem of SSNs as identifiers and authenticators.

But I want to point out that our credit reporting system, how we obtain credit in society, a bad guy doesn't try to get your credit report. That's very hard to do.

A bad guy gets your Social Security number and goes to a creditor, and a creditor, being a trusted partner to the credit bureaus, gets your credit report and gives credit to the imposter. That's a very flawed system that needs to be fixed.

The principal thing that I think Congress should do in response to Equifax, and I think it's bipartisan, is make credit freezes free.

Credit freezes are the best way to protect your identify from financial identity theft. But, unfortunately, they cost money in most States.

The problem of KBA authentication has already been discussed. I want to point out it's so obsolete it's pathetic and it also upset—

it's not only bad because imposters can do one-second searches on the internet and obtain answers to the questions.

Sometimes consumers don't know the answers to the questions. My colleague was asked how much credit her—you know, her family member Chester had. Chester was her dog. He died years ago. She was 5 years old. Why is Chester a security question? What is the name of your first student loan company? Was it Sallie Mae or was it Navient? They keep changing the names of all of these companies. It's all ludicrous.

On multifactor identification, I think it's a real positive step. But I do want to point out that biometrics, the third general multifactor authentication—something you know, something you have, and something you are—privacy groups are very concerned about databases of biometric information posing privacy and civil liberties threats.

But on the other hand, if my fingerprint is only stored in my phone, perhaps that's a better solution. I'm very encouraged by the work that the other witnesses have talked about.

The FIDO Alliance and the NIST program have been open-source, open-standard, multistakeholder investigations of how to improve our privacy and authentication mechanisms.

On the other hand, I contrast that to the credit card PCS standards that have been imposed on merchants. The Target and the Home Depot, the Michael's, et cetera—all the merchant breaches—you can't blame the merchants for having to use an obsolete credit card with a magnetic stripe.

And now the—now the first have gone to a chip card, which is a type of tokenization, and that is good but they could have gone further. They could have gone to chip and PIN. They could have gone to best available technology.

So we have made some progress but a lot more needs to be done. Thank you very much for the time.

[The prepared statement of Mr. Mierzwinski follows:]

**Testimony of Edmund Mierzwinski,
U.S. PIRG Consumer Program Director
Hearing on “Identity Verification In A Post-Breach World”**

Before the House Committee on Energy and Commerce,

Subcommittee on

Oversight and Investigations

30 November 2017

Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director Before the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit

Vice Chairman Griffith, Representative DeGette, members of the committee, I appreciate the opportunity to testify before you on the important matter of data security and cyber threats. Since 1989, I have worked on data privacy issues, among other financial system and consumer protection issues for the U.S. Public Interest Research Group. The state PIRGs are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members.

Summary:

I appreciate that the committee is holding an oversight hearing on approaches to improving identity verification. It is important to review the best ways to move past the use of obsolete authentication systems that rely on social security numbers. You cannot authenticate with a number that is also an identifier, especially one that anyone can obtain, thanks to the data breach world we live in. Further, I am not sure so-called knowledge-based authentication was ever adequate, when it has often relied on a series of somewhat predictable questions. The problem has now worsened when any imposter can obtain most answers in real-time searches and, worse, when most actual consumers are asked truly stupid questions. Simply to place a credit freeze, my colleague had to try to explain to Equifax, after its well-publicized and ongoing debacle, that “No, Chester doesn’t co-own any property with me or have any credit cards. He was my dog when I was 5 years old and he died a long time ago.” And how many times has your student loan servicer changed names or changed hands? Is it Sally Mae or Navient? How do you answer?

My testimony also discusses that data breach responses need a careful approach by Congress. The authoritative Privacy Rights Clearinghouse has estimated that at least 10,057,873,432 records have been breached in a total of at least 7,831 data breach occurrences made public since 2005.¹ The massive exploit against Equifax, a major consumer credit reporting agency (colloquially, a credit bureau), not only affected at least 145.5 million

¹ See Data Breach page at Privacy Rights Clearinghouse, last visited 28 November 2017, <https://www.privacyrights.org/>.
Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

consumers, but compromised perhaps the richest trove of personal information I have seen in my over years of privacy and data security research.² While Yahoo³ now says all 3 billion of its user accounts may have been breached in 2013, much of the information taken could only be used for “phishing” emails or “social engineering” phone calls designed to use a little information to try to gain a lot more. While the Target⁴ and other retail breaches resulted in the theft of millions of credit and debit card numbers, those numbers can only be used in the short-term for “existing account fraud” before banks change the numbers. Meanwhile, Uber has finally reported the breach, in 2016, of some 57 million consumer and driver profiles.

I believe that multi-factor authentication is part of the solution. One factor might be something secret that only “you know,” such as a password, but certainly not your SSN. Another might be something “you have,” such as a phone or computer that can receive a verification text. A third might be something “you are,” such as your fingerprint or retina scan.

I do, however want to point out that the privacy and civil liberties communities are concerning about some of the implications of biometric identifiers. I am quite happy to have the convenience of a fingerprint passcode on my computer and cell phone, but only if they remain encrypted on those devices and are not made part of some larger, hackable database in the cloud and/or available to the government.

I also want to make the point that, like clockwork, after any big data breach is disclosed, powerful special interests seek to turn the problem into a bigger problem for consumers by using it as an opportunity to enact some sort of narrow federal legislation that broadly eliminates state data breach notification, state data security and other privacy protections. Industry lobbyists routinely mask their Trojan Horse efforts behind a “fix the patchwork, balkanized notice system” narrative to hide their broader plans. They don't simply want to create a

² Equifax's primary and best-known business is as one of three (Experian and Transunion are the others) national “Consumer Reporting Agencies” (colloquially “credit bureaus”) that do their consumer reporting business under the Fair Credit Reporting Act (FCRA) but also engage in a wide variety of lightly to unregulated direct marketing as “data brokers.”

³ Lily Hay-Newman, “Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts,” 3 October 2003, <https://www.wired.com/story/yahoo-breach-three-billion-accounts/>

⁴ The Target breach reportedly exposed 40 million credit and debit card numbers, as well as the customer account records -- including phone numbers and emails -- of millions more consumers. See Eric Dezenhall, “A Look Back at the Target Breach,” 6 June 2015, https://www.buffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

"uniform national breach law." Inside that Trojan Horse is their ultimate plan: to permanently take away all existing state data security laws and deny the states any authority to enact new privacy laws, even on new problems identified that Congress hasn't yet or purposely didn't solve.

I construe data security and the issues it raises broadly in this testimony to include an examination not only of data security and proper data breach response. I also review the history of how public policy decisions trending against the concept of consumer privacy have encouraged and promoted greater collection, sale and sharing of consumer information – without concomitant consumer control, without adequate regulatory requirements for data security, and certainly without market incentives for firms to protect the consumer financial DNA they collect and then sell.

I urge the Congress, at a minimum, to enact free credit freeze legislation. I caution the Congress, however, not to move forward on any breach or data security legislation that would preempt strong state privacy leadership or would endorse closed or non-technology neutral standards. Federal law should never become a ceiling of protection, it should always serve as a minimal floor that allows state experimentation. Further, any federal law to address the issues before this committee today should not endorse specific solutions that limit innovation or perpetuate oligopoly.

1) The Flaws of Authentication Based on Ubiquitous SSNs and Hackable Knowledge Based Authentication and Possible Solutions

In the U.S., new account identity theft and other frauds, including tax refund fraud and medical services fraud, are fueled both by the high demand for “instant credit” and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant. The Social Security Number genie left the bottle years ago. While we would prefer that it not be used as a commercial identifier, in numerous databases, it already is. The Congress needs to examine how to prevent it from being used as both an authenticator and an identifier. As a simple explanation, your ATM card PIN is a secret authenticator. It is different from your bank account number and known only to you. Whether it is a two-factor authentication or

some other solution, we need to move on from using Social Security Numbers for both identification and authentication because SSNs are not secret and don't do the job.⁵

As stated in the committee's majority staff hearing memo: "Given that much of modern commerce relies on a process of remote identity verification known as knowledge-based authentication or KBA, through which individuals prove who they are by answers to series of questions to which only they -- in theory -- should know the correct responses, this ability to "package" identity information raises even more significant questions about the reliability of traditional KBA practices. [...] With the wide-spread use of social media, consumer's unique identifiers for static KBA, are often available to the public [including] malicious actors."

I certainly agree that to rely on either static or dynamic KBA is to rely on an obsolete system. In addition to the ubiquity of much personal relationship information, easily available in one-second, real-time searches, much of the information remains a mystery to the consumer: "What lender originally held my student loan or mortgage?" It is likely that loan has been serviced more than once, or that the lender has changed its name at least once—from Sallie Mae to Navient, for example. My favorite recent example is the experience of one of my co-workers who tried to place a credit freeze on her Equifax credit report following their public announced of their debacle. Her "security" question generated by Equifax was "Where did Chester [Last Name] have credit cards when you lived with him?" Her answer: "I was 5 years old and Chester was my dog and he died a long time ago." But that simply generated another question from Equifax.

A) Multi-Factor Authentication

I believe that multi-factor authentication is part of the solution. One factor might be something secret that only "you know," such as a password, but certainly not your SSN. Another might be something "you have," such as a phone or computer that can receive a verification text. A third factor under consideration might be something

⁵ See "Security In Numbers: SSNs and Identity Theft," an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>
Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

“you are,” such as your fingerprint or retina scan.

I do, however want to point out that the privacy and civil liberties communities are concerning about some of the implications of such biometric identifiers. As a simple example, I am quite happy to have the convenience of a fingerprint passcode on my computer and cell phone, but only if they remain encrypted on those devices and are not made part of some larger, hackable database copied to the cloud. As the authoritative Electronic Frontier Foundation has pointed out:

Biometric identifiers include fingerprints; iris, face and palm prints; gait; voice; and DNA, among others. The government insists that biometrics databases can be used effectively for border security, to verify employment, to identify criminals, and to combat terrorism. Private companies argue biometrics can enhance our lives by helping us to identify our friends more easily and by allowing us access to places, products, and services more quickly and accurately. **But the privacy risks that accompany biometrics databases are extreme.** (Emphasis added).⁶

B: NIST in U.S. Government, Private Consortium FIDO Seek Trusted Identities

In an ongoing project, the U.S. government’s National Institute on Standards and Technology has done multi-stakeholder research into development of principles for a new paradigm to develop online trusted identities to ensure that: “Individuals and organizations employ secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.”

NIST’s project describes the principles of confidence, privacy, choice, and innovation in this way:

“Identity solutions will be: privacy-enhancing and voluntary; secure and resilient; interoperable and cost-effective and easy to use.”⁷

⁶ The Electronic Frontier Foundation, Biometrics Issues, undated resources webpage available at <https://www EFF.org/issues/biometrics>

⁷ Trusted Identities Group, “Overview: Building partnerships to advance digital identity,” undated webpage available at <https://www.nist.gov/itl/tig/about/overview>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

This project appears to have undertaken numerous pilot projects and partnerships. Its output is worthy of further review.

In the private sector, the Fast Identity Online Authentication (FIDO) Alliance⁸ is a 4-year-old international consortium seeking to replace the use of passwords with public-key encryption based multi-factor authentication. While I have not had the opportunity to examine it in detail, it appears to rely on an open standard and an open standard-setting setting process.

In my view, any project that the Congress endorses must rely on open, technology-neutral, technology-forcing performance standards and not memorialize any specific way of achieving them, which could become obsolete, into law.

C. Closed Standards Don't Work

Contrast the apparent openness of the FIDO approach with the oligopolistic Payment Card Standards (PCS) system that the card networks and the banks impose on merchants that seek to accept credit and debit cards.⁹ While the banks and card networks have largely blamed merchants (Home Depot, Target, Michael's Stores, Barnes & Noble, etc.) for a series of massive merchant breaches, the real problem was always the card networks' insistence on over-extending the lifespan of obsolete magnetic-stripe cards, which the merchants were forced to accept. Then, when they finally announced the so-called EMV transition, the networks chose the partial solution of switching to Chip, rather than Chip and PIN cards, which had already been in use in many countries for years. The oligopolists chose to advance not to the "current best available technology," but only to "the best available technology that helps maintain profits and locks out would-be competitors." While a Chip card used in a card-present transaction proves your card is not a clone and scrambles a one-time use number so card numbers are not

⁸ Fact Sheet, "What Is FIDO?," undated, available at <https://fidoalliance.org/about/what-is-fido/>

⁹ Wikipedia, "Payment Card Industry Data Security Standard Page," October 2017, available at https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard.

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

retained in merchant systems, a PIN-requirement would also prove that the user is not an imposter.¹⁰

Of course, the rollout of Chip cards has reduced card-present fraud, but caused fraudsters to move to online scams. This predictable result, however, has also hastened the development of better online transaction security systems. In fact, some of the best new online security methods include services allowing the use of a PIN to protect against fraud online.¹¹

2) Equifax and Other Breaches:

A. Equifax, A Huge Warning; The Uber Breach, A Nagging Reminder:

I remain incredulous that Equifax, a data broker with only one job -- buying and selling consumer information -- had such an epic fail in protecting that information and then responded badly to its epic fail. I commend the bipartisan Energy and Commerce committee leadership for persistently demanding further information from this recalcitrant wrongdoer.¹²

The Equifax breach was among the worst ever because the firm lost your financial DNA. Your Social Security Number is the key to identity theft: it doesn't change and may become more valuable to thieves over time, unlike a merchant breach of a credit card number, which has a limited shelf life.

Yes, Equifax is a highly-regulated credit bureau. But its larger business is as a largely unregulated data broker. In the broad data broker and Big Data universes consumers have no rights to control the collection and sale of their personal information. We are products, not customers. Dates of birth and Social Security Numbers do not change. They do not have a shelf life and can be used for more serious identity theft such as hard-to-deal-with new

¹⁰ See my testimony before the House Committee on Small Business, "The EMV Deadline and What it Means for Small Businesses: Part II," 21 October 2015, available at https://smallbusiness.house.gov/uploadedfiles/10-21-2015_mierzewski_testimony.pdf

¹¹ For illustrative purposes, not endorsement, you can see video demos for this service by Acculynk (now owned by First Data) available at <http://acculynk.com/resource/list/1>

¹² Letter from Chairman Greg Walden, Subcommittee Chairman Bob Latta, Ranking Member Frank Pallone and Subcommittee Ranking Member Jan Schakowsky to Equifax Interim CEO Paulino do Rego Barros, Jr., and Equifax Chairman Mark Feidler, 17 November 2017, available at <https://energycommerce.house.gov/news/press-release/committee-leaders-continue-push-equifax-data-breach-details/>

Testimony of Edmund Mierzewski, U.S. PIRG, 30 Nov 2017

account fraud, tax refund fraud, and theft of medical services. To me, the Equifax breach is rivaled only by the loss of similar information for 22 million employees, applicants and even friends providing character references for those applicants by the U.S. Office of Personnel Management (OPM)¹³ in 2015.

Unlike credit card numbers, your Social Security Number and Date of Birth don't change and may even grow more valuable over time, like gold in a bank vault. Much worse, they are the keys to "new account identity theft," which can only be prevented by a credit report freeze, as discussed in detail at several other Congressional hearings.¹⁴

While Equifax and other consumer credit reporting companies are required by the Fair Credit Reporting Act (FCRA) to make it hard for imposters to obtain another's credit report (how many security questions did you answer to obtain your own report?); identity thieves don't want your credit report. Instead, they use your SSN and DOB to apply for credit in your name; so that it's the bank or other creditor, which is a trusted third party (and likely answers no security questions) and has easy access to the credit reporting company, that obtains your credit report and/or credit score and then wrongly issues credit to the thief. In the U.S., such new account identity theft is fueled both by the high demand for "instant credit" and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant.¹⁵

B. Worse, Equifax Is A Data Broker: A Firm With Only One Job—Buying And Selling Consumer Information:

Equifax should do better at protecting data: it is a data broker, not a corner store, department store, health care

¹³ Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," 23 October 2017, <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>

¹⁴ See testimony of Mike Litt, U.S. PIRG before the committee, 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-mlitt-20171025.pdf>

¹⁵ See "Security In Numbers: SSNs and Identity theft," an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

provider or government agency. Incredibly, this is not the first security problem Equifax has faced recently.¹⁶

Equifax should have had a deeper moat and thicker castle walls, with more cross-bow archers, more trebuchets and more cauldrons of boiling oil on the watchtowers to defend your data than a merchant or even a government agency. It did not.

The Equifax breach extensively reviewed in numerous Congressional hearings demonstrates several paradoxes of our data use, privacy and data security laws and regulations. While the security of the *consumer credit reports* sold by Equifax in its role as a Consumer Reporting Agency (CRA) is strictly regulated by the Fair Credit Reporting Act (FCRA),¹⁷ the security of the *Social Security Numbers and Dates of Birth and other personally-identifiable-information (PII)* lost in the breach is regulated only under the limited data security requirements of Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).¹⁸ In addition, other (non-credit report) consumer profiles sold by Equifax and its hundreds, or thousands, of competitors in the *data broker* business are hardly regulated at all.

The Federal Trade Commission has recognized this. In two major reports in the last 5 years, it has called for greater authority to regulate the collection, sharing and sale of consumer information outside the limited walls of the FCRA, which primarily applies only to reports used in the determination of a consumer's eligibility for credit, insurance or employment. From the FTC's landmark report recommending Congress give it more authority over data brokers:¹⁹

¹⁶ Thomas Fox-Brewster, "A Brief History of Equifax Security Fails," 8 September 2017, Forbes. <https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#192afb0a677c> ¹⁷ 15 U.S.C. 1681 et seq.

¹⁸ The prudential regulator rules implementing Title V of GLBA generally only require that a breach notice plan be "considered." See bank regulators' joint "Interagency Guidelines Establishing Information Security Standards" are available at: <https://www.fdic.gov/regulations/laws/rules/2000-8660.html> The FTC Safeguards Rule applicable to national consumer credit reporting agencies including Equifax, which is silent on breach notification, is available here: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314.020523standardsforsafeguardingcustomerinformation.pdf The FTC is currently adding elements of a breach notification plan to its 2002 final rule above. All documents related to Title V are archived by the FTC here: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

¹⁹ FTC News Release, "Agency Report Shows Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer," 27 May 2014, <https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

“Data brokers obtain and share vast amounts of consumer information, typically behind the scenes, without consumer knowledge. Data brokers sell this information for marketing campaigns and fraud prevention, among other purposes. Although consumers benefit from data broker practices which, for example, help enable consumers to find and enjoy the products and services they prefer, data broker practices also raise privacy concerns. [...] Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences such as those related to ethnicity, income, religion, political leanings, age, and health conditions. Potentially sensitive categories from the study are “Urban Scramble” and “Mobile Mixers,” both of which include a high concentration of Latinos and African-Americans with low incomes. The category “Rural Everlasting” includes single men and women over age 66 with “low educational attainment and low net worths.” Other potentially sensitive categories include health-related topics or conditions, such as pregnancy, diabetes, and high cholesterol.”

When the Big 3 credit bureaus are in their alternate guise as nearly unregulated data brokers, they sell numerous consumer profiles to businesses. Consumers have no rights to know about these files, to examine these files, to correct these files or to limit their use. Congress should consider the FTC’s proposals.

- The data broker Experian:²⁰ “New markets targeted. Response rates improved. Revenue increased. These are the results we at Experian, as the industry leader, help you achieve with our business services.”
- The data broker Equifax:²¹ “The power behind our solutions—and your acquisition programs—is the superior quality of our data.”
- The data broker Transunion:²² “TransUnion offers more complete and multidimensional information for informed decisions that create opportunities for your business.”

C. Privacy Laws Need to Be Based on Fair Information Practices

²⁰ <http://www.experian.com/business-services/business-services.html>

²¹ <http://www.equifax.com/business/acquire-more-customers>

²² <https://www.transunion.com/business>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

Paradox: the FCRA is one of our strongest privacy laws. Despite the abysmal failure over the years of firms regulated under the FCRA to maintain the accuracy of consumer credit reports, or to adequately respond to consumers who dispute the inaccuracies that harm their financial or employment opportunities,²³ it remains that the 1970 FCRA's framework is fundamentally based on the Code of Fair Information Practices (FIPs), developed by a committee of the HEW Advisory Committee on Automated Data Systems in 1972, which was codified in the 1974 U.S. Privacy Act and governs information use by federal agencies.²⁴ The Privacy Rights Clearinghouse notes:

"In contrast to other industrialized countries throughout the world, the U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level. Instead, the Principles have formed the basis of many individual laws in the U.S., at the both federal and state levels -- called the "sectoral approach." Examples are the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.²⁵"

The FIPs are nevertheless embodied in the FCRA: The FCRA limits the use of consumer credit reports only to firms with certain permissible purposes (generally, determinations of a consumer's eligibility for credit, insurance and employment), it requires credit bureaus (data collectors) to meet certain accuracy standards and it allows consumers to review their files, dispute and demand corrections of mistakes and to control the secondary use of their files by opting out of marketing uses of their reports.

Nevertheless, the U.S. sectoral-only privacy laws should be contrasted with the new European **General Data Protection Regulation (GDPR)**. It provides over-arching privacy rights to European citizens over corporate usage of their information, including rights to control the use of their information and to seek redress (and

²³ "...the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly." See page 3, testimony of Chi Chi Wu, National Consumer Law Center, before the committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-ccwu-20171025.pdf>

²⁴ "U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)", https://epic.org/privacy/consumer/code_fair_info.html

²⁵ Privacy Rights Clearinghouse, "A Review of The Fair Information Principles: The Foundation Of Privacy Public Policy," 1 October 1997, <https://www.privacyrights.org/blog/review-fair-information-principles-foundation-privacy-public-policy>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

compensation) against the infringing company. Importantly, the GDPR, when it goes into final effect next year, trumps the existing Privacy Shield²⁶ applicable to U.S. firms doing business in Europe and provides a roadmap for U.S. companies to improve their treatment of U.S. consumers.²⁷ The GDPR would also subject firms to civil penalties for failing to report data breaches.²⁸ We support, as does the National Consumer Law Center, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties for a first violation of the rules; it can only impose penalties after an enforcement order is violated. The FTC has no authority to supervise firms, as the Consumer Bureau does. The Consumer Bureau has much broader rulemaking authority than the FTC.

Paradox: Identity theft is a business opportunity. The big credit bureaus have responded to the scourge of identity theft driven by instant credit, sloppy credit report-granting practices, and of course, data breaches, not by improving their own security and compliance but by seizing new business opportunities:

Consumers scared of either fraud and identity theft or low credit scores are urged to buy their subscription credit monitoring services, for as much as \$10-20/month. The GAO has determined that such “services offer some benefits but are limited in preventing fraud.”²⁹ Estimates are that consumers spend at least \$3 billion/year on credit monitoring services.³⁰

Despite that the bureaus have failed to either protect credit reports or maintain the “maximum possible accuracy” required by law, they have also monetized a lucrative business-to-consumer (B2C) channel for over 20 years to market their over-priced, under-performing credit monitoring products.³¹

²⁶ For information on the Privacy Shield, see <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield>

²⁷ The GDPR is explained here https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

²⁸ Nina Trentmann, “Data Breaches Will Soon Cost Companies in Europe,” the Wall Street Journal, 22 November 2017, available at <https://www.wsj.com/articles/data-breaches-will-soon-cost-companies-in-europe-1511386000>

²⁹ U.S. General Accounting Office, March 2017: “Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud,” <http://www.gao.gov/assets/690/683842.pdf>

³⁰ Steve Weisman, “Is Identity Theft Protection Worth It?”, 22 April 2017, USA Today, <https://www.usatoday.com/story/money/columnist/2017/04/22/identity-theft-protection-worth/100554362/>

³¹ On 7 September 2017, the date that the Equifax breach was announced to the public, the Financial Services Committee held a hearing on a discussion draft from Mr. Royce, a bill which we oppose. The bill would exempt credit bureau marketing and education programs from the Credit Repair Organizations Act, and exempt the bureaus, and others that might seek the same license, from strong consumer protection laws. The discussion draft is available at

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

Prices for credit monitoring, credit scoring and identity theft protection and remediation products from credit bureaus, banks and firms such as Lifelock range up to \$19.99/month or more. The marketing of the products, often based on scant 3-5 day free trial periods, is often deceptive. In 2017, the Consumer Bureau imposed fines totaling over \$23 million on both Equifax and Transunion over their marketing of credit scores and subscription credit monitoring services.³² Lifelock has been fined both for unfair marketing and contempt (\$100 million) when it failed to comply with an FTC order.³³

And of course, the big credit bureaus and others have also leapt into the business of B2B identity validation and verification, largely in response to their own, and others', failure to maintain the security of information.

Paradox: Businesses are customers and consumers are products. Despite nearly 50 years of FCRA requirements to handle consumer disputes and over 20 years of aggressive-direct-to-consumer advertising of pricy subscription-based credit monitoring products, its ex-CEO repeatedly apologized to Congress that, as a business-to-business company, it had no idea how many consumers would call or email. How is this possible? Well, it turns out consumers are not looked at by Equifax as customers.

This absurd disconnect is because of a market failure in credit reporting: we are not their customers, we are their product. The consumer credit reporting market is dominated by the Big 3 gatekeepers to financial and employment opportunity. Yet, you cannot choose a credit bureau. When you are mad at your bank's fees or policies, you can vote with your feet and find a new bank. You're stuck with the credit bureaus. Richard Cordray, first director of the Consumer Financial Protection Bureau, often calls credit reporting one of several "dead-end

https://financialservices.house.gov/uploadedfiles/bills-115_royce020_pih.pdf We concur with Chi Chi Wu's testimony against both the Royce bill and against a bill from Mr. Loudermilk also discussed that day. HR2359, the so-called FCRA Liability Harmonization Act, would eliminate punitive damages and cap other damages in actions brought under the FCRA. Testimony of Chi Chi Wu, National Consumer Law Center is available at

<https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ccwu-20170907.pdf>

³² Press release, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 January 2017, available at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/>

³³ Press release, "Lifelock Fined \$100 Million for Contempt," 17 December 2015, available at <https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

markets” in need of stricter regulation to counter that market failure.³⁴

The Big 3 bureaus (Equifax, Experian and Transunion) were fined an inadequate total of \$2.5 million by the Federal Trade Commission (in 2000) for failing to have enough employees to answer the phones to handle their complaints.³⁵ Nevertheless, we are encouraged by the recent efforts by the Consumer Bureau to achieve changes to the Big 3’s operations through supervision.³⁶

D. Consumers Have Little Control of their Information:

The 1999 Gramm-Leach-Bliley Financial Modernization Act was largely enacted to allow mergers of commercial banks, investment banks, securities firms and insurance companies. However, due to privacy complaints at the time about a number of large banks, including U.S. Bank, which was sued by the State of Minnesota for sharing customer records with a third-party telemarketer that then preyed on its customers,³⁷ the law did include a modest privacy and data security provision, Title V, that gave consumers the ability to opt-out of sharing of their personal information only with non-affiliated, non-financial firms (but explicitly allowed sharing with affiliates or other financial firms, regardless of a consumer’s wishes).³⁸ A wide variety of organizations, ranging from the ACLU to consumer groups to Phyllis Schlafly’s Eagle Forum, supported more comprehensive privacy protection provisions

³⁴ Richard Cordray, “Prepared Remarks of CFPB Director Richard Cordray at the National Association of Attorneys General,” 23 February 2015, <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-national-association-of-attorneys-general-2/>

³⁵ Press release, “Nation’s Big Three Consumer Reporting Agencies Agree To Pay \$2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act,” 13 January 2000, available at <https://www.ftc.gov/news-events/press-releases/2000/01/nations-big-three-consumer-reporting-agencies-agree-pay-25>

³⁶ Consumer Financial Protection Bureau, “Supervisory Highlights: Consumer Reporting, Special Edition,” March 2017, Issue 14, Winter 2017, available at http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf

³⁷ “Defendants US Bank National Association ND and its parent holding company, US Bancorp, have sold their customers’ private, confidential information to MemberWorks, Inc., a telemarketing company, for \$4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks.” Complaint filed by the State of Minnesota against U.S. Bank, 9 June 1999, available on Internet Archive, last visited 30 October 2017,

https://web.archive.org/web/20010423055717/http://www.ag.state.mn.us:80/consumer/privacy/pr/pr_usbank_06091999.html ³⁸

The 1999 GLBA required annual privacy notices of financial institution information sharing practices and of the limited right to opt-out it provided. Industry organizations have relentlessly sought to eliminate the annual notice provisions. A transportation bill known as the FAST Act codified a narrowing of the requirement as a rider in 2015, as explained by the Consumer Financial Protection Bureau, <https://www.federalregister.gov/documents/2016/07/11/2016-16132/annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p> HR 2396, We also oppose “The Privacy Notification Technical Clarification Act,” to further narrow consumer rights to notice about privacy practices, was approved by this committee in a markup held on 11-12 October 2017,

<https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402416>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

approved in this committee as proposed by a broadly bi-partisan group led by then-Rep./now Sen. Ed Markey (D-MA) and Rep. Joe Barton (R-TX).³⁹ The final law also required banks and certain non-banks, including consumer credit reporting firms, to comply with its data security provisions.⁴⁰

Although the 2010 Dodd-Frank Act enacted in the wake of the 2008 financial collapse transferred authority to regulate credit reporting under FCRA to the tough new Consumer Financial Protection Bureau, its Section 1093 retained Title V data security provisions for non-banks under the weaker FTC. Unlike CFPB, that agency cannot supervise the activities of firms on a day-to-day basis, nor can it impose civil money penalties for a first violation.

D. Don't Forget the Uber Breach

Then came the Uber breach. Mr. Pallone, the full committee ranking member, has rightly urged an investigation. Some 600,000 drivers had their financial DNA taken. While the information of over 56 million consumers that was also breached was apparently limited to names, email addresses and phone numbers subject to social engineering phone calls and “phishing” emails, the announcement of the Uber breach, hard on the heels of the Equifax breach, should serve as a reminder that until we do something, breaches will continue. Of course, Mr. Pallone’s request for an investigation also points out that Uber, as many breached entities before it, chose to ignore clear state laws requiring prompt notification to victims and also, in many states, to law enforcement officials, when it waited over a year to notify anyone. Worse, of course, Congress needs to get to the bottom of its apparently paying a ransom to the thieves to keep it quiet for their own business development purposes. I would also ask Uber what proof it has that thieves would actually give back their only copy of stolen information, even if a ransom were paid.

3) Recommendations:

³⁹ The variety of groups that worked together for stronger privacy provisions is listed in this letter of 9 May 2000 to prudential regulators urging faster compliance of stronger rules, available on Internet Archive, last visited 30 October 2017, <https://web.archive.org/web/20010425154255/http://www.pirg.org:80/consumer/glbdelay.htm>

⁴⁰ The Federal Trade Commission’s 2002 Safeguards Rule implements the law for non-bank “financial institutions, including the consumer reporting agencies and is available at <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

A. Congress Must Reject Industry Trojan Horses Seeking State Preemption:

I cannot overstate the political conundrum that although the severity of the Equifax breach and the relentless march through the headlines of other breaches demand that policymakers enact stronger, not weaker, consumer protections, Congress instead often considers industry-backed bills to preempt, or override, numerous stronger state data breach and data security protections. Worse, the bills have a kicker: most permanently take the states off the board as privacy first responders and innovators.

A small federal gain should not result in a big rollback of state authority. As one example of a Trojan Horse provision I call your attention to HR 1770, the Data Security and Breach Notification Act of 2015, a bill approved by this committee in the last Congress. The bill included sweeping data security and data notification preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general. While I note that this bill has numerous other objectionable provisions, which I am happy to discuss, its sweeping preemption language is illustrative of long-sought industry goals to take states – historically privacy leaders -- off the privacy board.

Of course, this committee's Trojan Horse preemption language was not as sweeping as one in a bill approved by the Financial Services Committee in the last Congress. HR 2205,⁴¹ the Data Security Act of 2015 (Neugebauer), included even more sweeping preemption language. (Section 6).

Numerous critical provisions of California, Massachusetts, Illinois, Texas and other state breach notification laws could be eliminated as would 17 state laws that include a consumer private right of action to sue data breach notification law violators. I urge the committee not to preempt state privacy laws. Instead, focus on proposals that return some control over their personal information to consumers, such as widely supported proposals to allow consumers to place and lift credit freezes on their credit reports for free. While that action may not be squarely in the committee's ambit, it is the best narrow, do-able response to the breach debacle.

⁴¹ HR 2205 is available at <https://www.congress.gov/bills/114th-congress/house-bill/2205/>
Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the states to enact stronger data security and identity theft protections. We argued that since Congress hadn't solved all the problems, it shouldn't prevent the states from doing so.⁴²

From 2004-today, nearly every state enacted security breach notification laws and enacted credit, or security, freeze laws. Many of these laws were based on the CLEAN Credit and Identity Theft Protection Model State Law⁴³ developed by Consumers Union and U.S. PIRG.

Congress should not preempt stronger state breach notification laws. **California** and **Texas**, for example, have very strong notification laws based on an *acquisition* standard. Information lost is presumed to be acquired, therefore requiring notice to breach victims. Industry actors would prefer use of a *harm trigger* before notice is required.

There are numerous problems with a harm trigger, which is a feature of some state laws and most proposed federal laws. The first is that the breached entity, which has already demonstrated extreme sloppiness with the personal information of its customers, gets to decide whether to inform them so that they can protect themselves.

The second problem is that industry groups would like any preemptive federal bill to define privacy harms very narrowly; their preferred bills would limit harms to direct financial harm due to identity theft.

Yet harms also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Further, consumers face very real additional problems including the stigma of being branded a deadbeat and facing the emotional costs and worry that brings.

Only an acquisition standard will serve to force data collectors to protect the financial information of their trusted

⁴² For a detailed discussion of how the FACT Act left the states room to innovate, see Gail Hillebrand, "After the FACT Act: What States Can Still Do to Prevent Identity Theft," 13 January 2004, available at <http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/>

⁴³ U.S. PIRG and Consumers Union, "The Clean Credit and Identity Theft Protection Act: Model State Laws - A Project of the State Public Interest Research Groups and Consumers Union of U.S., Inc." Version of November 2005, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=846505

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

customers or accountholders well enough to avoid the costs, including to reputation, of a breach. Only if an entity's reputation is at risk will it do its best job to protect your reputation.

Further, as Laura Moy has extensively pointed out to this and other committee, potential harms to consumers from misuse of information go well beyond financial identity theft to harm to dignity reputation and even physical harm.⁴⁴ Bad outcomes she describes range from elimination of broad definitions of harms requiring notice and elimination of growing types of information protected by state laws (including **California, Florida, and Texas** laws requiring protection of physical and mental health records, medical history, and insurance information as well as elimination of a variety of state laws protecting online credentials, GPS data and biometric data). Ms. Moy also correctly urges the Congress to leave the states room to respond to new, unknown threats.⁴⁵

New York Assistant Attorney General Kathleen McGee has recently suggested to Congress that state notification laws have been expanded to include protection account credentials, biometric data and other protections. She also notes that nearly every state also holds firms accountable based on their consumer protection laws, which would also be preempted by many federal proposals.⁴⁶

Other bills before the Congress have included similar, if not even more sweeping, dismissals of our federal system. Such broad preemption will prevent states from acting as innovators of public policy or as first responders to emerging privacy threats. Congress should not preempt the states but instead always enact a floor of protection. In fact, Congress should think twice about whether a federal breach law that is weaker than the best state laws is needed at all. Congress should maintain co-authority of state Attorney General and other state and local enforcers; Congress should also retain state private rights of action, especially if it declines to create any federal private rights of action.

⁴⁴ See section 3, especially, of testimony of Laura Moy, Georgetown University Law Center's Center on Privacy and Technology, before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

⁴⁵ Testimony of Laura Moy, Georgetown University Law Center's Center on Privacy and Technology, before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

⁴⁶ Testimony of Kathleen McGee, Assistant Attorney General, Office of the New York Attorney General, at a hearing before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-kmcgee-20171025.pdf>

The most recent testimony of Sara Cable, a **Massachusetts** Assistant Attorney General, who has previously appeared before this committee, made several points about the importance of state action abundantly clear:

“The Equifax breach may bring into consideration whether a national data breach notice and data security standard is warranted. As noted, Massachusetts has among the strongest data security and breach laws in the country. My Office has serious concerns to the extent any federal standard seeks to set weaker standards than those that currently exist for Massachusetts consumers and that would preempt existing or future state law in this field. States are active, agile, and experienced enforcers of their consumers’ data security and privacy, and need to continue to innovate as new risks emerge.”⁴⁷

Ms. Cable’s testimony also notes Massachusetts Attorney General Maura Healey’s strong support for free credit freeze legislation to be enacted by the state. To the extent any national notification standard is considered by the Congress, it must contain strong, minimum data security standards that do not erode existing state protections.

Other state attorneys general including **Illinois** Attorney General Lisa Madigan, concur.⁴⁸ General Madigan’s office is also actively involved in the multi-state Equifax investigation, is calling for Equifax to pay for credit freezes for all Illinois residents and is supporting state legislation to provide free credit freezes.⁴⁹

No GLBA Safe Harbor: Nearly every federal breach notification bill that requires breach notification by covered entities (regardless of its harm trigger or other provisions), also seeks to provide a safe harbor to entities already covered by Title V of the Gramm-Leach-Bliley Act or other federal data security laws, such as those applicable to health care entities.⁵⁰ As merchants and retailers have long pointed out, this leaves them, as non-financial institutions under the GLBA scheme, subject to notification standards higher than those of GLBA “financial institutions.” Such a two-tiered system makes no sense from a policy perspective. Of course, merchants have also

⁴⁷ Testimony of Sara Cable, Assistant Attorney General, Office of the Massachusetts Attorney General, before this committee, 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-scable-20171025.pdf>. Note also that Ms. Cable references her earlier, more comprehensive testimony before the Congress for further details on the Massachusetts data security requirements.

⁴⁸ “Getting it Right on Data Breach and Notification Legislation in the 114th Congress,” A Hearing of the U.S. Senate Committee on Commerce, 5 February 2015, available at <http://1.usa.gov/1tGf5m>

⁴⁹ News Release, 12 September 2017, available at http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170912.html

⁵⁰ See the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR Subpart C of Part 164).

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

suffered enmity from banks and credit unions which seek affirmative legislation holding them liable for breach costs. Such disputes should be covered in contract, not law.

B. Congress Should Allow Consumers to Hold Breached Firms Accountable In Court

In the immediate circumstance, the best way to give consumers protection against data breaches is to let us hold firms that lose our information accountable, including through their wallets. Threats to consumers can include fraud on existing accounts, new account identity theft, medical identity theft, tax refund identity theft and imposters committing crimes using your identity. Measurable harms from these misuses are obvious, but any measure of harms must also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Consumers also face very real emotional stress and even trauma from financial distress. Breach harms also include the threat of physical harm to previous domestic violence victims.⁵¹ Congress must main private rights of action against corporate wrongdoers.

Virtually all federal privacy or data security or data breach proposals specifically state that no private right of action is created. Such clauses should be eliminated and it should also be made clearer that the bills have no effect on any of the 17 state law private rights of action that apply to data security and breaches. . Further, no bill should include language reducing the scope of state Attorney General or other state-level public official enforcement. Further, any federal law should not restrict state enforcement only to state Attorneys General, but allow enforcement by local enforcers, such as district attorneys.

C. Congress Should Enact A Free Credit Freeze For All Law and Implement One-Stop Shopping for Freezes and also Consider Making the Freeze an Always-On Default

Of course, I also believe that the minimum action Congress should take would be to extend free credit freezes at all 3 national consumer reporting agencies to all consumers at all times. The Congress should also ensure one-stop

⁵¹ See Page 10, Testimony of Laura Moy, Deputy Director, Center on Privacy and Technology, Georgetown University Law Center, 25 October 2017, available at: <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

shopping for credit freezes, as is already the law for fraud alerts. You should need to contact only one credit bureau to gain protection at all three.

While we support the credit freeze as a minimum, a next step, once radical but now worthy of discussion, would be to make the credit freeze the always-on default. Consumer DNA should always be frozen; freezes should only be lifted at the consumer's request.

D. The Congress Should Transfer Authority Over Gramm-Leach-Bliley Title V to the Consumer Bureau

We support, as does the National Consumer Law Center, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties for a first violation of the rules; it can only impose penalties after an enforcement order is violated. The FTC has no authority to supervise firms, as the Consumer Bureau does. The Consumer Bureau has much broader rulemaking authority than the FTC.

Conclusion: A Threat to Consumers Is Posed by the Basic Business Model of the Digital Data Advertising Ecosystem

This testimony focuses primarily on the impact of a failure to secure consumer information. Congress should also investigate the broader problem of the over-collection of consumer information for marketing, tracking and predictive purposes. While the digital advertising ecosystem expands the number of vectors for misuse, the ubiquitous tracking of consumers as commodities or products poses threats as a business model itself.⁵²

In many ways, data breaches are the mere tip of the iceberg when it comes to privacy threats in the Big Data world. In the Big Data world, companies are collecting vast troves of information about consumers. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New

⁵² See Edmund Mierzwinski and Jeff Chester, "Selling Consumers, Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act," 46 Suffolk University Law Review Vol. 3, page 845 (2013), available at http://suffolklawreview.org/wp-content/uploads/2014/01/Mierzwinski-Chester_Lead.pdf
Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

technologies allow a web of interconnected businesses – many of which the consumer has never heard of – to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm. Increasingly, the information is being collected in the mobile marketplace and includes a new level of hyper-localized information.

Contrast the FCRA with the new Big Data uses of information which may not be fully regulated by the FCRA. The development of the Internet marketing ecosystem, populated by a variety of data brokers, advertising networks and other firms that collect, buy and sell consumer information without their knowledge and consent, is worthy of much greater Congressional inquiry.⁵³ As I wrote, with a colleague from the Center for Digital Democracy:

⁵³ See the FTC's March 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report>

Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

“Dramatic changes are transforming the U.S. financial marketplace. Far-reaching capabilities of “Big-Data” processing that gather, analyze, predict, and make instantaneous decisions about an individual; technological innovation spurring new and competitive financial products; the rapid adoption of the mobile phone as the principal online device; and advances in e-commerce and marketing that change the way we shop and buy, are creating a new landscape that holds both potential promise and risks for economically vulnerable Americans.”⁵⁴

Congress has largely failed to address numerous digital threats to consumers, from data breaches to data brokers running amok to the very architecture of the digital ecosystem, where nearly every company -- known and unknown -- is tracking consumers, building a dossier on them and even auctioning them off to the highest bidder in real time (for advertising or financial offers). Any data security, breach or privacy legislation should provide individuals with meaningful and enforceable control over the collection, use and sharing of their personal information.

It is important that policymakers understand that you cannot bifurcate the issues of data security and privacy. Consumer privacy is threatened when companies can buy or sell our information and we have little choice or control. Consumer privacy is threatened when data collectors do not keep data secure. In the new Big Data world, where firms are racing to vacuum up even more data than ever before, with even less acknowledgement of any privacy interest by consumers (or citizens), it is important that we re-establish norms that give consumers and citizens greater control over the collection, and use, of their personal information.

I appreciate the committee’s thoughtful approach in taking a closer look at ways to improve online authentication of consumers and for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

—

⁵⁴ Edmund Mierzwinski and Jeff Chester, “Big Data Means Big Opportunities and Big Challenges,” 27 March 2014, U.S. PIRG and the Center for Digital Democracy, available at <https://uspirg.org/reports/usfbig-data-means-big-opportunities-and-big-challenges>
Testimony of Edmund Mierzwinski, U.S. PIRG, 30 Nov 2017

Mr. GRIFFITH. Thank you. Appreciate that, and we will now begin the questioning, and I will start with questions.

Mr. Hunt, in your testimony you talk about the exposure of data due to accidental misconfigurations of cloud services. You were certainly spot on.

One such misconfiguration was discovered in the Federal Government this week, and it has been reported that this is the fifth time the Government has suffered a similar accidental exposure this year.

Indeed, many companies, including Uber, have suffered information compromises because of these kinds of misconfigurations.

Why does this keep happening? Is it really that easy to accidentally share your cloud services with the world?

Mr. HUNT. Well, the easy answer to the last question is yes, it is that easy. It's very often just a simple misconfiguration, and the difference between, let's say, a storage account within Amazon being protected and needed credentials in order to access it and being wide open is literally one configuration that can take seconds to make.

So in terms of why it's that easy or how come this keeps happening so frequently, very often this is a competency problem. So people have access to resources such as cloud services that aren't sufficiently skilled in order to figure out how to configure them securely. Sometimes it can just be a simple oversight and there's not enough backup controls to identify when something like this is exposed publicly.

It is also very difficult for organizations because when cloud services are used they tend to very frequently sit outside their known address base.

So, traditionally, an organization could say these are our IP addresses, this is the range of our scope of assets and then you can go onto the cloud and you can put things in totally outside that construct.

And then compounding that as well we have this—this, I guess, construct called Shadow IT and for the longest time we have had the concern of Shadow IT—people working outside the formal constructs of the way the IT department and organization should run.

And today, it is very simple for someone in an organization to go to the likes of Amazon and say, "Look, I would like a storage account. I am going to publish data there," and the IT department never even knows about it.

So there's a number of factors leading to the prevalence of what is now becoming a very common event.

Mr. GRIFFITH. Now, are any of the data breaches included in your service from such a misconfiguration?

Mr. HUNT. From which, sir?

Mr. GRIFFITH. From—from your service.

Mr. HUNT. Oh, from misconfiguration?

Mr. GRIFFITH. Yes.

Mr. HUNT. Yes, many of them. So we are seeing many incidents. The perfect example that comes to mind, earlier this year we had an OIT device called a CloudPet.

It is literally a teddy bear with a listening device that talks to the internet. Their data was left publicly exposed in a database fac-

ing the worldwide web without a password. And, again, that is just a simple misconfiguration on their behalf.

Mr. GRIFFITH. Wow. What can companies do to decrease the likelihood of this kind of a misconfiguration?

Mr. HUNT. It's a combination of things. To me, many of these incidents, whether it be misconfiguration or flaws in software, come back to education, and this is the sort of thing we are trying to do with Pluralsight.

Let's try and get education out there to the people that are building these systems and standing them up. Because so frequently it is just such a simple little thing and had the person understood what the ramifications of the configuration change they're making or the code change they're making was, it wouldn't have happened. So I would love to see more education.

Mr. GRIFFITH. And what are the consequences? I mean, we can all think of some. But what are the consequences of companies exposing this kind of data?

Mr. HUNT. Really depends on the data. I mean, at sort of the least end of the scale, very often we are seeing large amounts of email addresses and passwords.

Now, that then often becomes a skeleton key into other things because we know that people reuse their passwords.

So that—I almost hesitate to say that's the best that could happen. But when we think about the worst that could happen, well, now we start to talk about large amounts of very personal data.

So we have been speaking about the impact of things like the Equifax incident. South Africa just recently had an incident which was data exposed as a backup on a publicly facing server that had information about the entire country and this included their national identifier, so think about a Social Security number, which within there also includes date of birth and gender, and now we have got a whole country saying we literally had all of its data published on the internet and we know that it had been obtained by other unauthorized parties and redistributed.

But what do we do? And to me, that's sort of the worst-case scenario, because now you got a whole country saying, how are we going to do knowledge-based authentication when the knowledge about the whole country has gone public?

Mr. GRIFFITH. Now, from what I understand, when folks go back and analyze many security instances like data breaches, they find that somewhere along the line someone in the organization chose convenience such as the ability to check their personal email from their work computer, for example, over security. Have you found that to be true as well, in your work?

Mr. HUNT. Absolutely. I mean, the concern with convenience—I will give you a really good analogy—is very often I will say to people, look, we might see an application talking to a database that has effectively server admin rights—the most privileged user you could possibly have—and I will say to people, why would that happen. And they say, well, it was easy—it was much easier to give access to everything than to start implementing fine-grained permissions. And they are right, it is much easier. But that then leads to the problems we have got here.

Mr. GRIFFITH. And so, how do we make it easier to protect things—protect that data?

Mr. HUNT. Well, again, I go back to that education side. This is people making mistakes unknowingly, and when we see these happen over and over again and we look at the behaviors of the individuals, very often it is because they've never been taught what are the ramifications of setting this configuration or writing code that way.

Mr. GRIFFITH. Yes. I do think we all choose convenience from time to time when we know in our hearts we ought not.

With that, I have to yield back because my time is up and now recognize Ms. Castor of Florida for 5 minutes of questions.

Ms. CASTOR. Well, thank you, Mr. Chairman.

As the Equifax breach made all too clear, there's an astounding amount of data that is collected by companies and especially credit bureaus.

The Equifax breach, for example, exposed the personal information including names, Social Security numbers, birth dates, addresses, other sensitive data of almost 150 million Americans.

Mr. Grant, if this data is out there, should companies no longer use this information as a component of identity verification online?

Mr. GRANT. I wouldn't say that they shouldn't use the information anymore, but they should be smart about the ways in which they use it and I think there needs to be a recognition, you know, across Government and industry that these first-generation systems that we were using, the attackers have caught up with them.

So let's figure out where it can be valuable in a process to establish identity or authenticate identity and where it can't be. I think there are still tools that are out there that are using some of this data that could be—you know, I often talk about, you know, you have an arrow with multiple quivers in terms of, you know, the tools that you're using.

There still may be some value. But I think we need to recognize that it is been greatly diminished and we need to focus on next-generation solutions.

Ms. CASTOR. So, Mr. Mierzwinski, a similar question. In your testimony, you stated in reference to Social Security numbers that, quote, "you cannot authenticate with a number that is also an identifier, especially one that anyone can obtain, thanks to the data breach world that we live in."

This seems like a good reason to prevent companies from using the Social Security number as an authenticator. Is that right?

Mr. MIERZWINSKI. Well, I think you're absolutely right, Congresswoman, and many people don't know that the Social Security number was invented so long ago it doesn't even have a correct check sum number.

When you type your credit card number and make a mistake in an online form, it knows instantly. Your Social Security number can be completely garbled and it wouldn't know.

The first five digits actually aren't really about you. They're about when you were born and where you got your number more than unique. So it is a very big mistake.

I am encouraged that some of my banks know that when I've logged on from a new machine or even a new place. But others of

my banks and other companies that I do business with don't ask me extra questions or don't want to send me a text.

So it is uneven how companies are doing better authentication and, to me, you have also got to penalize them when they make a mistake.

I realize Equifax and other firms will be penalized by the market. However, I wonder whether regulators need more authority to penalize companies that lose our info.

Ms. CASTOR. So let's talk about that especially. You mentioned the data brokers. Even outside of data breaches, internet-connected datasets contain vast information.

A University of North Carolina study showed that data brokers can obtain almost anything from demographic data to financial data to travel data.

In your opinion, are there adequate safeguards in place to limit what information data brokers collect, store, and sell about us? It seemed in your testimony you said no, it is kind of the —

Mr. MIERZWINSKI. No, despite—and you can find many items on the record from me criticizing the credit bureaus and the Fair Credit Reporting Act for being too weak. It actually is one of our stronger privacy laws. There are virtually no laws that apply to data brokers and they are out there in a Wild West ecosystem of digital collection and selling of information about consumers in real time, and as I believe the vice chairman pointed out in his opening statement, a lot more information is being collected into their databases.

Your locational information is, for one, a new piece that should be protected that isn't protected under many laws.

Ms. CASTOR. So are there any incentives currently in place for companies to minimize the data they collect and store?

Mr. MIERZWINSKI. Unfortunately, I don't know that there are enough and there—public shaming helps but regulatory accountability would help even more, and companies just feel that we are not their customers.

Consumers are not Equifax's customer. Mr. Smith, the ex-CEO, said that before numerous committees over the last month. Business is their customer. We are their product. We need to get them to think about taking care of us, and they haven't.

Ms. CASTOR. Mr. Grant, thank you for all of your work on the National Strategy for Trusted Identities. The identity ecosystem adheres to fair information practice principles, one of which is data minimization.

This is the idea that organizations should collect only information that is directly relevant and necessary to accomplish the specified purpose. Is that right?

Mr. GRANT. Yes.

Ms. CASTOR. So now it seemed to me, in this day and age, companies want to know everything about you. I am going to ask you the same question. What incentives are currently in place for companies to minimize the data they collect and store?

Mr. GRANT. Well, I will say concerns both about regulatory enforcement as well as liability that they might face by having too much data.

You know, Mr. Hunt talked before about data maximization. When I was running the NSTIC program there was a term one of our staffers coined, which was data promiscuity—the practice that, you know, companies are just quite open in terms of collecting and sharing gobs of data.

And I do think one thing you're starting to see now, particularly when some of that data is exposed in a massive breach, is other companies take a look at it and say, do we actually want to have all of this data.

And so, you know, now that I am in the private sector I spend a lot of time working with companies, advising companies on how to minimize their risk, and I would say there are some companies that still want to hoard data and there are some that are realizing that it might be a liability and are actually trying to put proactive measures in place to reduce the footprint of data that they have on their customers and really focus only on what they need.

So I do think a mix of regulation and liability does have an impact in the marketplace. You know, certainly, if you look across the ocean to what's happening in Europe right now with the impending implementation of Europe's general data protection regulation—GDPR—there's a lot of companies here in the U.S. that are still going to be impacted by that and that's also causing some firms to wake up and reevaluate in some cases what data they collect, how they store it, how they use it.

Ms. CASTOR. Thank you.

Mr. GRIFFITH. I thank the gentlelady for yielding back.

Now recognize the gentleman from New York, Mr. Collins, for 5 minutes of questions.

Mr. COLLINS. Thank you, Mr. Chairman.

And Mr. Hunt, I guess it is 3:00 a.m. right now so I am hoping you got some sleep on the flight coming up from Down Under.

I want to try to put today's hearing maybe in context just for the everyday person. So many of us—you know, every three months one of our credit cards is accessed in some way. Usually we find out because we get a notification—a fraud alert from American Express or Master Card. They've actually got some algorithm somewhere that says, this looks unusual, or something.

So I want to make sure I understand. That's a little—people doing that, grabbing our credit report and stealing our numbers is perhaps different than the data breach area, or not?

Mr. HUNT. Where it probably differs to credit cards is there are a lot of different places where credit cards are exposed which may not be as a result of a data breach.

I've had my wife's card compromised several different times now and, as you say, you hear from American Express—

Mr. COLLINS. Because I am sure she uses it daily.

[Laughter.]

Mr. HUNT. Well, she does appear to use it regularly, evidently. When this happens, she will, as you say, get fraud alerts from the bank.

Now, that could have been anything from—we might have been in a taxi in a particular location and they scribbled down the number when they had physical access to it. You give it to someone at a restaurant, they go behind the counter. It could have happened

in an incident like that. It could have been that a single merchant resold the data after purchasing something online.

Now, that's not necessarily the same as someone who was a malicious party came along, found a vulnerability in software, and sucked out a million different records in one go.

Mr. COLLINS. Yes. So I wanted to kind of make—because I think sometimes we confuse the two and I think most of us are impacted by somebody grabbing our credit card more than not.

Then we got to go to the inconvenience—getting a new card, set up on autopay. You know, I probably have to do that three, four times a year, even.

So here we are talking about data breach. So now it begs the question, when someone is getting that, and I certainly understand someone, if they had enough, could try to apply for, I don't know, a mortgage or something.

But that probably doesn't impact too many Americans as much as somebody stealing their credit cards.

So it kind of begs the question, these data brokers, as we call them—it sounds like a business because there's guys—and it sounds like they're—are they continuing to try to fill out, you know, for, you know, myself, you know, there's people with my same name, so I don't know.

Are they sorting by my last name? My first name? My middle initial? As they find out that I, you know, just went to the SPCA and got a new cat, you know, what's the cat's name.

You know, how are they sorting this? By Social Security number? By address, in multiple ways, and as you said, trading baseball cards—are they doing this for fun? And then once they have it, and they're just out there selling it, why can't we catch these guys?

If somebody—I think of Raymond Reddington on "The Black List," you know. He'd be the guy buying this stuff. Why can't we find them, shut them down? And so that kind of general questions. What would you add to that?

Mr. HUNT. I would say one point to maybe sort of disambiguate here is when I made the comment about trading baseball cards what I am talking about is there are a lot of individuals out there who obtain access to data breaches and then they redistribute them between peers—not necessarily commercial legal entities like data brokers such as Equifax but individuals, in many cases children, sitting in their bedroom going, hey, I've got a data breach—you have got this one—let's swap and we'll build up these personal collections.

Now, that is not necessarily with malicious intent but it does lead to the redistribution and the growth of the amount of data that's out there.

And then in terms of the data brokers, in terms of the legally operating entities, very often they refer to data enrichment, which is like let's just get as much data as we can about the individuals, refine it so that we have very, very clear pictures because that makes the product that they offer that much more valuable.

And then whether they sort it by your Social Security number or your name or your job title, whatever it may be, that got significant amounts of data that they can offer people, whatever sort of sorting or filtering mechanism they like.

Mr. COLLINS. So in this case, you're referring to a data broker as a legal entity—

Mr. HUNT. Correct.

Mr. COLLINS [continuing]. Not a blacklister that's out there selling it?

Mr. HUNT. That's right.

Mr. COLLINS. All right. So the folks that are out there selling it on the darknet or whatever, just walk us through—we don't have a lot of time—how are they finding their customers, verifying it is not an FBI or somebody under cover?

Mr. HUNT. Well, they don't always get that right.

[Laughter.]

So how are they selling it? Well, very often we see data breaches being traded on the same sorts of marketplaces that are trading things like drugs.

So we have seeing very prominent darkweb Web sites—the Silk Road, Hansa Market, AlphaBay. Now, many of those services have now been shut down but others have emerged in their place and they operate on Tor hidden services on the darkweb, which does make it very difficult many times to actually track them down. So they operate illegal marketplaces and data breaches are another commodity like heroin.

Mr. COLLINS. Well, I appreciate all your comments. My time is up. I yield back, and thank you for coming up from Australia.

Mr. GRIFFITH. I thank the gentleman for yielding back.

I now recognize Mr. Tonko of New York for 5 minutes for questions.

Mr. TONKO. Thank you, Mr. Chair.

In recent years, as breaches have become more common, companies and technology have not kept pace to protect consumers. As more breaches occur, more consumers are at risk for identity theft and other crimes.

While progress has been made, we must do much more to, obviously, protect consumers. Many ongoing concerns were brought to the forefront once again with the Equifax breach. More than 8 million New Yorkers were affected by the Equifax breach including many of my constituents.

One constituent, who I will label as Lee from Albany, asked Equifax, why are you using this gross misconduct to turn your victims into customers for a paid monitoring service that you will profit from.

Mr. Mierzwinski, can you speak to Lee's concerns that companies are profiting off these breaches?

Mr. MIERZWINSKI. We think it is outrageous and we wish it would stop. The companies have turned consumers into cash cows.

They're responsible for keeping our information safe and keeping it accurate. They don't, and so instead they say, you better buy this credit monitoring service at \$19.95 a month, and the marketing of these services is extremely deceptive. Several banks have been fined by the bureau and several of the credit bureaus have been fined by the FTC.

A third party company, Lifelock, has been fined by the FTC and numerous State's attorneys general. After it violated the terms of

its settlement order, it was fined an additional \$100 million for contempt.

So the marketing of credit monitoring is unfair, and you don't need credit monitoring either because you can get your credit report for free under Federal law. In seven States, you can get a second credit report for free from each of the three companies.

If you file a fraud alert—a 90-day fraud alert—after you have been a victim of a breach, you could get an additional free credit report, get them every three months, and you have got your own free credit monitoring.

But Equifax should not be profiting. We'd like to put a stop to it and we'd like them to not charge consumers for freezing.

Mr. TONKO. Thank you.

And Mr. Mierzwinski, again, you discussed the privacy risks that come along with biometrics. Can you elaborate on these risks?

Mr. MIERZWINSKI. Well, very simply, I think that as we put our biometric information into databases, it becomes another commodity in the cloud.

It becomes another way that you can steal information about a consumer, if you steal my fingerprints or my retina scan, it's—you could clone yourself as me in a lot of different ways.

I am not an expert on whether that is being done yet today, but we are very concerned and also concerned about the civil liberties aspects of Government agencies getting access to the information in the databases without warrants, et cetera.

Mr. TONKO. Mm-hmm. I thank you for that.

And a 2017 New York Times article described the nightmare that Americans face when confronted with identity theft. The article referenced a study on identity theft and pointed out that, and I quote, "Last year, 15.4 million American victims of identity theft lost \$16 billion."

The article continues, describing cases where Americans were denied the ability to refinance their mortgages or tax refunds were fraudulently sent to hackers and other similar cases.

So Mr. Mierzwinski, many companies use certain information to verify someone's identity like a full name, home address, and Social Security number. Now with the data for nearly half of Americans stolen, is it true that malicious actors could retrieve those identifiers?

Mr. MIERZWINSKI. Absolutely malicious actors can retrieve your information in a variety of ways. They can even retrieve more information if they've only obtained some.

So the Yahoo breach largely obtained for the bad guys phone numbers and email addresses. That's the way that you can then conduct phishing and spear phishing exploits to get more information from consumers or even call them on the phone and say, "I've got your Social Security number. I am going to read part of it to you. You read the rest of it to me"—those kinds of gimmicks—social engineering. It is easier than hacking, actually.

Mr. TONKO. Mm-hmm. The article also makes the case that we shouldn't necessarily get rid of using Social Security numbers to identify someone but that we should stop using it as an authenticating factor.

Mr. Grant, do you agree with that?

Mr. GRANT. Yes. I wrote an op-ed that was published in The Hill about a month ago that made that same point. I think we need to understand how Social Security numbers are both an identifier and an authenticator and essentially stop recognizing them for use of the latter. If I call my credit card company and they ask for the last four of my Social Security number, my answer should be, "Why in the world would you think that me knowing that actually proves that I am me?" My information has been stolen several times over. It could be anybody who's calling in making that claim.

But as an identifier, look, identifiers are needed in the modern economy. The Government needs a way to track how much money I am making from both my job and my bank accounts. You know, individual companies need an identifier as well.

Let's just treat it as something that's widely available and I think once we acknowledge that it is not something that is a secret, then we can start to focus on what comes next, which are better solutions for identity verification, better solutions for authentication that don't have the weaknesses that the ones that we are using today have.

Mr. TONKO. Thank you.

And with that, I yield back, Mr. Chair.

Mr. GRIFFITH. I thank the gentleman, and now recognize Mr. Costello of Pennsylvania for 5 minutes for questioning.

Mr. COSTELLO. Thank you, Mr. Chairman. I am going to try this with my voice.

To all three of you, I am just going to read through a series of questions and ask that you weigh in as appropriate.

You spoke in your testimony about the role of Social Security numbers, both as they are used now and as they should be used in the future.

In particular, you're both adamant that we don't need to replace Social Security numbers, as some have suggested we need to.

Instead, you have said that using them—or, the need to change them, from using them as identifiers and authenticators to using them solely as identifiers.

My questions are oriented in this fashion. Are there barriers to moving away from Social Security numbers as both identifiers and authenticators? For example, are there Government regulations that require them in certain instances?

Are there private sector standards that recommend or require their collection? And how will these organizations begin making the change you suggested?

How expensive both in terms of time and resources would this change be and are there any potential down sides, and if so, what are they?

Mr. GRANT. So I am happy to jump in with that first.

I think one point you raised is there are a lot of entities that are required to collect my Social Security number.

I started a new job at Venable five months ago. They needed to know my SSN. Any bank account that I open they need to know my SSN. And that's for the purpose of an identifier and I don't know that there are any real issues there with them continuing to use that.

There are issues that are out there in terms of, you know, particularly when opening financial accounts. I mean, one big problem we have in this country is what, you know, many people refer to as synthetic identity fraud—when you'll see fraudsters try and combine a real name and a real Social Security number that don't match and then start throwing it into the system in an attempt to establish credit, and that's, you know, one way that, you know, organizations are then defrauded or people are defrauded.

I mean, so, you know, I think there's good reasons to keep using the SSN as an identifier but we could also use better systems to verify.

One of the things I talked about in my opening statement was what Government could actually do as a provider of identity verification services themselves.

The Social Security Administration knows that there's a Jeremy Grant that has my Social Security number that matches but if I go to open a new account at a bank today or a mobile network operator or anybody else who's collecting it, there's no way to electronically verify that with Social Security that that really matches up.

There's a paper-based system that requires a wet signature. It was a great thing 20 years ago. It is 2017 now. I think you could actually help cut down on fraud in new account opening if there was an electronic way for Social Security to validate those numbers if queried.

I think where there's going to be bigger issues—you were asking about barriers and costs and things like that—is where we replace the Social Security numbers and authenticator.

So I can make fun of the credit card company I called last week who asked for the last four of my Social Security number and, obviously, there's no security value to that in 2017.

But their next question is, well, then how do I authenticate you when I am talking to you on the phone, and that's a much harder question. I think there's some interesting products. There's new standards that are emerging. There's—there are ways that you can do it. But there tends to be—the pace of adoption tends to lag the creation of new technology.

And so I think this is actually an area where I would love to see Government partnering with industry focus more is how can we identify where those are—where there are promising technologies that could replace the first-generation tools that have, you know, started to fail and accelerate the pace of adoption everywhere.

Mr. MIERZWINSKI. I agree.

Mr. COSTELLO. That's a good answer.

Mr. MIERZWINSKI. Yes. Try to keep some of your time for you.

Mr. COSTELLO. Very good. I will yield back, Mr. Chair.

Mr. GRIFFITH. I thank the gentleman for yielding back.

I now recognize Ms. Clarke of New York for 5 minutes for questions.

Ms. CLARKE. I thank you, Mr. Chairman. I thank our ranking member. I thank our panelists for their expert testimony here today.

And I wanted to bring up the National Strategy for Trusted Identities in Cyberspace. Under President Obama, the White House re-

leased this strategy and this spurred the public and private sectors to collaborate on issues related to identities and online transactions.

Mr. Grant, is it accurate that this strategy laid the framework for privacy-enhancing technology as well as identity solutions that must be secure and cost effective?

Mr. GRANT. Well, I would say it helped. I think where NSTIC really helped was throwing down a marker in 2011 for an industry that, you know, hadn't really started to think about this yet, and when I look at the impact several years later, you know—I talked about this in my written statement—companies that liked it came in and said, hey, "Hey, this is a great idea. How can we actually work with you to come up with solutions that align with it?"

Even companies that didn't like the fact that the Government had thrown down a marker still had to pay attention to it because their customers were focusing on it.

So when I look at where the market is today, look, we still have plenty of problems in the identity space. We wouldn't be having this hearing if it wasn't the case. But I think the strategy helped and some of the specific activities that we—that we sponsored and funded out of NIST during the time that there was a national program office implementing NSTIC really helped to move the market along at a point much faster than it would have gone otherwise and, you know, also pointed the way to, you know, create the—you know, just pointing out basic things like security doesn't have to be at odds with privacy.

Security doesn't have to be at odds with user experience. Those are concepts—it is not a radical statement to make, but there were some vendors in the space who seemed to think that they were going to be at odds, and this helped to show that there could be other ways.

Ms. CLARKE. So what—can you elaborate a little bit more as to what a privacy-enhancing solution may look like in the age of data breaches?

Mr. GRANT. Sure. So, you know, the concept of privacy enhancing it is, you know, how does—how do you create solutions that can actually give people more control over their personal information—have more choice in terms of what attributes they choose to share about themselves when they go online.

And, you know, it is a catch-all term. But in terms of practical application, I think it is, you know, something you see today. Let's say you're logging in to a Web site with a social provider and they now give you radio buttons that, you know, let you choose—do I just share my name?

Do I log in anonymously or do I share—let's say it is using Facebook Connect—a whole bunch of information about me with that site. That's, you know, one example of giving consumers choice in a way that's also pretty easy to select, you know, with radio buttons, for example, that you can click on or off. That is something that we didn't have in the marketplace before.

I think there's other interesting approaches. You know, people can get—we could really go down the rabbit hole in terms of talking about privacy-enhancing encryption, which is an area that I will say there's been a ton of R&D done but I would say we still

have barriers in the marketplace in terms of coming up with systems that can scale.

I know there's really a commercial—a need for. We, you know, funded a lot of research there as well and NIST continues to do good work there today. That's probably some of the next generation work, I think, in terms of where the market focus is next.

Ms. CLARKE. So can you tell us the benefits of a universal two-factor authentication or similar types of technologies that secure a user's identity?

Mr. GRANT. Well, it is a universal two factor. Whether it is universal or whether you're just using two-factor authentication everywhere. You know, I mentioned in my opening statement 81 percent of breaches last year were caused by exploiting passwords.

There is a reason for that. The password is really easy to compromise and the notion that there's such a thing as a secure password just doesn't make sense. You know, a lot of the attacks we see these days are spear phishing attacks where you get something that looks like a normal login to your email provider or your bank but it is not. It is somebody who's inside trying to phish your user name and password.

If you have unphishable two-factor authentication behind it, that attack doesn't work anymore. Although one problem we are actually seeing in the marketplace is some of the first-generation tools that we have seen for two-factor authentication—things like getting a code through SMS or, you know, through an app on your phone.

That is phishable as well. And so, you know, I keep making the point we had solutions that were good for a while and now the attackers have caught up with them.

Moving to unphishable authentication—you know, we have talked in this hearing about, you know, standards bodies like the FIDO Alliance that are coming up with solutions based on public key crypto, which is unphishable. That, I think, is where, you know, we need to focus there.

Ms. CLARKE. Where we need to go. OK.

And just sort of in closing, you know, I am glad that we somewhat have a roadmap to improve the security of our online identities but it seems that more efforts are needed to implement these effective solutions and we need to continue to evolve, as you have stated, because we sort of get static after a while and, of course, there are those who are out there constantly working at how to phish and break through.

So thank you for your response today. Hopefully, we will heed what you have shared with us today.

I yield back, Mr. Chairman.

Mr. GRIFFITH. I thank the gentlelady for yielding back.

I now recognize Mr. Walberg of Michigan for 5 minutes of questions.

Mr. WALBERG. Thank you, Mr. Chairman, and thanks to the panel for being here.

Mr. Hunt, I appreciate you coming all that distance. In fact, I've often had some sinister thoughts of sending some of these hackers, et cetera, back to Darwin, Australia, and let them confront some

of the wildlife there in that beautiful but dangerous part of your great country. But I won't suggest that.

One of the reasons that we are having this hearing today is to shine a light on a problem that we think is getting worse, namely, that there is so much data available on individuals from these various breaches that malicious actors can package or enrich data to create very robust profiles of almost any given person.

Is that something that you have seen or heard about and if so is it a growing problem?

Mr. HUNT. Yes. Look, it is certainly a concerning thing because, obviously, the more personal attributes you can gather about an individual the richer the picture you have.

And then when it then comes to things like knowledge-based authentication you start to build up many different attributes. And in my written testimony I talk about the concern of aggregating from multiple services, and they're not always data breaches either.

So someone might take certain attributes from one data breach—let's say a name and a birth date. They'll go to another data breach and they may get gender and home address.

And then they'll go to open source intelligence sources such as LinkedIn, Facebook, Twitter, and aggregate further data attributes from there—your profile photo, your social connections. And the real concern I have there is that even beyond just data breaches alone there are so many sources of information that we literally willing publish ourselves publicly that we now have to start to work on this assumption that so many known attributes about ourselves, which we did previously consider to be personal attributes, are now public and that's the concern I have. There's just so many different sources and it is not just data breaches.

Mr. WALBERG. And that's what makes it so valuable then, that—

Mr. HUNT. Oh, absolutely, and I can see why the likes of legally operating data aggregators are running great businesses these days because there is so much data that they can obtain from us.

Mr. WALBERG. Yes.

Mr. Grant, as former head of NSTIC, this is likely an issue that you're familiar with as well. Did NSTIC look at this kind of problem and, if so, what were its conclusions and recommendations?

Mr. GRANT. So I would say we spend a lot of time looking at it in the Trusted Identities Group and NIST continues to focus on this.

You know, I think probably the most—well, there's a lot of things that NIST has done in this space that's been impactful.

But one that I would point to are the updated digital identity guidelines. One of the NIST special publications, 800-63-3, is the title or the code that was put out this past summer, which was an effort led by my old office to basically take a look at what is the modern state of solutions in terms of what we can use for identity verification and authentication in the marketplace and also recognize where some of the attackers have caught up with some of the old technologies.

And so they published new guidance this past summer which I think—you know, what's been nice about it is not just in Government but also a number of entities in industry have looked at this

and said, this is fantastic—this is a guidebook that we can use as we are building solutions for the private sector to make sure that we are, you know, both taking into account new technologies and new standards that are emerging—things like FIDO as well as make sure that we are not using some of the legacy solutions that just aren't as good anymore.

So, you know, certainly, in the topic of identity verification, one of the things that the new guidelines did was diminish the role of KBA in terms of how much you can trust it for identity proofing.

It establishes that there's still a role for it in the process of identity resolution, you know, trying to figure out whether I am the Jeremy Grant who's actually applying for an account but says you cannot use it alone for, you know, full-blown identity verification. That was a big change from what we've seen in the past.

So, you know, one thing I mentioned in my written testimony some of the budget for NIST work in this area has been proposed for a cut in 2018 at a time when everybody's looking at, you know, where we can actually take some actions after events like the Equifax breach. I think we, you know, are going to continue to need more funding for research and standards in this area, both to help Government implement better solutions as well as the private sector.

Mr. WALBERG. What updated standards are you talking about there?

Mr. GRANT. There is updated—well, I think there's other work to be done still. So I think NIST has put out digital identity guidelines.

I would say two things. One, attackers are always evolving and technology is always evolving and so it is something that should be updated I would say, you know, on a regular basis rather than, you know, a cycle that's every 5 or 10 years, which is often how NIST tackles the special publications.

Beyond that, I think there's other research for areas. You know, for example, one of the questions that Mr. Hunt was asked before was about the security of cloud services and how entities are getting into that.

And often, again, the attack vector there when you're guarding against big enterprise class data breaches is through identity.

I think NIST could do a lot more work looking at enterprise identity and how you actually manage administration, authentication, authorization, analytics, and audit—what I call the five A's of the identity life cycle.

There is not great guidance out there anywhere in the world and NIST is really well poised to help enterprises apply better identity security.

Mr. WALBERG. Thank you. My time has expired.
I yield back.

Mr. GRIFFITH. I thank the gentleman for yielding back and now recognize Representative Jan Schakowsky of Illinois. The gentlelady is recognized for 5 minutes.

Ms. SCHAKOWSKY. Thank you so much.

As we talk about consumer protection, which has really kind of been my bailiwick for a very long time, I have to mention what's going on right now at the Consumer Financial Protection Bureau.

OMB Director Mick Mulvaney is serving now as acting director as his appointment continues to be challenged in the—in the courts and Mr. Mulvaney has been pretty much a longtime opponent of the CFPB and no friend of consumer protection regulations.

He has already put a hiring freeze and a regulatory freeze in place at the agency. So Mr. Mierzwinski, I wondered if you could just share your thoughts on what is currently going on at the CFPB and perhaps how it relates now to this issue also of data protection, et cetera.

Mr. MIERZWINSKI. Well, thank you, Congresswoman, and of course, the Consumer Bureau was created after the big collapse of the economy and it was designed to be independent of the political process that has corrupted a lot of the control of how we protect consumers in the financial system.

By appointing—by suggesting that the head of the OMB, a deeply political agency of the White House, could also at the same time be the director of the independent Consumer Bureau, we just don't think that computes and we support Director Cordray's appointment of Leandra English as acting director.

We truly recognize the president has the authority to eventually nominate and get someone confirmed by the Senate. But we hope that person is qualified as a consumer advocate and is not someone who has attacked the bureau and called it a sick, sad joke, as the current acting director has.

The Consumer Bureau, in just 6 years of existence, has recovered over \$12 billion—about \$12 billion for 29 million Americans and has restored confidence in the financial system.

So we like—we'd like to protect it. Going forward, you have pointed out one issue that is in conflict there is actually data security. Interestingly, the Consumer Bureau gained authority over Equifax when it sells credit reports through the Fair Credit Reporting Act.

But the Gramm-Leach-Bliley Act under the Federal Trade Commission still controls on data security for a number of nonbanks including the credit bureaus. That's a real problem.

Ms. SCHAKOWSKY. Yes, although before he left, Chairman Cordray said that he thought that there ought to be embedded regulators at Equifax and companies—and the other companies.

Mr. MIERZWINSKI. Well, actually, he does have the authority or he did have. The bureau still retains the authority to supervise Equifax in the same manner that bank regulators including the bureau supervise banks, meaning the ability to be there in an embedded basis and look for problems before they get bad and also to look at the toxic—not the toxic but the secret sauce that the company uses to generate its credit scores.

There are a lot of things that the bureau can and should do. But there is this one little piece of Gramm-Leach-Bliley that says the Federal Trade Commission is still the regulator for when you have a breach, when you have to notify.

The Federal Trade Commission rule still has not created a notification standard at the Federal level and this is something people may not be aware of. The Federal Trade Commission under Gramm-Leach-Bliley cannot impose a penalty for the first violation of the data security rules.

The bureau can and any bank regulator can impose a penalty for any first violation by companies they regulate. The Federal Trade Commission cannot.

Ms. SCHAKOWSKY. So regardless of how big the breach is, how many people are affected, they do not have the authority?

Mr. MIERZWINSKI. Not under their statute and not under their regulations. They've never done it so I don't believe they have the authority and it is been confirmed to me by former staff there.

Ms. SCHAKOWSKY. Oh, I see. Do I have time?

Well, let me see if I can get to one last question and that is about credit freezes. So the long-term risk from data breaches underscores the need for strong data security and breach notification legislation such as the—I have a bill called the Secure and Protect America's Data Act that I introduced with Ranking Member Pallone, several other members of this committee.

So, again, Mr. Mierzwinski, when a company fails to protect consumers' data, then where does that leave the consumer? And let me just add also in the wake of the Equifax breach you have talked about making credit freezes free for consumers. How would that help?

Mr. MIERZWINSKI. Well, how—making credit freezes free would give us control of our own data, and by the way, that has almost become a bipartisan issue.

The next step is to make credit freezes the default on switch. Make the consumer information always protected until the consumer agrees to turn it on.

Ms. SCHAKOWSKY. So the—

Mr. MIERZWINSKI. The opposite of the current situation.

Ms. SCHAKOWSKY. OK. Thank you so much. I yield back.

Mr. MIERZWINSKI. Thank you.

Mr. GRIFFITH. Appreciate the gentlelady yielding back.

I now recognize the gentlelady from Indiana, Mrs. Brooks.

Mrs. BROOKS. Thank you, Mr. Chairman, and thank you to all of our witnesses for being here.

I am a former Federal prosecutor—former U.S. attorney that worked on and prosecuted identity theft cases between 2001 and 2007. So this is certainly not something new.

I haven't heard very much, quite frankly though, about going after the bad guys, and we are talking about the hackers and I want to learn a little bit more.

And Mr. Hunt, when you talked about the analogy of it is like shopping for heroin or so forth on the darknet and so forth, could you please talk with me a little bit more? Because I haven't been in that world, quite frankly, since '07 and really want to learn a little bit more about the buyers, the sellers, and how do they purchase it, select their buyers and sellers.

Do they earn reputations on the darknet? Can you tell us a little bit, and then for yourself and maybe Mr. Grant a little bit about what kind of cooperation you have engaged in with law enforcement.

Mr. Hunt?

Mr. HUNT. I think we can sort of speak to the last part of the question first, which is around reputation, so how do people establish a reputation.

One of the quite intriguing things when you do see these dark market marketplaces or darkweb marketplaces is that in many ways they look very familiar.

They look like an eBay, for example, and there are buyers and sellers on there that have a reputation that they gain over a series of trades. Now, of course, the difference is they're not buying iPhones or consumer electronics. It is, literally, drugs, data breaches, and so on.

So that's sort of the first part of the answer. The establish a reputation. In terms of then identifying who those parties are, one of the difficulties we have with privacy and anonymity tools is whilst they're very good for maintaining privacy and anonymity for people that want to do good things, they're also very good at maintaining privacy and anonymity for people doing bad things.

Now, we have seen a number of these marketplaces taken down over time but, obviously, they are much harder to track down.

I guess to the other points, one of the things that sort of concerns us is that there is a thriving marketplace for this data and there are, I guess, various shades of gray in terms of who finds this data attractive.

That's, clearly, criminals—those who literally want to go out and mount identity theft attacks. They find this data attractive.

One of the things that worries me a little bit more is that it is also an attractive piece of information for more mainstream legitimate organizations who are looking to gain access to this data so that they can figure out which of their customers are protected.

So we are now seeing very mainstream online web properties that many of us know and use on a daily basis that will tell people when they have appeared in a data breach and some of these are actually purchasing information in order to gain access to that to protect their customers.

And, frankly, that—I am a little bit torn with that because I understand the desire to protect their consumers but I also worry about the incentives that provides those who are breaking into systems.

Mrs. BROOKS. Mr. Grant, anything you want to add?

Mr. GRANT. Not too much. I mean, my—look, law enforcement is quite important. It is—I think as Mr. Hunt pointed out, it is becoming quite hard to attract people down in part because of the international nature of, you know, many of the criminal rings that are actually running all of these, you know, marketplaces and what not.

I would agree in terms of what, you know, Mr. Hunt said as well in terms of the same tools that can protect us and keep us anonymous can also be protecting them. So there are definitely challenges there.

Mrs. BROOKS. Has there also been evidence that nation-states besides entities, individuals, criminal organizations are involved in this as well?

Mr. GRANT. Absolutely. I mean, that's something we haven't talked about much. I am sure most of us in this room were victims of the OPM breach, which I guess I appreciate that the Government is giving me credit monitoring services for this.

I don't think that the government of China is looking to establish credit in my name. They're interested in looking through the 75 pages or so of my SF-86 and figuring out if they can compromise me because I have a top-secret clearance.

But this is certainly something that has been quite interesting to other nation-states who are looking to execute attacks, you know, both for those purposes as well as just for, you know, getting into basic accounts.

Again, if we are protecting access to an account with only something like static KBA and they've now stolen the answers to those questions, well, then you can get into them and do things with them.

You know, likewise, Mr. Mierzwinski talked before about, you know, some of the risks of biometrics. All of my fingerprints are now sitting in another country somewhere because of the OPM breach, which means I wouldn't feel particularly comfortable using anything that's doing remote match fingerprint to secure anything that I care about.

That said, I am really comfortable with using a fingerprint on my phone because you have to come get my device out of my hands first before you can compromise it.

Mrs. BROOKS. Mr. Mierzwinski mentioned that the credit monitoring services maybe have been not very honest in their practices.

Do you agree that when we receive these requests after we've been a target of a breach that people should or should not be accepting those services by the company?

Mr. GRANT. You know, I don't think it hurts to accept them. Whether you pay for them is another question that I think—

Mrs. BROOKS. Right.

Mr. GRANT [continuing]. You know, folks are asking right now. Look, I think they are helpful because it is good to know if something is happening. It is good to be able to monitor your account.

Whether you need to pay for it is another question. From, you know, the Government perspective as a victim of the OPM breach I don't know what value it offers me other than it is nice thing to have to be able to keep close watch on my credit.

So it—you know, value in the service, yes. Whether, you know, I want to pay for it as a consumer that's another question.

Mrs. BROOKS. Thank you. Thank you all for your work.

Yield back.

Mr. GRIFFITH. Thank you.

I now recognize the gentleman from Georgia, Mr. Carter, for 5 minutes of questioning.

Mr. CARTER. Thank you, Mr. Chairman, and thank all of you for being here and for your efforts to get here. Appreciate it very much.

This is, obviously, very, very important to all of us. I want to start with you, Mr. Grant, and just ask you if you can, and please dumb it down for me, if you will, what are trust marks? Can you just explain that to me?

Mr. GRANT. Trust marks—sure. Best example of a trust mark is the Visa logo that's on two credit cards in my wallet.

So that if I go down to the cafeteria here afterwards and have lunch with Troy or Ed, the cafeteria doesn't really care which credit

card I pay with. I got one issued by Capital One and one issued by Chase.

Because it is got that Visa trust mark on it, which stands for a bunch of standards and operating rules that govern everything from how that card's authenticated at the point of sale terminal, what security is in place, how long it takes for my bank to pay the cafeteria for my lunch, what transaction rate that they're actually going to pay in terms of, you know, the fee for processing that, and some would argue most importantly if—let's say Vice Chairman Griffith steals my credit card and buys lunch for the committee and I contest that with my bank—what am I liable for and what's the merchant liable for.

So the trust mark is essentially something that represents all those standards and operating rules that in the credit card network everybody who's an issuing bank has to follow and everybody else has to follow.

In the identity space, one argument—this was a lot of the focus of NSTIC is that we need to create something similar to the Visa network before identity, which is that I could have the issuer be my State DMV or the Social Security Administration, my bank, my mobile network operator.

It could be an advocacy group like the NRA or the ACLU or U.S. PIRG, who all could validate my identity a certain way, issue me a credential that I could use everywhere and the reason it would be trusted is because it has that trust mark.

Mr. CARTER. Well, that's really what I am getting at because as I understand it, the Trusted Identities Group has actually farmed out, if you will, pilot projects and the Georgia Tech Research Institute has actually come up with the emphasis on the machine-readable trust marks, and it is been very successful and the results have been positive, particularly when it was—when it was over a trusted framework and that would encourage greater trust.

How can this be implemented in industry? How can we use this?

Mr. GRANT. So I don't think—you know, a little bit of background on the GTRI pilot that was one of the ones that I selected for funding when I was, you know, running the NSTIC program and the idea was, you know, how can you do something for identity that's, you know, similar to what you see in financial services.

I would say, you know, where it has gone as a pilot, it was a great—look, it is a pilot. It is a proof of concept, basically. It isn't something that's been picked up yet by industry.

What I can say, though, is that work is being looked at by—I don't want to break confidentiality with anybody I am, you know, doing work with now.

Mr. CARTER. Right. Right.

Mr. GRANT. But some bigger players that matter in the ecosystem who are actually looking at taking that similar concept and actually developing a, you know, broader federated identity system that could be led by the private sector for making it easier for consumers to identify themselves.

The idea would be to basically leverage work that's being done there already with I can actually say some financial services.

Since banks know you, thanks to the Know Your Customer rules that they go through and you might trust your bank—not every-

body does but some might—how could they vouch for you other places when you're looking to open up a new account.

Mr. CARTER. Right. But do you agree that this is kind of the route we ought to be going?

Mr. GRANT. I think—yes, I think it is a big part of the solution. I don't know that trust marks are going to solve everything. You know, look, so we did some good things with NSTIC.

One of the things we didn't do is solve all the problems and it is because it is really complicated and there's a whole bunch of, you know, whether it is legal barriers, technical barriers, how do you create something that's really easy for consumers to use. There's issues that are out there.

For as much as everybody loves to beat up on KBA and what the credit bureaus do, there's a reason it is been used so much in the market for years because that for many people it is work.

Mr. CARTER. Right.

Mr. GRANT. I am applying for a new credit card. I can do something instantly. When I went to lease a new car for my wife a year ago, I was able to get quick credit.

So I don't want to suggest we throw the baby out with the bath water because there's problems. It is more realizing where attackers have caught up and how do we develop better solutions.

Mr. CARTER. OK.

Mr. Hunt, any—any comments on trust marks and how it can be implemented into the private sector?

Mr. HUNT. I think I would probably defer back to Mr. Grant as the expert on trust marks there.

Mr. CARTER. Right. Right.

Were there any other new technologies that you find interesting and perhaps that have some potential?

Mr. HUNT. I think ultimately we are going to see an augmentation of different practices. I mean, many people, for example, say, well look, is the answer biometrics or is the answer physical tokens.

And where we are getting to now is I think an acknowledgement that we can't rely on one single knowledge-based authentication attribute, for example—that we do have many other things available to us now that we didn't have, say, two, decades ago.

We have ubiquitous mobile devices with internet connectivity. We have SMS. We have other forms of identifiers like physical YubiKey tokens, for example. And I think the right strategy moving forward is going to be the right augmentation of those under the right scenarios, depending on the trust level that you need to establish.

Mr. CARTER. Great. Thank you all again, and I yield back.

Mr. GRIFFITH. I thank the gentleman for yielding back. I do have a couple of follow-up questions just to try to clarify some things. Staff did a nice job, as they always do, in educating me beforehand. But, Mr. Grant, you used the term public encryption.

Mr. GRANT. No, public key crypto.

Mr. GRIFFITH. Oh. And what does that mean?

Mr. GRANT. Well, so there's—we can get really geeky talking about cryptography now—there's essentially two ways you can manage cryptographic keys.

One is called symmetric-key, which is when I got a key and you know the key, and I have to present the key to you for it to match. It is a lot—similar to the way passwords work.

The other is what's commonly known as asymmetric public key cryptography, or PKI for public key infrastructure. It is what the Defense Department as well as the Federal Government had been using for years, in many cases in lieu of passwords, in order to, you know, come up with unphishable authentication to protect Federal networks and systems.

At the end of the day, the concept is rather than each entity having the same key, I get a key pair, and the public key is known to everybody but the private key is only residing with me.

It can be in my mobile phone. It could be in my computer. It can be on a device like the YubiKey, which is—that Mr. Hunt mentioned which is a FIDO standard token, and when I am logging in someplace, I am basically asked to sign a cryptographic challenge where my public key is presented but the only way I can get in is if I have the corresponding private key with me physically.

And so the—we could really go into the details of it in ways that would make everybody's head explode. It is not—this is actually one of the problems with—about the adoption of technology, by the way.

It has been very complicated. But I think the most important point to keep in mind is it is a way to deliver unphishable authentication. It is not based on shared secrets.

And when I talk about how attackers have caught up not only to passwords but also things like SMS codes or other one-time passwords that are only good for 30 seconds, you know, that 30 seconds is still enough for a moderately skilled attacker to phish my authentication code.

Asymmetric public key crypto is where we should be building authentication solutions in the future so that we don't have phishable authentication.

Mr. GRIFFITH. All right. I appreciate that.

Mr. Hunt, you travelled a long way. Is there anything that you had a burning desire to tell us that you haven't had an opportunity already to do so?

Mr. HUNT. I think that the other thing I would add, obviously, I am very interested in how do we stem the flood of data breaches that we are seeing. And, you know, the things that really come to my mind that I would love to see implemented I mentioned education.

So we are making lots of fundamental little mistakes. Another thing that's very important is making the disclosure of these incidents much easier.

So I myself have been in this situation many times where someone has sent me data from an organization and just the ability to disclose it to the company, to find the right person who will listen, who will take it seriously, is enormously difficult.

So I am very supportive of some of the initiatives we are seeing like bug bounties. So, for example, companies like BugCrowd are running many bug bounties where you as an organization can say if someone finds something wrong with my systems, I would like

to know about it and I will likely pay a reward for that. And it is done legally, ethically, and it encourages the right behaviors.

And I guess, finally, we'd also like to see more in the way of penalties because at the moment there's not enough accountability when things do go wrong, and I think we are all very curious to see how things like GDPR, which Mr. Grant mentioned earlier, how that plays out when it comes into effect in Europe in May where potentially an organization can be fined up to 4 percent of their annual gross revenue.

Now, that starts to sting and we really hope that that actually drives more positive behaviors in the industry.

Mr. GRIFFITH. All right. I appreciate that.

Mr. Tonko? Ms. Castor?

Appreciate you all being here. This has been very informative. I suspect it'll be one of the more popular reruns on CSPAN, for those folks who are really into this, and I have learned so much.

Thank you all for your time today and I appreciate it.

And with that, got to go to my script so I don't leave anything out. I would remind Members that they have 10 business days to submit questions for the record and I ask that the witnesses all agree to respond promptly to those questions.

Do I need to say anything else? All right. Got all that business—housekeeping taken care of.

With that, the subcommittee is adjourned. Thank you.

[Whereupon, at 11:47 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]



U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

November 28, 2017

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing entitled "Identity Verification in a Post-Breach World"

I. INTRODUCTION

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

II. WITNESSES

- Troy Hunt, Information Security Author and Instructor, Pluralsight;
- Jeremy Grant, Managing Director of Technology Business Strategy, Venable, LLP; and,
- Ed Mierzwinski, Consumer Program Director, U.S. PIRG.

III. BACKGROUND

In recent years, a series of data breaches originating with companies throughout the financial, healthcare, and commercial sectors have compromised the security of personally identifiable information (PII) for hundreds of millions of individuals across the globe. Recent data from the Identify Theft Resource Center (ITRC) indicates that as of November 15, 2017, over 1,100 data breaches have occurred in the United States in 2017 alone, exposing over 171 million records.¹ The compromised data ranges from more readily available information such as full names, emails, and dates of birth, to more highly sensitive information like addresses, work histories, and driver's license numbers. This information, once stolen, can be sold through online forums and is often used to facilitate identity theft and other related crimes.

While any one of these breaches on its own creates serious policy issues, there now exists the potential for malicious actors to combine multiple stolen data sets into one, thereby enabling them to obtain more complete "packages" of identity information.² Given that much of modern commerce relies on a process of remote identity verification known as "knowledge-based authentication" or KBA, through which individuals prove who they are by answering series of

¹ *2017 Data Breach Stats*, IDENTITY THEFT RESOURCE CENTER, Nov. 15, 2017, http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachStatsReport_2017.pdf.

² *The Big Data Breach Suffered by Equifax has Alarming Implications*, THE ECONOMIST, Sep. 16, 2017, <http://www.economist.com/news/finance-and-economics/21728956-financial-industry-worries-about-who-next-big-data-breach-suffered>.

Majority Memorandum for November 30, 2017, Subcommittee on Oversight and Investigations
Hearing
Page 2

questions to which only they – in theory – should know the correct responses, this ability to “package” identity information raises even more significant questions about the reliability of traditional KBA practices.

As such, the effectiveness of KBA has, in recent years, been criticized by some professionals in the financial and information security professions. They point out that, between individuals’ pervasive use of social media and these massive PII breaches, enough information is readily available on almost any given individual to render the ability to answer a series of knowledge-based questions nearly meaningless as an identity verification mechanism.³ Indeed, as more data breaches are discovered and disclosed, the weaker KBA appears.

A. Knowledge-Based Authentication

Knowledge-based authentication is a type of multifactor authentication used to verify users’ credentials for logins and other transactions. In some cases, KBA is also used for password recovery when consumers are unable to access their accounts. KBA relies on the use of “secret questions” that are either pre-established by the consumer or pulled from a profile associated with the user. The former is considered static KBA and the latter dynamic KBA.⁴

Static KBA allows users to pre-select questions to which only they should know the answer. This includes questions such as “What was the name of your first pet?”, “What is your mother’s maiden name?”, and “Who was your first college roommate?”

Dynamic KBA uses information that is, in theory, more secure and questions are randomly generated based on profiles or public records associated with the consumer. This can include credit histories, housing records, and loan applications. An example of dynamic KBA is “Which company issued your 1997 student loan?”⁵ Unlike static KBA, dynamic KBA may give consumers multiple-choice options to answer the questions.

There are issues facing the security of both types of KBA. With the widespread use of social media, consumer’s unique identifiers for static KBA are often available to the public. Malicious actors only need to look through Facebook for familial connections, old pictures of friends, and location information to answer many of the questions posed. In the case of dynamic KBA, the large-scale breaches of consumers’ credit information, social security numbers, and work histories makes it possible for even the most private financial questions to be answered by someone other than the consumer.

³ 4 *Big Problems with Knowledge Based Authentication*, NUDATA SECURITY, INC., Oct. 10, 2013, <https://nudatasecurity.com/blog/risk-based-authentication/4-big-problems-with-knowledge-based-authentication/>.

⁴ Margaret Rouse, *Knowledge-Based Authentication (KBA)*, TECHTARGET SEARCHSECURITY, Feb. 2015, <http://searchsecurity.techtarget.com/definition/knowledge-based-authentication>.

⁵ *Knowledge Based Authentication (KBA) – Out-of-Wallet Questions*, IDOLOGY, <https://www.idology.com/knowledge-based-authentication/knowledge-based-authentication-kba>.

Majority Memorandum for November 30, 2017, Subcommittee on Oversight and Investigations
Hearing
Page 3

B. Public and Private Sector Efforts to Address KBA Issues

i. The National Strategy for Trusted Identities in Cyberspace and the Trusted Identities Group

In recognition of the growing issues with KBA and other associated identity verification challenges, the National Institute for Standards and Technology (NIST) was tasked with developing a framework for secure, reliable online identity verification known as the National Strategy for Trusted Identities (NSTIC). NIST released the NSTIC in April 2011, focusing on the ability to establish convenient, efficient, secure, and innovative identity verification technologies in ways that acknowledged and protected privacy concerns.⁶

After the NSTIC's release, NIST transitioned the effort, along with its statutorily-mandated "Digital Identity Guidelines, Enrollment and Identity Proofing"⁷ to a group known as the "Trusted Identities Group" (TIG). The NSTIC, Digital Identity Guidelines, and other associated NIST efforts now form the primary basis for the government's efforts to leverage more secure, reliable identity verification technologies.⁸ As part of these efforts, the TIG provides funding to companies and organizations seeking to develop innovative new technologies and strategies that meet the NSTIC's goals.⁹

ii. The Fast Identities Online (FIDO) Alliance

Many companies and organizations in the private sector have similarly recognized the inherent risks of KBA, and have created the Fast Identities Online (FIDO) Alliance to collectively explore, develop, and implement more secure, reliable identity verification technologies. Its membership includes large technology companies such as Amazon and Google, hardware companies such as Intel, Qualcomm, and Lenovo, as well as several banks and healthcare companies, among others.

This broad, diverse membership has enabled the FIDO Alliance to propose and develop standards that are deployable across multiple sectors, and that – most importantly – are interoperable.¹⁰ In addition, the Alliance provides its standards for free; companies and organizations looking to leverage them may do so free of charge, and without joining the FIDO

⁶ *National Strategy for Trusted Identities in Cyberspace*, THE WHITE HOUSE, April 2011, <https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf>.

⁷ Paul A. Grassi & James L. Fenton, *Digital Identity Guidelines, Enrollment and Identity Proofing*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, June 2017, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>.

⁸ *Trusted Identities Group – Projects*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, <https://www.nist.gov/itl/tig/projects>.

⁹ *Trusted Identities Group – Pilots*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, <https://www.nist.gov/itl/tig/pilots>.

¹⁰ *Download Specifications*, THE FIDO ALLIANCE, <https://fidoalliance.org/download/>.

Majority Memorandum for November 30, 2017, Subcommittee on Oversight and Investigations
Hearing
Page 4

Alliance.¹¹ As a result, FIDO-compatible technologies are deployed throughout many well-known platforms and companies, including PayPal, Google, Dropbox, and more.¹²

C. Conclusion

While the challenges to identity verification in a post-breach world are well-known, and while both the public and private sectors have recognized the resulting issues and begun efforts to address them, significant work remains. Witnesses at this hearing will provide an overview of the problem, including an in-depth exploration and examination of the data breaches that have created the current climate, as well as provide a discussion of current public and private sector efforts and potential next steps.

IV. ISSUES

The following issues may be examined at the hearing:

- The potential for malicious actors to combine breached data sets to create more complete profiles of individuals.
- The effectiveness of KBA in protecting consumer's private information.
- Potential alternatives to KBA in remote identity verification and best practice recommendations for companies throughout the public and private sector.

V. STAFF CONTACTS

Please contact Jessica Wilkerson or John Ohly of the Committee staff at (202) 225-2927 with any questions.

¹¹ *Id.*

¹² FAQ's, THE FIDO ALLIANCE, <https://fidoalliance.org/faqs/>.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

December 18, 2017

Mr. Troy Hunt
Information Security Author and Instructor
Pluralsight
[REDACTED]
Surfers Paradise QLD 4217
Australia

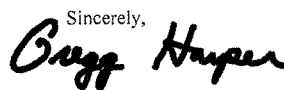
Dear Mr. Hunt:

Thank you for appearing before the Subcommittee on Oversight and Investigations on November 30, 2017, to testify at the hearing entitled "Identity Verification in a Post-Breach World."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, January 8, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Ali.Fulling@mail.house.gov.


Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,


Gregg Harper
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Troy Hunt

 Surfers Paradise
 QLD 4217
 Australia

ATTN: The Honorable Morgan Griffith

Dear Mr. Griffith:

Thank you for the opportunity to testify before Congress in the "Identity Verification in a Post-Breach World" hearing. It was a privilege and I hope I was able to lend a valuable voice to the dialogue.

Please find following the answers to your questions sent following the hearing:

1. **In your testimony, you talked about how data is often "irrevocable" once it's been compromised. In other words, there really isn't a way for a consumer, or even a business, to find their stolen information and "take it back."**
 - a. **Once information has been stolen from an organization, where does it typically end up? Is it someone's personal computer, a hosting service, somewhere else?**

Stolen data may exist in all of these locations. Individuals will keep personal copies on their PCs (their intentions may vary from benign curiosity to malicious use) and hosting services are often used to redistribute this data further afield. Peer to peer torrent services are also frequently used, a perfect example of which appeared only the week after my testimony via a thread on Reddit:
https://www.reddit.com/r/pwned/comments/7hhqfo/combination_of_many_breaches/

Here we have a 593GB torrent of literally hundreds of different data breaches in one handy download. The context of that Reddit thread was that an individual had then taken those breaches, extracted the email addresses and passwords (removing the cryptographic protection that was provided to many of them) and turned it into another torrent of 41GB with 1.4 *billion* credentials. This data is now being actively used to compromise the accounts of victims where they've reused their password across other services.

- b. **Do malicious actors looking to sell this kind of compromised data sell it more than once?**

Yes. A notable example was the sale of the LinkedIn data breach in May 2016 via the seller known as "peace_of_mind" who sold the data multiple times over for as much as 5 BTC each time (about US\$2.2k at the time). In fact, as the data was sold over and over again, the value dropped as the data began circulating more:
https://motherboard.vice.com/en_us/article/53ddqa/linkedin-finally-finished-resetting-all-the-passwords-leaked-in-2012

- c. **Based on your testimony and reporting that we've seen, compromised information, once it becomes well-known that a service has suffered a breach, seems to become much more widely available. Is this true?**

Yes. When a data breach is unknown, the victims have no impetus to protect themselves from this specific risk, for example they wouldn't proactively change their passwords. Once known, a breached organisation will frequently force password resets thus protecting their members. They'll also notify members of the incident which then prompts them to change that same password on other services where they've reused it thus decreasing the value of the data to malicious parties. As that value decreases, there is less value in holding the data and it tends to begin circulating more broadly.

- d. **So, after this whole process, how many copies of a single breached database or set of information might exist?**

Once data begins circulating, it's simply impossible to say. In a case like Ashley Madison where the data was intentionally redistributed as broadly as possible, there would be *at least* tens of thousands of copies of the data and it continues to replicate to this day.

- e. **Even with these multiple copies of information floating around, what makes it so difficult for organizations to find this data and "take it back?"**

It's very dependent on the nature of the breach. Some data breaches may be difficult to find because the data is being quite tightly held; the original attacker may not have shared it or only done so within a small, trusted circle. But then in cases like the aforementioned LinkedIn and Ashley Madison data breaches, that data remains very easily discoverable to this day and both those organisations would have obtained copies of it very early on in order to assess their risk posture.

"Taking it back", however, is a very different story. Digital theft is unlike physical theft in that a stolen item can't simply be retrieved because there is always the risk that other copies remain. I've been involved in data breaches cases in the past where all parties known to have the data have made commitments that they've removed all copies (for example, the Australian Red Cross Blood Service data breach), but this ultimately relies on trusting an unidentified third party that they've kept their word and not redistributed the data or made additional copies. This is why my testimony referred to "there's no putting the data breach genie back in the bottle" because there's (usually) no guarantee that data in unauthorised hands hasn't been further distributed.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

December 18, 2017

Mr. Jeremy A. Grant
Managing Director
Technology Business Strategy
Venable, LLP
600 Massachusetts Avenue, N.W.
Washington, DC 20001

Dear Mr. Grant:

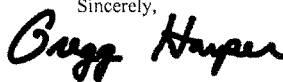
Thank you for appearing before the Subcommittee on Oversight and Investigations on November 30, 2017, to testify at the hearing entitled "Identity Verification in a Post-Breach World."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, January 8, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Ali.Fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Gregg Harper
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Additional Questions for the Record

Jeremy Grant
Managing Director, Technology Business Strategy, Venable LLP

U.S. House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

“Identity Verification in a Post-Breach World”

1. In your testimony, you discussed how certain government agencies like the Social Security Administration are well-poised to help address the online identity challenges we’re discussing today. You discuss a hypothetical service that the SSA could offer that would be valuable to both consumers and businesses looking for identity authentication mechanisms that would essentially make SSA’s current process digital.
 - a. Drawing on your government experience, how would SSA – or a government agency with similar potential – go about creating these types of systems and services?
 - b. What do you think the cost might be of implementing such systems, both in time and resources?

My understanding is that the SSA already offers a digital service today to validate name and SSN through a “yes/no” response, but this service is only available because Congress directed SSA to offer this service in support of two government programs: the E-Verify program and the Real ID Act. Congress specifically authorized SSA to provide this digital service for both programs. However, Congress has never directed SSA to provide such a service for financial institutions or others.

SSA will validate a name-and-SSN combination for opening of accounts at financial institutions if a “wet signature” (ink on paper) is collected from the applicant, through an offering called the “Consent Based SSN Verification System.” (See <https://www.ssa.gov/cbsv/>). That requirement for a wet signature creates notable friction in any online account-opening process; there is no place for ink and paper in digital transactions. The result is that financial institutions generally do not do SSN validation – the current requirements are incompatible with online account opening. It’s 2018 – and it’s time to change that.

While I ultimately defer to SSA on the cost and complexity of implementing such a system, it seems at a high level to be something that would not be overly complicated, especially given that SSA already has created a system to support electronic validation for other programs. I would imagine this existing system could be expanded – though to be clear, I do not want to make any assumptions about the scalability of the current system, SSA should be able to provide the most reliable information there.

Two items to note on the point above:

1. I believe that such a system, would it to be offered to financial institutions and potentially other entities – would be valuable enough to those entities that they would be willing to pay for the service. This would allow the government to recoup the costs of the service.
 2. I can anticipate some concerns, if I was at SSA, about the challenges with allowing hundreds – or potentially thousands – of different entities to have access to the SSA services. This concern could be mitigated by channeling validation requests through one (or perhaps several) hubs – allowing SSA to offload the challenge. This model has been successfully employed in their support of the Real ID Act – rather than each state pinging SSA individually, all validation requests are routed through a system established by the American Association of Motor Vehicle Administrators (AAMVA), who is charged with managing the requests from each state. A similar model could work here for commercial transactions.
2. The federal government is not exactly well-known for successfully designing and implementing complex, large-scale systems such as the one you're describing.
 - a. Do you believe that the federal government has the resources and capabilities it needs to implement such systems?
 - b. Beyond resources and expertise, does the federal government have a plan for designing and implementing such systems, or would agencies tasked with these kinds of projects be starting from scratch?
 - c. What are some of the potential pitfalls of the government undertaking such a project?

As I outlined above, SSA has already designed and implemented such a service. The issue here is more a matter of sorting out:

1. Whether SSA could legally offer this service, or if this would require Congressional authorization
2. Whether the existing service can be easily scaled, or whether it would require a new service to be built.
3. What sorts of policies and operating rules would apply to the new system? For example, would requests be routed through a hub or direct to SSA? What would the cost be, if any, for such a service? If a hub (or hubs) were established, what sorts of requirements would it have to meet?

I would defer to SSA on many of these particulars, as I assume they are in the best position to answer.

One additional note: the question described this system as one that would be “complex” and “large scale.” I am not sure that either of these would apply here. At the end of the day, the idea is to establish a system that would allow SSA to issue a simple “yes/no” response when asked “Do you have a John Doe with SSN 123-45-6789 in your system?” Likewise, other agencies might be asked to establish similar “yes/no” services to validate other identity attributes. Such a service should not need to be overly complex in nature.

3. As we understand it, the FIDO Alliance has already published several standards.

- a. Can you give us some examples of FIDO standards, and what these standards allow organizations to do?
- b. We’ve heard that organizations are now releasing “FIDO-compatible” products, in some cases. Can you give us some examples?
 - i. Do you have a sense of how expensive these types of standards and techniques are to deploy in company products, both in time and resources?

a. The FIDO Alliance initially published two standards, centered around two different multi-factor authentication (MFA) use cases:

- Universal Authentication Framework (UAF). UAF focuses on leveraging 1) the biometrics included in most consumer devices in concert with 2) the hardware-based, restricted execution environments (i.e. TEE/TPM/SE) in these devices, to deliver “single-gesture, passwordless login” experiences.

In this use case, a user presents a biometric to her device to be locally matched on the device; that match then unlocks a private cryptographic key stored in the device that is used to log her in to the service. There is no password required; the two authentication factors are the biometric and the cryptographic key, which together are used to prove cryptographic proof-of-possession. Bank of America, eBay, Aetna and PayPal are among the firms with major UAF deployments.

- Universal 2nd Factor (U2F). U2F focuses on augmenting a password (or other initial login factor) with second factor that is a private cryptographic key, generally carried by the user in a form factor that is separate from her device – such as in a Security Key, for example a Yubikey.

U2F authenticators offer the same level of unphishable security as UAF, but instead of binding a key to a single device, they allow one key to be used across multiple devices. Google, Dropbox, GitHub and Facebook are among the firms with major U2F deployments; U2F is also being used to secure Veterans accounts at the vets.gov site run by the VA.

The two standards have evolved in parallel and share basic FIDO principles such as user privacy protection and use of public key cryptography for unphishable authentication.

FIDO Alliance is now releasing a new suite of standards as “FIDO2” which will harmonize support for the two use cases under a single standard. It will also add support for “device to device” use cases – for example, letting a user use her FIDO-certified smart phone as a second factor to log in to a site on a desktop. That means that someone using their phone for a traditional UAF use case could also use their phone as a distinct second factor when logging on to a separate device such as a laptop (a traditional U2F use case). FIDO2 will allow support for all FIDO use cases to be embedded in all Web browsers, thanks to FIDO’s work with the World Wide Web Consortium (W3C) in creating the Web Authentication standard (<https://www.w3.org/TR/webauthn/>)

I have seen FIDO members continue to enhance and evolve the FIDO standards to support an increasing array of use cases and form factors, with a focus on seeing support for FIDO embedded in most devices, operating systems and browsers in the next two years.

- b. On the topic of products that are “FIDO Compatible” – the actual development here has been the launch of a formal “FIDO Certification” program in 2015. This program allows companies (both FIDO members, as well as non-members) to have their products go through a process to demonstrate that they are implementing the FIDO standards correctly, and in a way that supports interoperability with other FIDO products. Details are online at <https://fidoalliance.org/certification/>

To date, more than 380 products have been “FIDO Certified” – including chipsets from major semiconductor firms that are embedded in devices, standalone devices such as laptops and phones, and commonly-used identity services, such as those run by eBay and Google.

My observation is that pledges by Google and Microsoft to embed FIDO in the operating system (OS) level, as well as in browsers, will make it so that most major consumer devices soon ship with FIDO “built in” – much as most devices ship with Bluetooth and Wi-Fi today. This development is significant: it means that most people will be using devices that support strong, multi-factor authentication based on public key cryptography “out of the box” – making it much easier for app developers and online service providers to deliver strong MFA to users.

In terms of how expensive it has been for firms to deploy FIDO in their products, I do not have specific numbers. However, most firms that I have talked to have reported that building in support for FIDO authentication has been a relatively easy lift, both because it is standardized, as well as because of the way in which the standards were designed – to be easy to implement.

Note that FIDO standards can be downloaded for free from FIDO’s website. In addition, there are a number of freely-available open-source tools to support FIDO implementations, as well as companies who have built products that can be used for these implementations.

4. An issue that we tend to see with efforts to address cybersecurity issues broadly, not just identity issues, is that proposed solutions are often proprietary, which limits the ability of smaller companies and developers to leverage them.
 - a. Are FIDO Alliance standards proprietary?
 - b. How does an organization – large, small, or maybe just a single individual – access FIDO Alliance standards?

FIDO standards are not proprietary.

As I noted in my response to question 3, they can be accessed for free at <https://fidoalliance.org/download/> – anyone can download and use them. FIDO Alliance also allows anyone who is not a member of FIDO Alliance to provide comments on draft public standards.

5. I understand that you led the development of the National Strategy for Trusted Identities in Cyberspace, or NSTIC, on behalf of NIST. The NSTIC was published in 2011, six years ago. Obviously, the situation has developed since then, not simply with regards to the types of information and connected devices that are available on the Internet, but in the sheer number of compromised PII records available.
 - a. How does this affect the findings from the NSTIC, if at all?
 - b. Are you aware of any work to update the NSTIC? Is it a living document that gets updated regularly?

First off, let me clarify that I led the implementation of the NSTIC, but I did not have a hand in its development. NSTIC was drafted by the Obama Administration, through a multi-stakeholder collaborative process that incorporated significant input from the private sector. I was recruited to lead its implementation only after the Strategy was completed and the President was prepared to sign it.

On question (a): while the market has changed significantly since 2011 – as have the threats we face – I believe that the vision and guiding principles laid out in NSTIC are just as relevant today as they were seven years ago.

The NSTIC Vision:

Individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation.

The NSTIC Guiding Principles:

1. *Identity Solutions will be Privacy-Enhancing and Voluntary*
2. *Identity Solutions will be Secure and Resilient*
3. *Identity Solutions will be Interoperable*
4. *Identity Solutions will be Cost-Effective and Easy to Use*

Beyond the vision and guiding principles, there is a healthy debate as to whether some of the specific implementation steps or use cases that were called for are the right ones to follow in 2018, or whether there are new technologies or business models that may allow some of the solutions envisioned in the NSTIC to be delivered a bit differently. But as a guidepost for the industry, it remains a very relevant document.

On question (b): there has not been any effort to update the NSTIC, it is not a living document. It would be worthwhile, in my view, for government to work with industry to evaluate the current NSTIC and contemplate whether changes are needed, particularly in terms of steps government may need to take to address barriers to better digital identity solutions in the market.

6. I realize that you're no longer with NIST, but we understand that you are generally still well informed about their current efforts.
 - a. Could you tell us a little more about the Trusted Identities Group, how it relates to the NSTIC, and how the TIG is working to bring advanced identity verification mechanisms to the federal government and private sector?

The Trusted Identities Group (TIG) at NIST was an outgrowth of NSTIC.

While NIST planned for the formal "National Program Office" for NSTIC to wind down at the end of the Obama Administration, there was a notable portion of the NSTIC work focused on identity research and standards – as well as industry engagement – that was core to NIST's mission, as well as important to addressing current and future cybersecurity and identity challenges.

This portion of the NSTIC work was never intended to wind down; instead, NIST rolled it into the newly-launched Trusted Identities Group (TIG) as part of the Applied Cybersecurity Division at NIST to continue this work and expand on it.

As I noted in my testimony, when I look at the positive impacts of NSTIC, one of the top items has been the emergence of a robust TIG, focused on working with government and industry to develop better standards, guidelines and best practices for next-generation identity solutions. The publication of NIST's updated "Digital Identity Guidelines" this past summer is one

example of the great work that NIST has done here – it’s a document that has been nearly universally praised around the world in taking a forward-thinking approach to digital identity.

Among other things, NIST SP 800-63A – which covers “Enrollment and Identity Proofing” – lays out a modern approach for identity verification that is created to mitigate many of the current threats to legacy identity verification systems.

It is an excellent document, but given that both threats and technology are constantly evolving, it is not one that should remain static.

7. In your testimony, you mentioned that funding for NIST’s efforts in this space is being cut.
 - a. Do you have a sense of why?
 - b. Is it funding for pilots that will be affected, or the office itself?
 - i. What are some of the dangers of the lack of funding?

There are a few issues at play here:

1. NSTIC was initially conceived as a program that would “surge” in terms of resources for several years – then wind down, in part, once these surge activities were complete.

The reason for this was that NSTIC, while a government initiative, called for the private sector to lead development of the identity ecosystem. The role of the NSTIC National Program Office (NPO) at NIST was to coordinate activity across the public and private sectors, with an eye toward tackling barriers to better identity systems and catalyzing the marketplace.

My view when running the NPO was that if we were to catalyze the market, we had to work at market speed – or as close as feasible, given what government can do. That meant that the NPO should not exist forever.

For this reason, parts of the NSTIC budget – specifically, those dollars allocated to pilots, as well as support for the privately-led Identity Ecosystem Steering Group (IDESG) – were expected to wind down. So some of the cuts were planned.

2. However, about 30% of the NSTIC budget supported work on identity research and standards – as well as industry engagement – that was core to NIST’s mission, as well as important to addressing current and future cybersecurity and identity challenges. This portion of the NSTIC work was never intended to wind down; instead, NIST rolled it into the newly-launched Trusted Identities Group (TIG) as part of the Applied Cybersecurity Division at NIST to continue this work and expand on it.

3. Each year I worked at NIST, there was material opposition to funding NSTIC from the House Appropriations Committee. Each year, the White House proposed funding (\$24.5M) for NSTIC, only to see the House zero out this funding; NSTIC was only funded thanks to efforts from the Senate and White House to address these cuts in conference committee, and only at roughly 2/3 of the intended budget.

While I am not privy to budget discussions and negotiations that have taken place since I left government service in 2015, I assume that the change in Administration was a factor that contributed to the language in the proposed FY2018 budget that cut NSTIC funding further – particularly the language in the Trump Administration’s budget proposal that singled out NIST’s work on biometrics for commercial and government applications for cuts. This was notably different budget language than what came out of the previous Administration.

4. Beyond the specific language in the proposed FY2018 budget – the Trump Administration’s FY2018 budget proposal included major cuts to all of NIST, including a proposed \$88.7 million reduction to NIST’s budget for Scientific and Technical Research and Services (STRS). This has created an environment where NIST is being forced to make difficult choices across many important programs.

Given that NSTIC and identity were a priority of the previous Administration – but have not been flagged as a priority of the current Administration – I would not be surprised if the funding that remains has become an area to target. Programs that nobody is looking out for are easy to cut when budgets get tight.

Against this backdrop, funding has been cut both for pilots, as well as the office itself. NIST has also worked to roll many of the dollars from NSTIC and the TIG into the National Cybersecurity Center of Excellence (NCCoE). A number of key experts from TIG have left NIST in this environment – or been assigned to other projects – and not been replaced.

The history I provided above is hopefully helpful as background for the current budget environment. However, the more important question is: what should the government be doing in 2018 and beyond?

Given that identity continues to be the top vector of attack in cyberspace – and given that many of the challenges with identity verification in the post-breach era continue to get more difficult – I believe it is important for the government to continue to fund a robust Trusted Identities Group at NIST. The work NIST does here is incredibly relevant; industry is increasingly concerned about the exodus of some of the top leadership from TIG and questioning whether they will be replaced.

As I noted in my testimony: if we’re worried about “Identity Verification in a Post-Breach World,” government should be increasing the government’s budget for research as well as development of better standards and best practices in this area, not cut it back. The FY18 budget cut funding for what is literally the one office in government that is tasked with working with industry on tools that can improve the reliability, security and privacy of biometrics and other next-generation authentication technologies.

The dangers of cutting TIG and other relevant NIST cyber identity research are that it means that the government is stepping back from its important leadership role at a time when identity challenges – and attacks – keep growing, and both government and industry need additional help. NIST plays a critical role here – and if they abdicate that role, I do not believe other entities in or out of government are poised to fill the gap.

Note that I do not believe that the budget for the NSTIC pilots need to be reinstated – at least not in their previous form. The pilots addressed a specific gap in the marketplace at a specific time.

I do believe, however, that there may be a future need for some sort of similar grant funding to support the next round of work in addressing identity verification challenges in the post-breach world. NSTIC demonstrated that a relatively small amount of funding can help to catalyze the market to create and implement better identity solutions, and as government considers the next wave of activities to improve identity, there may be areas where resources are needed to move things forward.